Date Found	Type	Risky Data Type	Module	Children	Correlations	Distance	Starred	Annotation	
2023-05-12 02:53:17	IPv6 Address	No	Mnemonic PassiveDNS	16	0	1	0	None	2a06:98c1:3121::1
2023-05-12 03:09:08	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	165.232.113.95
2023-05-12 02:55:01	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-12T01:28:39.865Z", "ip": "188.114.96.1", "location_updated_at": "2023-04-29T20:40:06.346917Z", "autonomou "lt.makingprojec.com": {"record_type": "A", "resolved_at": "2022-10-24T13:34:44.275517531Z"}, "mybots.amirhsvip.ir": {"record_type": " {"record_type": "A", "resolved_at": "2022-09-30T15:32:44.686639976Z"}, "download.8t.cx": {"record_type": "A", "resolved_at": "2023-02- {"record_type": "A", "resolved_at": "2023-01-21T13:35:04.083346865Z"}, "mytampered.golf": {"record_type": "A", "resolved_at": "2022-12 16T01:18:53.784985236Z"}, "inthemachine.com.au": {"record_type": "A", "resolved_at": "2023-04-15T12:22:39.481058126Z"}, "www.athletich
2023-05-12 03:33:52	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	"Exif 8Photoshop 3.0 mntrRGB XYZ acspAPPL -appl 0cprt Pwtpt chad gTRC mluc 3mluc 2XYZ 5CrOZpRG? rE8d0'8 hl1b1 GJ2W< zkHdm J\pwt P49$v
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Playstation Network (Category: gaming) https://psnprofiles.com/xhr/search/users?q=ayshoo
2023-05-12 03:00:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.23): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:19	Web Content Type	No	Web Spider	0	0	4	0	None	application/javascript
2023-05-12 03:13:04	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [000justin000.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Powered_By": "DISPLAY_UTF8", "Keep_Alive": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Connec
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:03:2F:04:BB:BC)
2023-05-12 02:54:20	HTTP Headers	No	Censys	0	0	4	0	None	{"Content_Length": ["0"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "
2023-05-12 03:10:04	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	cloudflare.com
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	scratch (Category: coding) https://scratch.mit.edu/users/ayhu/
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	4	0	3	0	None	https://funny.battleb0t.xyz/gallery.css
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	PP2104 (Net ID: 00:19:CB:7B:6C:D7)
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Pragma": "DISPLAY_UTF8", "Set_Cookie": "DISPLAY_UTF8", "X_Content_Type_Options": "DISPLAY_UTF8", "Connection": "DISPLA
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BeensGroep (Net ID: 00:01:21:1C:17:B0)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	KNOLBEHEER (Net ID: 00:01:24:F0:5F:22)
2023-05-12 02:50:29	Physical Address	No	GLEIF	1	0	3	0	None	2155 E. GoDaddy Way, Tempe, US-AZ, US, 85284
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	2	0	3	0	None	https://pics.battleb0t.xyz/images/reveloder.jpg
2023-05-12 02:56:30	Physical Location	No	Fraudguard	0	0	3	0	None	Germany, Hesse, Frankfurt am Main
2023-05-12 03:09:46	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	66.170.74.34.bc.googleusercontent.com
2023-05-12 02:44:35	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	netlify.app
2023-05-	Co-Hosted	No	SSL Certificate	0	1	2	0	None	

12 02:44:15	Site		Analyzer						netlify.app
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 03:34:02	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	IDATx m_p Y 0a6-X h5Zh5b 4L8uS >m7xY YGhP5 10IMLR bc<p0 :"CGlZ k>04D A nL/ "KBt:-t h\dHkQU 2<qC jg>v\i AW$@C V3\/g :>2'F WF93l IDATV S
2023-05-12 02:53:56	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:50c0:8001::/48
2023-05-12 02:46:55	Internet Name	No	DNS Resolver	0	0	2	0	None	panel.battleb0t.xyz
2023-05-12 03:09:16	Co-Hosted Site - Domain Whois	No	Whois	3	0	3	0	None	Domain Name: nom-nom.link Registry Domain ID: DO_219392db582b99394c2ad318b07284eb-UR Registrar WHOIS Server: whois.namecheap.com Regis the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the quer processes that send queries or data to the systems of any Registrar or any Registry except as reasonably necessary to register domain 6779e29dade44d91b5a12e78669866ac.protect@withheldforprivacy.com Name Server: rachel.ns.cloudflare.com Name Server: wesley.ns.cloudflar
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.200): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	reflektions (Net ID: 00:01:38:8D:E0:8C)
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 03:23:09	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.0:2053
2023-05-12 02:54:21	HTTP Headers	No	Web Spider	2	0	5	0	None	{"x-content-type-options": "nosniff", "content-encoding": "gzip", "transfer-encoding": "chunked", "expires": "Fri, 12 May 2023 04:54:2
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 02:54:21	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "104.18.40.148:443"\n "142.250.189.174:443"\n "142.251.2.156:443"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identi (f+="&sign="+Hh.se);var g=Qh||Zh?gs(b,f):void 0;g||(g=So("https://","http://",Hh.Gd+f));Cl().destination[a]={state:1,context:c};mc(g)} boozt-08d85fbec897e7d82f0a6036c9faf79f_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUID: N/A]\n "logo-white-arcticsho "_257433F7-CA39-11ED-BBDD-0800270C1BB7_.dat" has type "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]
2023-05-12 03:31:58	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.0:8080
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: <REDACTED> Cache-Control: no-cache, no-store, must-re
2023-05-12 02:51:07	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [172.67.135.9] https://www.virustotal.com/en/ip-address/172.67.135.9/information/
2023-05-12 03:08:47	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.225
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.215): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:31	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	tiktok.battleb0t.xyz
2023-05-12 03:00:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.22): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:15	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.135): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:56	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-	Co-Hosted	No	SSL Certificate	0	0	2	0	None	

12 02:44:24	Site - Domain Name		Analyzer						github.com
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	draadloos (Net ID: 00:01:E3:4A:CD:74)
2023-05-12 02:59:51	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	jloup@gzip.org
2023-05-12 03:11:20	Physical Coordinates	No	AbstractAPI	0	0	3	0	None	50.1188, 8.6843
2023-05-12 02:57:24	Internet Name	No	Certificate Transparency	0	0	1	0	None	nwapi.battleb0t.xyz
2023-05-12 02:47:55	SSL Certificate - Raw Data	No	Certificate Transparency	2	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:02:6d:eb:8d:63:78:04:f2:b8:5c:db:39:06:ab:26:ed:a9 Signature Algorithm: sha256Wi 73:d4:39:8b:bb:51:02:17:cb:89:c6:27:d9:b8:f2:7c:d7:bd: a5:b5:9a:11
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	oconnell (Net ID: 00:02:2D:2F:3E:1F)
2023-05-12 03:32:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.8:443
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.196): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:51	HTTP Headers	No	Censys	0	0	3	0	None	{"Date": ["<REDACTED>"], "_encoding": {"Date": "DISPLAY_UTF8", "Content_Length": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "S
2023-05-12 03:00:36	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	28efa154c841448e9e98cc948672b2d4.protect@withheldforprivacy.com
2023-05-12 02:57:23	Internet Name	No	Certificate Transparency	0	0	1	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:37:42	Physical Location	No	MetaDefender	0	0	3	0	None	Frankfurt Am Main, Germany
2023-05-12 03:00:50	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0.github.io
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:33:50	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	pHYs iTXtXML:com.adobe.xmp <xmp:CreatorTool>Adobe ImageReady</xmp:CreatorTool> <tiff:Orientation>1</tiff:Orientation> </rdf:Descriptio
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2082
2023-05-12 02:58:45	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 0c:e3:f4:1c:e8:cb:bb:cf:13:f7:6c:6f:36:5e:c2:eb Signature Algorithm: sha256WithRSAE a8:21:d4:b0:1c:8c:61:d9:0a:ed:8a:98:0e:ec:59:d1:7e:8a: 57:4f:81:85:21:9d:81:17:a5:6d:50:b7:02:17:30:3f:51:39: 0f:0d:a8:d9:9c:3b:6f:9f:
2023-05-12 02:44:07	Software Used	Yes	Tool - Wappalyzer	0	0	1	0	None	Varnish
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	iTrack at Milbank (Net ID: 00:02:2D:2D:57:34)
2023-05-12 02:51:45	Raw Data from RIRs	No	Hybrid Analysis	2	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "stats.g.doubleclick.net"\n "webrtc.github.io"\n "www.bigmarker.com"'}, {u'category': u'General', u'origin': u'File/Memory', u'identif "urlref_httpswww.bigmarker.comtaxadminThe-Inbound-Customer-Experiencebmid_a85668108cb3_bmid_type_member")'}, {u'category': u'Unusual C Indicator: "key.com")\n ""baseballmonkey.com"," (Source: wallet-stable.json, Indicator: "key.com")'}, {u'category': u'Installation/Per "Add-Content"; File: "urlref_httpswww.bigmarker.comtaxadminThe-Inbound-Customer-Experiencebmid_a85668108cb3_bmid_type_member")'}, {u'c
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	datezone (Category: XXXPORNXXX) https://www.datezone.com/users/login/
2023-05-12 02:55:15	Software Used	Yes	Censys	0	0	3	0	None	openssh
2023-05-12 02:54:07	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:4700:3031::/48

2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Jacobson1 (Net ID: 00:09:5B:C6:54:54)
2023-05-12 02:54:51	Physical Location	No	Censys	0	0	3	0	None	North Charleston, South Carolina, 29418, United States, North America
2023-05-12 03:33:50	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	pHYs tEXtSoftware ezgif.com IDATx owqpphF \\\`gg !LHH EEEF3 HJJBDD //Oq bcc1o mll84 jerrrLl Q_dv4k <x _! 8xOOO 322H\\ BHnn.y vvv$..NI
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	devRant (Category: coding) https://devrant.com/users/login
2023-05-12 02:54:48	Open TCP Port	No	Censys	0	0	3	0	None	34.148.97.127:80
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	MS54GURN (Net ID: 00:0D:3A:70:7B:09)
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00nave198.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	00:02:2D:05:7E:8A (Net ID: 00:02:2D:05:7E:8A)
2023-05-12 02:45:44	Physical Coordinates	No	AbstractAPI	43	0	2	0	None	37.751, -97.822
2023-05-12 02:44:40	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	jQuery CDN
2023-05-12 02:44:07	Internet Name	No	CertSpotter	44	0	1	0	None	www.battleb0t.xyz
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	VIGO (Net ID: 00:01:E3:4A:C7:EB)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:77:9F:5D)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	fse2 (Net ID: 00:01:38:A0:A1:09)
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	7717 7361 (Net ID: 00:00:C5:FC:FE:34)
2023-05-12 02:52:05	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': 00000000-00006768]\n "History" has type "SQLite 3.x database last written using SQLite version 3039003"- Location: [%LOCALAPPDATA%\\Mi with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\be503e2a-334b-416d-8133-7309c5f020e8.tmp]- [targetUI Data\\Default\\f838898f-efdb-43ba-a200-ee2debfcb004.tmp]- [targetUID: 00000000-00006768]\n "9fa1a642-dc59-4b5c-b3dc-8b2fdacab608.tmp"
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	tc (Net ID: 00:12:BF:FD:D7:70)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Maingau (Net ID: 00:02:2D:74:7A:73)
2023-05-12 02:52:45	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [35.229.48.116] https://www.virustotal.com/en/ip-address/35.229.48.116/information/
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	YILBEKKIMYA (Net ID: 00:02:CF:C6:17:D5)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:26:98:C5)
2023-05-12 03:01:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.240): Search Engine Last Activity: 0 days ago Threat Level: 29

2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	kids (Net ID: 00:0C:41:FC:94:E2)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	myLGNet (Net ID: 00:01:36:41:8C:04)
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.96): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	1	0	2	0	None	001viet.com
2023-05-12 02:44:35	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:cd:b7:3c:d6:71:f3:4f:d0:0b:1c:3a:89:f9:32:41:9b:99 Signature Algorithm: sha256Wi Extensions: none Signature : ecdsa-with-SHA256 30:44:02:20:7D:43:FE:B2:8F:39:1E:47:D3:4E:E0:E7: C1:B1:8B:57:06:D2:76:ED:81:DE:13:92:4B
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.140): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Brandis Wifi 2GHz (Net ID: 00:01:9F:20:CA:50)
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:2087
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MainSurf (Net ID: 00:02:2D:8B:15:E0)
2023-05-12 02:55:21	Software Used	Yes	Censys	0	0	3	0	None	Ubuntu Linux
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	CFS (Net ID: 00:18:39:0C:15:86)
2023-05-12 02:49:32	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\Local\\VERMGMTBlockListFileMutex"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_FILEMAPSWITCH_ "urlblockindex_1_.bin" as clean (type is "data")\n Antivirus vendors marked dropped file "TarF3EF.tmp" as clean (type is "data")'}, {u Scalable Vector Graphics image"- [targetUID: N/A]\n "5fb4d2ad16e1b572e8f24659_nav-compliance_1_.svg" has type "SVG Scalable Vector Gra image/*;q=0.8, */*;q=0.5Referer: https://preventor.com/solutions/preventor-namesAccept-Language: en-USUser-Agent: Mozilla/5.0 (Windows
2023-05-12 02:54:20	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.207): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Vienna (Net ID: 00:09:5B:B1:9F:16)
2023-05-12 02:53:17	IPv6 Address	No	Mnemonic PassiveDNS	16	0	1	0	None	2a06:98c1:3120::1
2023-05-12 02:59:59	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	robert@broofa.com
2023-05-12 02:53:20	IP Address	No	Mnemonic PassiveDNS	0	0	2	0	None	64.226.81.43
2023-05-12 02:53:32	BGP AS Membership	No	Censys	0	0	2	0	None	54113
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BSL (Net ID: 00:02:2D:39:EF:C9)
2023-05-12 03:10:00	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	ondigitalocean.com
2023-05-12 02:59:56	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	fernando.r@alliedglobal.com

2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-timer: S1683860053.299752,VS0,VE13
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	^[^_^_^Y^I (Net ID: 00:02:2D:6F:81:A0)
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 02:44:28	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:89:fe:30:65:f6:62:86:64:4f:34:07:5e:a0:a9:be:d2:24 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: C4:B4: 40:6e:0f:4b:38:de:68:41:9a:1e:f9:be:5b:6a:36:f0:9b:22: e3:a1:e1:ad:96:f6:ba:a2:d1:f4:e2:12:cb:ab:1f:bb:9a:53: 07:6b:08:bd:4c:58:68:74:
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:2083
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	10:37:58 (Net ID: 00:02:2D:28:06:03)
2023-05-12 02:44:09	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	2	1	1	0	None	github.io
2023-05-12 02:44:17	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:50c0:8002::153
2023-05-12 02:56:57	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 02:44:13	IP Address	No	DNS Resolver	107	0	1	0	None	185.199.109.153
2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.124
2023-05-12 03:00:50	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	000.github.io
2023-05-12 02:58:43	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	1	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:31:33	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namecheap.com
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2052
2023-05-12 02:54:30	Physical Location	No	Censys	1	0	3	0	None	Frankfurt am Main, Hesse, 60306, Germany, Europe
2023-05-12 02:45:10	Raw Data from RIRs	No	Hybrid Analysis	1	0	1	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'de lines with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\8c133cbc-cb4f-4494-9a53-681a41c38ec8.tmp]- [ta "https://creativecommons.org/compatiblelicenses"\n Pattern match: "https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imag very long lines with no line terminators"- Location: [%TEMP%\\7052_16790919\\adblock_snippet.js]- [targetUID: 00000000-00007052]\n "au
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	7567 3371 (Net ID: 00:00:C5:F7:76:3C)
2023-05-12 02:56:52	Internet Name	No	DNS Resolver	0	0	3	0	None	nwapi.battleb0t.xyz
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Cross-platform software
2023-05-12 03:34:36	BGP AS Membership	No	RIPE	0	0	4	0	None	44486
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	default (Net ID: 00:11:6B:13:88:06)
2023-05-12 03:04:46	Hosting Provider	No	Hosting Provider Identifier	0	0	3	0	None	PEER 1: http://www.peer1.com/

2023-05-12 03:01:00	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.105): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	My Passport (2.4 GHz) - 07B79D (Net ID: 00:00:C0:07:B7:9D)
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	MCName (Minecraft) (Category: gaming) https://mcname.info/en/search?q=battleb0t
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Audiojungle (Category: music) https://audiojungle.net/user/login
2023-05-12 02:54:23	Open TCP Port	No	Censys	0	0	4	0	None	2600:1f18:2489:8201::c8:80
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	4	0	None	Iceland
2023-05-12 02:49:22	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'ca "77EC63BDA74BD0D0E0426DC8F8008506" has type "Microsoft Cabinet archive data Windows 2000/XP setup 62582 bytes 1 file at 0x2c +A "authr Files\\Content.IE5\\37NU00GP\\59XOOQKO.htm]- [targetUID: 00000000-00003364]\n "QJEP1X8E.txt" has type "ASCII text"- Location: [%APPDAT u'description': u'"\ufffd\ufffd\ufffdy\ufffd\ufffd\u01b6gb^\ufffd\ufffd\ufffd}\ufffd\ufffdi\ufffd6\ufffd\ufffd\ufffd\ufffd\ufffd\ufffd
2023-05-12 03:00:25	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha1-etm@openssh.com
2023-05-12 03:03:17	Internet Name	No	DNS Resolver	0	0	2	0	None	www.ayhu.xyz
2023-05-12 03:10:24	Malicious IP Address	Yes	Threat Jammer	0	1	2	0	None	Threat Jammer - Risk score: 40 (MEDIUM) https://threatjammer.com/info/188.114.97.1
2023-05-12 02:53:35	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis "%WINDIR%\\System32\\api-ms-win-downlevel-shlwapi-l1-1-0.dll" at 75840000\n "iexplore.exe" loaded module "%WINDIR%\\System32\\shlwapi. "%WINDIR%\\System32\\WSHTCPIP.DLL" at 74B70000\n "iexplore.exe" loaded module "%WINDIR%\\System32\\dnsapi.dll" at 74F80000\n "iexplore module "%WINDIR%\\System32\\sspicli.dll" at 75580000\n "iexplore.exe" loaded module "%PROGRAMFILES%\\Internet Explorer\\IEShims.dll" a "%WINDIR%\\System32\\oleacc.dll" at 6D110000\n "iexplore.exe" loaded module "%WINDIR%\\System32\\oleaccrc.dll" at 021F0000\n "iexplore
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.5): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MobileInternet (Net ID: 00:02:B3:AE:67:D8)
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.159): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:29:45	Blacklisted IP Address	Yes	UCEPROTECT	0	1	3	0	None	UCEPROTECT - Level 2 (some false positives) (46.101.229.70)
2023-05-12 02:44:27	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	HTTP/3
2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	172.67.168.252
2023-05-12 03:10:23	Malicious IP on Same Subnet	Yes	VoIPBL OpenPBX IPs	0	0	4	0	None	VOIPBL Publicly Accessible PBX List [207.154.224.0/20] http://www.voipbl.org/update
2023-05-12 02:55:14	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 8, u'descr "Embedded OpenType (EOT) Font Awesome 5 Free Solid family"- [targetUID: N/A]\n "simple-jekyll-search.min_1_.js" has type "HTML documen cache: MISS\nX-GitHub-Request-Id: 285E:9A97:2F5E56:376309:63F4C196\nAccept-Ranges: bytes\nDate: Tue, 21 Feb 2023 13:05:27 GMT\nVia: 1. j3\nBGJ3&DQ~NO!QQp|(\'4G 9<pS4M0J2O]Khz=@La2z2AHB~hsN@DI;9Z$,@q7iqD=Qh/NjAC*\'<Eq&HX\n1L_2)GJpU%\n8Z5$1KaxV+y@C7aF\\u8:fx6u:XwSoAx"\'f
2023-05-12 03:16:24	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'NH', u'country_tld': u'.nl', u'ip': u'188.114.97.1', u'currency_name': u'Euro', u'currency': u'EUR', u'country_popu
2023-05-12 03:33:13	Web Content Language	No	Language Detector	0	0	3	0	None	English
2023-05-12 03:19:00	WiFi Access	No	Wigle.net	0	0	3	0	None	MOZAMBIQUE345 (Net ID: 00:01:E3:54:D4:57)

	Point Nearby								
2023-05-12 02:54:57	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-08T23:15:43.655Z", "ip": "2a06:98c1:3120::1", "location_updated_at": "2023-04-30T00:57:18.734276Z", "auto "resolved_at": "2022-10-30T17:30:49.591604261Z"}, "www.133335.xyz": {"record_type": "AAAA", "resolved_at": "2022-09-25T19:02:08.754559 ["*/*"]}, "method": "GET", "uri": "http://[2a06:98c1:3120::1]/"}, "response": {"body": "<!DOCTYPE html>\n<!--[if lt IE 7]> <html class translate=\"enable_cookies\">Please enable cookies. \n <div id=\"cf-error-details\" class=\"p-0\">\n <header class=\"mx-auto pt-1 id=\"feedback-button-no\" type=\"button\">No</button>\n \n <div class=\"feedback-success feedback-hidden\" id=\"error-feedback-s
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.64): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:09:18	Vulnerability - General	Yes	Tool - Retire.js	0	0	4	0	None	CVE-2018-14042 Score: Unknown Description: Unknown
2023-05-12 03:11:21	Physical Location	No	AbstractAPI	0	0	3	0	None	Frankfurt am Main, Hesse, 60313, Germany, Europe
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	FruityWifi-004 (Net ID: 00:04:E2:F4:8A:F5)
2023-05-12 03:01:18	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.158): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:22	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 02:48:03	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"gabu0912.github.io"\n "i.ibb.co"\n "query.prod.cms.m "PNG image data 552 x 338 8-bit/color RGBA non-interlaced" and extension "png"\n "tab-content-1_1_.png" has type "PNG image data 915 x "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%TEMP%\\Cab2CC1.tmp]- [targetUID: 00000000-00002972]\n "Cab2DAD.tmp" "c:\\users\\%osuser%\\appdata\\local\\microsoft\\internet explorer\\recovery\\high\\active\\{616d4f3b-ebb5-11ed-9a79-08002777c70f}.dat
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Microsoft subsidiaries
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.84): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:16	Internet Name	No	DNS Resolver	0	0	2	0	None	www.ayhu.xyz
2023-05-12 02:44:40	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Bootstrap
2023-05-12 02:55:58	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\InternetShortcutMutex"\n "{5312EE61-79E3-4A24-BFE1-132B85B23C3A}"\n "IsoScope_f04_IE_EarlyTabStart_0xf70_Mutex"\n "Local\\!Bro +A "authroot.stl" number 1 6 datablocks 0x1 compression"\n "77EC63BDA74BD0D0E0426DC8F8008506" has type "Microsoft Cabinet archive data "~DF0DA2B49B9610E864.TMP" has type "data"- Location: [%TEMP%\\~DF0DA2B49B9610E864.TMP]- [targetUID: 00000000-00003844]\n "RecoveryStor Related', u'origin': u'File/Memory', u'identifier': u'string-3', u'name': u'Found potential URL in binary/memory', u'attck_id_wiki': N
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	flinck (Net ID: 00:01:24:F1:89:80)
2023-05-12 03:13:06	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [007jedgar.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:09:37	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	224.30.196.104.bc.googleusercontent.com
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["163"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Keep_Alive": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "C
2023-05-12 03:03:30	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://pics.battleb0t.xyz/images/master058_1.PNG
2023-05-12 03:34:29	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	45.131.109.62
2023-05-12 03:13:10	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [etherum-libs.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:54:27	Open TCP Port	No	Censys	0	0	4	0	None	2600:1f18:2489:8202::c8:80

2023-05-12 02:44:09	Open TCP Port	No	SSL Certificate Analyzer	0	0	1	0	None	battleb0t.xyz:443
2023-05-12 02:44:05	Web Technology	No	Tool - WAFW00F	0	0	1	0	None	Cloudflare Inc. Cloudflare
2023-05-12 02:44:21	Internet Name	No	DNS Resolver	0	0	2	0	None	nuke.battleb0t.xyz
2023-05-12 02:45:36	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	funny.battleb0t.xyz. 300 IN CNAME frabjous-lebkuchen-324004.netlify.app.
2023-05-12 02:49:34	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'"@ntdll.dll"'}, {u'category': u'General', u'origin': u'Created Mutant', u'identifier': u'mutant-0', u'name': u'Creates mutants', u'a "widevinecdm.dll"'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Drop [targetUID: 00000000-00005628]\n "manifest.fingerprint" has type "ASCII text with no line terminators"- Location: [%LOCALAPPDATA%\\Mic u'File/Memory', u'identifier': u'string-3', u'name': u'Found potential URL in binary/memory', u'attck_id_wiki': None, u'threat_level_h
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	permissions-policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope
2023-05-12 02:57:25	Co-Hosted Site	No	Certificate Transparency	1	0	1	0	None	funny-face-pictures.nom-nom.link
2023-05-12 02:54:23	HTTP Status Code	No	Web Spider	0	0	4	0	None	403
2023-05-12 03:09:59	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	stage-sdb-n1-fra1.amcodev.me
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<hidden ssid> (Net ID: 00:01:E3:55:E9:E6)
2023-05-12 03:24:51	Country	No	Country Name Extractor	0	0	7	0	None	United States
2023-05-12 02:57:21	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\IsoScope_af8_ConnHashTable<2808>_HashTable_Mutex"\n "\\Sessions\\1\\BaseNamedObjects\\{5312EE61-79E3 Characteristics', u'origin': u'Binary File', u'identifier': u'binary-5', u'name': u'Drops cabinet archive files', u'attck_id_wiki': No "6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptne u'Malicious artifacts seen in the context of a contacted host', u'attck_id_wiki': None, u'threat_level_human': u'suspicious', u'capec_
2023-05-12 03:00:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.45): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	DMHS (Net ID: 00:02:2D:0B:17:3E)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-B3C2 (Net ID: 00:1D:D4:40:B3:C0)
2023-05-12 03:09:27	Co-Hosted Site - Domain Whois	No	Whois	2	0	4	0	None	Domain Name: 00RZ.COM Registry Domain ID: 1545841665_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://w only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transm Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.48062425 support the dissemination or collection of this data, in part or in its entirety, for any purpose, such as transmission by e-mail, tel
2023-05-12 02:44:24	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 02:54:12	Web Content Type	No	Web Spider	0	0	1	0	None	text/html;charset=utf-8
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Garmin connect (Category: health) https://connect.garmin.com/modern/profile/login
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:DB:1C:01)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	bl?htwlan (Net ID: 00:02:72:5E:F0:C4)
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:2096

2023-05-12 02:54:13	Raw Data from RIRs	No	Censys	0	0	4	0	None	{"last_updated_at": "2023-05-11T21:43:49.790Z", "ip": "2606:4700:3030::ac43:a8fc", "location_updated_at": "2023-05-05T16:26:00.823616Z 02T14:40:23.496602167Z"}, "domainwheel.vipe.us": {"record_type": "AAAA", "resolved_at": "2023-05-04T22:48:08.612020608Z"}, "take2s.com "resolved_at": "2023-04-14T02:12:59.832119313Z"}, "www.farasoacademy.com": {"record_type": "AAAA", "resolved_at": "2023-04-24T14:37:26 "resolved_at": "2023-05-09T14:49:34.524954322Z"}, "nieqiulemoru.gq": {"record_type": "AAAA", "resolved_at": "2023-05-03T17:22:24.19076 01T20:45:04.713699318Z"}, "zunbazapecomfo.tk": {"record_type": "AAAA", "resolved_at": "2023-05-10T20:52:13.680560969Z"}, "tiosmarigin.
2023-05-12 02:54:57	Physical Location	No	Censys	1	0	2	0	None	Hounslow, England, TW3, United Kingdom, Europe
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	jeja.pl (Category: misc) https://www.jeja.pl/user,login
2023-05-12 03:04:06	Malicious IP on Same Subnet	Yes	Greensnow	0	0	4	0	None	greensnow.co [64.226.80.0/20] https://blocklist.greensnow.co/greensnow.txt
2023-05-12 02:59:50	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@ecloanmoney.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	forumprawne.org (Category: misc) https://forumprawne.org/members/login.html
2023-05-12 02:44:17	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:91:08:65:b4:56:94:e3:89:37:6b:c8:ee:5a:fc:f4:80:52 Signature Algorithm: sha256Wi 2e:6c:74:7c:a4:74:32:5e:57:3b:4d:1a:2e:c8:ca:50:8a:41: 64:52:bd:34:33:b5:79:5d:6f:b7:40:8d:f2:19:bb:9c:7a:f4: 53:d5:b8:14:be:47:eb:83:
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	6	0	None	MarkMonitor Inc.
2023-05-12 03:13:03	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [000407.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-timer: S1683860053.050131,VS0,VE21
2023-05-12 02:54:14	HTTP Headers	No	Web Spider	1	0	2	0	None	{"content-encoding": "gzip", "transfer-encoding": "chunked", "vary": "Accept-Encoding", "server": "nginx", "connection": "keep-alive",
2023-05-12 03:24:47	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 02:58:34	SSL Certificate - Raw Data	No	Certificate Transparency	2	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:7b:a3:67:f4:76:b8:d0:86:bd:aa:81:68:7c:78:c6:53:24 Signature Algorithm: sha256Wi 19:07:08.083 2022 GMT Extensions: none Signature : ecdsa-with-SHA256 30:46:02:21:00:D0:FF:78:AE:C3:62:89:90:F2:A9:F6: CF:41:A5:B6:AB:5
2023-05-12 03:11:24	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'format': {u'international': u'+14805058800', u'local': u'(480) 505-8800'}, u'country': {u'prefix': u'+1', u'code': u'US', u'name':
2023-05-12 03:29:46	Blacklisted IP Address	Yes	UCEPROTECT	0	1	3	0	None	UCEPROTECT - Level 2 (some false positives) (207.154.228.169)
2023-05-12 02:55:21	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["46"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "X_Xss_Protection": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8",
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 02:44:13	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	1	2	0	None	github.com
2023-05-12 03:00:58	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0101kvmt.github.io
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Git (software)
2023-05-12 02:44:12	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	www.battleb0t.xyz:443
2023-05-12 02:57:22	Internet Name	No	Certificate Transparency	0	0	1	0	None	kekw.battleb0t.xyz
2023-05-12 03:09:31	Affiliate - Internet Name	No	DNS Resolver	2	0	3	0	None	cdn-185-199-111-154.github.com
2023-05-12 03:01:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.127): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:35:41	Physical Location	No	ipapi.co	1	0	3	0	None	Eygelshoven, Limburg, LI, Netherlands, NL
2023-05-12	Open TCP Port	No	Pulsedive	0	0	2	0	None	104.21.6.166:443

02:47:30									
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	5	0	None	cloudflare
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Maxx Hotel (Net ID: 00:02:2D:37:37:61)
2023-05-12 02:44:12	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	cloudwaysapps.com
2023-05-12 03:09:03	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.103
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	001328.github.io
2023-05-12 03:04:12	Malicious Co-Hosted Site	Yes	abuse.ch	0	1	2	0	None	abuse.ch URLhaus (Domain) [github.com] https://urlhaus.abuse.ch/downloads/csv_recent/
2023-05-12 02:53:03	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	None None
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet8FBA (Net ID: 00:01:36:5C:8F:B8)
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-64@openssh.com
2023-05-12 03:00:25	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-64@openssh.com
2023-05-12 03:16:17	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	ayu.xyz
2023-05-12 02:44:23	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:4d:72:d7:7c:dd:a7:02:dd:5a:67:f2:a2:3b:bd:d9 Signature Algorithm: sha256WithRSAE - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1-1.crt X509v3 Basic Constraints fa:29:72:01:3e:b7:06:f1:2f:1a:0e:91:c5:ec:35:bf:f5:da: 33:95:de:24:12:0d:f5:c3:23:8d:40:82:d1:5c:eb:de:0a:08: e8:e5:83:e5:0a:8b:3a:5e:
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Wireless (Net ID: 00:09:5B:34:6B:03)
2023-05-12 02:54:44	Physical Location	No	Censys	0	0	3	0	None	North Charleston, South Carolina, 29418, United States, North America
2023-05-12 03:18:06	Externally Hosted Javascript	No	Page Information	0	0	3	0	None	http://code.jquery.com/jquery-3.2.1.js
2023-05-12 03:09:01	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.96
2023-05-12 03:03:51	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	scoop.sh
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.167): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:10	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2023-05-12 02:56:25	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2023-05-12 02:59:45	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: BATTLEBOT.XYZ Registry Domain ID: D199559633-CNIC Registrar WHOIS Server: whois.namecheap.com Registrar URL: https://name than determining ownership of domain names, (2) not to store or reproduce this data in any way, (3) not to use any high-volume, automa State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext:
2023-05-12 03:05:41	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12	Blacklisted IP on Same	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.237): Search Engine Last Activity: 0 days ago Threat Level: 29

03:01:44	Subnet								
2023-05-12 03:09:54	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet2EE2 (Net ID: 00:01:36:5B:2E:E0)
2023-05-12 03:09:28	Co-Hosted Site	No	SSL Certificate Analyzer	1	0	3	0	None	www.donation.ecash-pay.com
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-128-etm@openssh.com
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet (Net ID: 00:01:36:36:56:5A)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	gfycat (Category: misc) https://gfycat.com/@login
2023-05-12 02:45:34	DNS SPF Record	No	DNS Raw Records	0	0	1	0	None	v=spf1 include:_spf.mx.cloudflare.net ~all
2023-05-12 02:59:00	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "IsoScope_eb4_IESQMMUTEX_0_331"\n "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "Local\\!BrowserEmulation!SharedMemory!Mutex"\n "IsoScope_eb4_IE_ "6BADA8974A10C4BD62CC921D13E43B18_28DEA62A0AE77228DD387E155AD0BA27" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptne "620BEF1064BD8E252C599957B3C91896" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\620BEF1064BD "C:\\Program Files\\Microsoft Office\\Office14\\OUTLLIB.DLL.DLL"\n "iexplore.exe" trying to touch file "C:\\Program Files\\Internet Ex
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.238): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:10:06	Malicious IP Address	Yes	VoIPBL OpenPBX IPs	0	1	2	0	None	VOIPBL Publicly Accessible PBX List [185.199.108.153] http://www.voipbl.org/update
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:02:2D:51:66:85)
2023-05-12 02:44:42	Internet Name	No	DNS Resolver	0	0	2	0	None	panel.battleb0t.xyz
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ANY (Net ID: 00:04:E2:0E:BB:DF)
2023-05-12 02:45:49	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'Chicago', u'security': {u'is_vpn': False}, u'city_geoname_id': 4887398, u'region_geoname_id': 4896861, u'country': u'Unite
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	palnet (Category: finance) https://www.palnet.io/@login
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:07:40:61:40:4D)
2023-05-12 03:09:18	Vulnerability - General	Yes	Tool - Retire.js	0	0	4	0	None	CVE-2018-14040 Score: Unknown Description: Unknown
2023-05-12 03:03:19	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ASE VISITORS (Net ID: 00:03:52:A1:3D:40)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_ipad (Net ID: 00:0C:E6:08:59:05)
2023-05-12 02:54:51	BGP AS Membership	No	Censys	0	0	3	0	None	396982
2023-05-12 03:11:25	Physical Location	No	AbstractAPI	0	0	3	0	None	Arizona, United States

2023-05-12 03:03:27	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-mitigated: challenge
2023-05-12 02:53:15	IPv6 Address	No	Mnemonic PassiveDNS	0	0	1	0	None	2606:50c0:8000::153
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	GBC_Insaat (Net ID: 00:14:C1:0B:28:CC)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	celikpalas (Net ID: 00:12:17:70:0F:C1)
2023-05-12 02:54:13	Open TCP Port Banner	No	Censys	0	0	4	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.210): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	ImageShack (Category: images) https://imageshack.com/user/ayhu
2023-05-12 02:59:51	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	madler@alumni.caltech.edu
2023-05-12 03:03:31	Co-Hosted Site - Domain Name	No	DNS Resolver	1	0	3	0	None	007316.xyz
2023-05-12 03:23:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.6:8080
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:22
2023-05-12 02:52:41	Raw Data from RIRs	No	Hybrid Analysis	3	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'de u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 2, u'description': u'"(0, propert u'"b38d7abaf0f5f8fb484f9be1484e98a17ea16df2_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUID: N/A]\n "f0438febff76847 [%LOCALAPPDATA%\\Microsoft\\Internet Explorer\\DomainSuggestions\\en-US.4]- [targetUID: 00000000-00001416]\n "RecoveryStore._88B090C0-
2023-05-12 02:56:36	Raw Data from RIRs	No	Hybrid Analysis	2	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\!BrowserEmulation!SharedMemory!Mutex"\n "Local\\URLBLOCK_FILEMAPSWITCH_MUTEX_3328"\n "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "IsoSc [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\6DB145CFEEC544B1582FED1ADA3370DD]- [targetUID: 00000000-00003328]\n "69C6F [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\57C8EDB95DF3F0AD4EE2DC2B8CFD4157]- [targetUID: 00000000-00003328]\n "BCB67 match: "crl.rootg2.amazontrust.com"- [Source: PCAP]\n Heuristic match: "GET /rootg2.crl HTTP/1.1\nConnection: Keep-Alive\nAccept: */*\
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	FruityWifi-003 (Net ID: 00:07:0E:65:CF:39)
2023-05-12 02:45:51	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'Montreal', u'security': {u'is_vpn': False}, u'city_geoname_id': 6077243, u'region_geoname_id': 6115047, u'country': u'Unit
2023-05-12 02:44:26	Internet Name	No	DNS Resolver	0	0	2	0	None	battleb0t.xyz
2023-05-12 02:55:28	Physical Location	No	URLScan.io	0	0	2	0	None	DE
2023-05-12 03:03:24	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:45:34	Raw DNS Records	No	DNS Raw Records	0	0	1	0	None	battleb0t.xyz. 300 IN MX 21 route2.mx.cloudflare.net. battleb0t.xyz. 300 IN MX 60 route3.mx.cloudflare.net. battleb0t.xyz. 300 IN MX 6
2023-05-12 03:17:56	Malicious IP on Same Subnet	Yes	CINS Army List	0	0	4	0	None	cinsscore.com [64.226.80.0/20] http://cinsscore.com/list/ci-badguys.txt

2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	2WIRE630 (Net ID: 00:02:2D:23:E0:24)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	HB (Net ID: 00:01:36:35:4A:AA)
2023-05-12 03:16:17	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	ashu.xyz
2023-05-12 03:00:56	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.89): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	WEST4541 (Net ID: 00:12:0E:7E:7A:31)
2023-05-12 02:51:49	Raw Data from RIRs	No	Hybrid Analysis	2	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"api.edgeoffer.microsoft.com"\n "bam.nr-data.net"\n "checkout.strip panelists will discuss a variety of questions including:" (Indicator: "dir "; File: "urlref_httpsclick9.bigmarker.comlinksBY79pHvYX2ZQ Indicator: "ubs.com")\n ""allieandmickey.com"," (Source: wallet-pre-stable.json, Indicator: "key.com")\n ""alteregoscrubs.com"," (Sour file "c:\\users\\%osuser%\\appdata\\local\\microsoft\\edge\\user data\\shadercache\\data_2"\n "msedge.exe" reads file "c:\\users\\%osu
2023-05-12 03:09:27	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	2	0	None	C=US,ST=California,L=San Francisco,O=Cloudflare\, Inc.,CN=sni.cloudflaressl.com
2023-05-12 03:01:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.250): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:50:23	Blacklisted IP Address	Yes	Honeypot Checker	0	1	2	0	None	Honeypotproject (104.21.6.166): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:53:56	Open TCP Port	No	Censys	0	0	2	0	None	2606:50c0:8001::153:80
2023-05-12 02:57:25	Internet Name	No	Certificate Transparency	0	0	1	0	None	funny.battleb0t.xyz
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://funny.battleb0t.xyz/images/master058_1.PNG
2023-05-12 02:45:50	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'Montreal', u'security': {u'is_vpn': False}, u'city_geoname_id': 6077243, u'region_geoname_id': 6115047, u'country': u'Unit
2023-05-12 03:01:17	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.145): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 02:44:38	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:81:34:2e:fd:61:48:b5:6f:11:ca:36:0b:dc:62:9a:cf:52 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: A7:55: 5f:25:e3:22:f8:d8:94:10:30:4c:38:a3:69:e5:a9:44:0f:99: ab:4f:8a:ac:8b:23:68:e6:f5:dc:3a:a2:45:58:75:61:f0:50: 88:14:ff:16:c7:72:ba:24:
2023-05-12 03:03:39	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	a-zoom (Net ID: 00:01:38:D4:87:A3)
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 500 Internal Server Error X-Powered-By: Express Content-Security-Policy: default-src 'none' X-Content-Type-Options: nosniff C
2023-05-12 03:31:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	d3fc0n6@protonmail.com
2023-05-12 03:11:12	Physical Coordinates	No	OpenStreetMap	77	0	4	0	None	33.6170672,-111.90564645297056
2023-05-12 02:44:17	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:50c0:8003::153
2023-05-12 02:44:15	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Express
2023-05-12 02:59:44	Co-Hosted Site - Domain Whois	No	Whois	1	0	2	0	None	Domain Name: GITHUBUSERCONTENT.COM Registry Domain ID: 1845671923_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.markmonitor.com Regist does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may

2023-05-12 02:54:13	Web Content Type	No	Web Spider	0	0	3	0	None	text/css
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	mail.ayhu.xyz
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	eminent819 (Net ID: 00:14:5C:87:8C:58)
2023-05-12 03:00:56	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.88): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	2WIRE681 (Net ID: 00:02:2D:68:92:B3)
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	tripadvisor (Category: social) https://www.tripadvisor.com/Profile/Altpapier
2023-05-12 03:24:33	Malicious Affiliate	Yes	VXVault.net	0	1	4	0	None	VXVault Malicious URL List [cdn-185-199-108-154.github.com] http://vxvault.net/URL_List.php
2023-05-12 02:53:56	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:b3:d3:7f:a8:50:41:aa:70:38:c6:ab:16:2e:24:50:f9:66 Signature Algorithm: sha256Wi 34:bf:dd:34:59:cd:80:f7:bc:54:a0:98:88:5b:c3:c9:31:8c: d5:fb:f3:f4:99:19:e3:f7:7b:0e:cf:b8:fd:2e:98:1e:df:5e: bd:32:3e:95:6e:85:fd:3c:
2023-05-12 02:56:56	Internet Name	No	DNS Resolver	0	0	6	0	None	www.ayhu.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:B9:5F:B7)
2023-05-12 03:15:36	Physical Location	No	ipstack	0	0	2	0	None	Colombia
2023-05-12 02:53:56	BGP AS Membership	No	Censys	0	0	2	0	None	54113
2023-05-12 02:50:30	Legal Entity Identifier	No	GLEIF	0	0	3	0	None	54930014QNWWH8OAC930
2023-05-12 02:54:12	Linked URL - Internal	No	Web Spider	0	0	1	0	None	http://battleb0t.xyz
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	4	0	None	Saint Helena
2023-05-12 02:54:21	HTTP Headers	No	Web Spider	3	0	3	0	None	{"transfer-encoding": "chunked", "expires": "Thu, 01 Jan 1970 00:00:01 GMT", "server": "cloudflare", "connection": "keep-alive", "cach
2023-05-12 02:53:35	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	7717 7361 (Net ID: 00:00:C5:FC:FE:34)
2023-05-12 03:41:52	Open TCP Port	No	Censys	0	0	3	0	None	45.131.109.53:445
2023-05-12 02:44:10	Co-Hosted Site	No	SSL Certificate Analyzer	2	1	1	0	None	githubusercontent.com
2023-05-12 02:46:49	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	3	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 02:5a:61:0f:58:eb:84:f1:ad:53:ae:03:dc:a9:84:7a Signature Algorithm: ecdsa-with-SHA 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: 1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73 Timestamp : Dec 21 09:03:52.857 2022
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MGOKCEN (Net ID: 00:14:C1:2B:03:F6)
2023-05-12 02:44:06	Domain Registrar	No	Whois	0	0	1	0	None	GoDaddy.com, LLC
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:32:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.9:443
2023-05-12	SSL Certificate -	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:8d:d7:e0:05:18:38:a5:db:8a:48:64:f2:68:9a:98:22:c8 Signature Algorithm: sha256Wi

02:44:20	Raw Data								80:6c:fc:c5:84:b0:c5:6b:a0:c4:07:ac:78:f3:1f:48:7e:f7: 86:c2:2f:cf:18:f5:92:dd:9a:51:6a:86:ae:51:1d:75:24:9f: d6:b2:e6:73:f5:1b:4b:e1:
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	suddenlink.net-4030 (Net ID: F8:1D:0F:69:40:38)
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.89): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	wirelessnet (Net ID: 00:04:5A:F9:8F:10)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	12M-5G20E240 (Net ID: 00:01:9F:20:E2:44)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	6	0	None	cf-ray: 7c5f60688e300ce1-EWR
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	BVITestNetz (Net ID: 00:01:E3:47:0D:EB)
2023-05-12 03:33:39	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	IDATx VC6.NV cN u:v O3dufp YEexY?w a:Y7" O5dgc vR K nkRZD 227sO5d ffFsk 4kFQZW /\\J J 4 N AaoCX 9$BfJ cod:5j M:IBU VBjeb d<nDA `CK2nF
2023-05-12 03:33:43	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	"Exif sgssso <Qwm7 >6x.O x>t7? g$sy? .b97< /Ggy! l/5-o ggs43Z x.o.n> NNEsz gmuss Mswy5 dIys6 >t6w6 03Ryr\G a>0xM g_on8 9!6sBsmms ?r:\t
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	4	0	None	China
2023-05-12 03:21:07	Malicious IP on Same Subnet	Yes	Emerging Threats	0	0	4	0	None	emergingthreats.net [46.101.128.0/17] https://rules.emergingthreats.net/blockrules/compromised-ips.txt
2023-05-12 02:44:06	Domain Whois	No	Whois	15	0	1	0	None	Domain Name: BATTLEB0T.XYZ Registry Domain ID: D333902916-CNIC Registrar WHOIS Server: whois.reg.ru Registrar URL: https://www.reg.ru/ any way, (3) not to use any high-volume, automated, electronic processes to obtain data from this service. Abuse of this service is mo System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2023.05.12T05:44:06Z <<< For more information on Whois status co
2023-05-12 03:03:59	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	malsup.github.io
2023-05-12 02:54:41	Raw Data from RIRs	No	Censys	0	0	3	0	None	{"last_updated_at": "2023-05-12T01:05:57.807Z", "ip": "104.196.30.220", "location_updated_at": "2023-05-02T18:59:17.407146Z", "autonom "bloomerly.app": {"record_type": "A", "resolved_at": "2022-12-25T12:05:25.788489726Z"}, "francotorres.dev": {"record_type": "A", "reso "resolved_at": "2023-01-29T13:39:11.151551213Z"}, "rumblewood.com": {"record_type": "A", "resolved_at": "2022-10-17T15:51:32.655397110 29T06:06:29.982491579Z"}, "www.fest.i.ng": {"record_type": "CNAME", "resolved_at": "2023-04-13T19:40:09.807661140Z"}, "www.airbear.ai" "2023-02-19T14:00:29.453539558Z"}, "www.hotflashheatwave.com": {"record_type": "CNAME", "resolved_at": "2023-04-07T00:45:16.120624048Z
2023-05-12 02:45:21	Physical Location	No	ipapi.co	0	0	4	0	None	Ashburn, Virginia, VA, United States, US
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	hhcpatp (Net ID: 00:06:25:3B:8E:16)
2023-05-12 03:01:30	Raw Data from RIRs	No	Tool - WhatWeb	1	0	2	0	None	[{u'request_config': {u'headers': {u'User-Agent': u'Mozilla/5.0'}}, u'target': u'http://nuke.battleb0t.xyz', u'http_status': 521, u'pl
2023-05-12 02:56:58	Internet Name	No	DNS Resolver	0	0	3	0	None	www.ayhu.xyz
2023-05-12 02:44:24	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	3	0	None	Netherlands
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	6	0	None	Montenegro
2023-05-12 02:44:19	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:b6:39:33:af:de:1e:32:f3:fc:2e:76:dc:bc:08:51:86:10 Signature Algorithm: sha256Wi 2023 GMT Extensions: none Signature : ecdsa-with-SHA256 30:46:02:21:00:87:F6:3C:B2:E0:C2:7B:F4:59:32:49: FF:84:EE:E1:AC:5D:A1:7E:84:DE
2023-05-12 02:45:54	Physical Location	No	AbstractAPI	1	0	4	0	None	Ashburn, Virginia, 20149, United States, North America
2023-05-12 02:47:56	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\SM0:6976:120:WilError_01"\n "SM0:6976:120:WilError_01"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifie data-lang="js">// autolink everything that looks like a Twitter username" (Indicator: "dir "; File: "urlref_ht

									stable.json, Indicator: "leu.com")\n ""aspirefashionscrubs.com"," (Source: wallet-pre-stable.json, Indicator: "ubs.com")\n ""augustble "auto_open_controller.js" has type "UTF-8 Unicode text with very long lines with CRLF line terminators"- Location: [%TEMP%\\4044_14342
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Reddit (Category: social) https://www.reddit.com/user/ayhu
2023-05-12 02:54:22	Linked URL - External	No	Web Spider	0	0	4	0	None	https://qolhub.cloudflareaccess.com/cdn-cgi/access/verify-code/panel.battleb0t.xyz?kid=0e8fcd5c4d6f2fbb6bc18c164812f146f66e83d772c2626
2023-05-12 02:54:00	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:54:10	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:4700:3031::/48
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.136): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:09:38	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	106.48.229.35.bc.googleusercontent.com
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Balcioglu (Net ID: 00:1A:2A:63:1A:23)
2023-05-12 02:47:32	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.135.9:8443
2023-05-12 02:44:15	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	1	2	0	None	netlify.app
2023-05-12 03:09:10	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	46.101.229.68
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	AMX (Net ID: 00:02:E3:40:F7:BD)
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:34:24	Affiliate - IP Address	No	DNS Look-aside	0	0	3	0	None	45.131.109.50
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.8): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:11	Co-Hosted Site	No	SSL Certificate Analyzer	4	1	1	0	None	github.com
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpeedStream (Net ID: 00:01:24:F0:82:16)
2023-05-12 03:03:43	Internet Name	No	DNS Resolver	0	0	3	0	None	www.ayhu.xyz
2023-05-12 02:45:17	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:9d:c5:27:de:ee:41:17:4e:89:34:e6:9d:87:79:d7:50:31 Signature Algorithm: sha256Wi none Signature : ecdsa-with-SHA256 30:46:02:21:00:84:8B:29:D3:64:84:A1:88:50:9E:D3: 9D:A2:EF:43:30:D4:86:D3:E7:90:33:F8:14:58:7B:CF: 3
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:57:9F:CA)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATTDGsRAys (Net ID: 88:96:4E:86:44:00)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cross-origin-resource-policy: same-origin
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	NETGEAR48 (Net ID: B0:39:56:06:50:02)
2023-05-12 02:45:35	Internet Name	No	DNSDumpster	0	0	1	0	None	oldfluid.battleb0t.xyz
2023-05-	Co-Hosted	No	HackerTarget	2	0	2	0	None	000yesnt.github.io

12 03:00:53	Site								
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:EB:D7:15)
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	TikTok (Category: social) https://www.tiktok.com/@ayshoo?lang=en
2023-05-12 02:56:46	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: lor.instructure.com\nDNT: 1\nConn Trident/7.0; rv:11.0) like Gecko\nHost: lor.instructure.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "user-agent: ")\n "GET /api/c Language: en-US\nAccept-Encoding: gzip, deflate\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nHost: lor. u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObjects\\UpdatingNewTab
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.198): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom2888 (Net ID: 00:01:38:85:BD:9E)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet (Net ID: 00:01:36:45:9F:3A)
2023-05-12 03:00:52	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.81): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	lcgteach (Net ID: 00:0B:86:22:0F:30)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:02:2D:6A:57:0B)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Apple Network 3668a9 (Net ID: 00:02:2D:00:C6:8F)
2023-05-12 03:09:28	SSL Certificate - Issued to	No	SSL Certificate Analyzer	0	0	3	0	None	CN=donation.ecash-pay.com
2023-05-12 03:03:18	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	mail.ayhu.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Fly By (Net ID: 00:02:6F:5D:6C:20)
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Bug and issue tracking software
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:33:13	Web Content Language	No	Language Detector	0	0	3	0	None	English
2023-05-12 02:44:24	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:01:E3:56:FE:F7)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Disqus (Category: social) https://disqus.com/by/ayhu/
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	art_vacation5.0 (Net ID: 00:01:9F:30:06:7C)
2023-05-12 02:48:40	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\ChromeProcessSingletonStartup!"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identi "twitter")\n "<meta name="twitter:description" content="iHealth is making personal healthcare management easier for everyone! Improve text">Twitter" (Indicator: "twitter")\n "<a class="social-icons__link" href="https://www.linkedin.com/company/ihealth-lab/about [targetUID: 00000000-00004280]\n "0ba2ec1e-18bb-4a7d-80cb-d06eae98d168.tmp" has type "gzip compressed data from FAT filesystem (MS-DOS

2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-fastly-request-id: 4232179a2468cad7d8e788f0a4fe958396bfc091
2023-05-12 03:03:47	Co-Hosted Site	No	ThreatMiner	2	0	2	0	None	malsup.github.io
2023-05-12 02:47:42	Open TCP Port	No	Pulsedive	0	0	3	0	None	35.229.48.116:80
2023-05-12 02:44:42	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 03:24:52	Country	No	Country Name Extractor	0	0	3	0	None	Turkey
2023-05-12 02:45:22	Physical Location	No	ipapi.co	0	0	4	0	None	Ashburn, Virginia, VA, United States, US
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	SoundCloud (Category: music) https://soundcloud.com/ayshoo
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	crowdin (Category: hobby) https://crowdin.com/profile/login
2023-05-12 03:09:43	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	121.97.148.34.bc.googleusercontent.com
2023-05-12 03:18:06	URL (Purely Static)	No	Page Information	0	0	3	0	None	http://nwapi.battleb0t.xyz
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	xfinitywifi (Net ID: 00:0D:67:37:7A:7A)
2023-05-12 03:09:07	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	165.232.113.89
2023-05-12 03:00:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.37): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	ExtraLunchMoney (Category: XXXPORNXXX) https://extralunchmoney.com/user/login
2023-05-12 02:44:15	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:2c:84:3a:08:10:23:75:f2:8a:d5:a0:cb:cc:f6:da:14:6e Signature Algorithm: sha256Wi Extensions: none Signature : ecdsa-with-SHA256 30:45:02:21:00:AA:9D:DE:C7:1A:03:CE:A4:C0:00:4F: 87:A8:C3:99:28:44:9B:D2:01:EB:31:A5:4D
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ThermiCam2Production TRC (Net ID: 00:05:FE:C6:35:F0)
2023-05-12 02:55:27	Physical Location	No	URLScan.io	0	0	1	0	None	US
2023-05-12 02:54:18	HTTP Status Code	No	Web Spider	0	0	2	0	None	200
2023-05-12 02:54:13	Web Content	No	Web Spider	0	0	3	0	None	*{box-sizing:border-box;margin:0;padding:0}html{line-height:1.15;-webkit-text-size-adjust:100%;color:#313131}html,button{font-family:s image:url(prompt:not(.hidden){flex-wrap:wrap;justify-content:center}}.pow-button{margin:2rem 0;background-color:#0051c3;color:#fff}.pow-button:h color:#4693ff}}body.dark{background-color:#222;color:#d9d9d9}body.dark a{color:#fff}body.dark a:hover{text-decoration:underline;color:
2023-05-12 03:27:54	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.138:80
2023-05-12 02:45:34	DNS TXT Record	No	DNS Raw Records	0	0	1	0	None	v=spf1 include:_spf.mx.cloudflare.net ~all
2023-05-12 03:32:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.13:8080
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	my_instants (Category: music) https://www.myinstants.com/en/profile/login/
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.176): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	hk (Net ID: 00:02:A8:1F:B9:47)

2023-05-12 03:23:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.7:8443
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetFBC6 (Net ID: 00:01:36:5A:FB:C4)
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	5	0	None	United States
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	6	0	None	cf-ray: 7c5f60726fad1912-EWR
2023-05-12 02:53:07	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.111.154:80
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Twitter (Category: social) https://twitter.com/ayhu
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 02:53:35	Open TCP Port	No	Censys	0	0	2	0	None	185.199.110.153:443
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	007.github.io
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.220): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:19	Web Content Type	No	Web Spider	0	0	4	0	None	application/javascript
2023-05-12 02:53:02	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	None None
2023-05-12 02:54:30	BGP AS Membership	No	Censys	0	0	3	0	None	14061
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Frodo (Net ID: 00:02:2D:25:7C:6A)
2023-05-12 02:47:29	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "IsoScope_f2c_ConnHashTable<3884>_HashTable_Mutex"\n "\\Sessions\\1\\BaseNamedObjects\\UpdatingNewT Alive\nHost: software.verapdf.org" (Indicator: "user-agent: ")\n "GET /wp-content/themes/veraPDF-site/includes/js/ie10-viewport-bug-wo NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: maxcdn.bootstrapcdn.com\nDNT: 1\nConnection: Keep-Aliv application/javascript, */*;q=0.8\nReferer: https://software.verapdf.org/dev/verapdf_windows-x64_1_18-rc.exe\nAccept-Language: en-US\n
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-proxy-cache: MISS
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:06:25:BA:AB:53)
2023-05-12 03:01:20	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.181): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MatrixEx Guest (Net ID: 00:01:21:26:34:40)
2023-05-12 02:44:29	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	2	0	None	githubusercontent.com
2023-05-12 03:00:53	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.82): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:41	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.109.133:443
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	beeline1 (Net ID: 00:01:38:A8:7B:F3)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Allstate 2.4G (Net ID: 00:02:6F:F8:0A:40)

2023-05-12 03:13:05	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0031.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:17:33	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: AIHU.XYZ Registry Domain ID: D351663834-CNIC Registrar WHOIS Server: whois.resellercamp.com Registrar URL: https://idwebh determining ownership of domain names, (2) not to store or reproduce this data in any way, (3) not to use any high-volume, automated, the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, electronic mail, or by telephone. The c
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cf-ray: 7c5f6036af1541db-EWR
2023-05-12 02:46:49	Open TCP Port	No	SSL Certificate Analyzer	0	0	3	0	None	104.196.30.220:443
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	prr (Net ID: 00:0C:41:CA:76:65)
2023-05-12 02:59:44	Co-Hosted Site - Domain Whois	No	Whois	1	0	2	0	None	Domain Name: GITHUB.COM Registry Domain ID: 1264983250_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.markmonitor.com Registrar URL: ht guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this
2023-05-12 02:49:59	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'capec_id': None, u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObje datablocks 0x1 compression"'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'nam Related', u'origin': u'File/Memory', u'identifier': u'string-3', u'name': u'Found potential URL in binary/memory', u'attck_id_wiki': N u'DNS', u'informative_identifiers': [], u'tactic': u'Command and Control', u'informative_identifiers_count': 1, u'suspicious_identifie
2023-05-12 03:24:19	Account on External Site	No	Account Finder	0	0	8	0	None	Trello (Category: social) https://trello.com/baptistevauthey
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Power IT (Net ID: 00:00:00:05:55:55)
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.221): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:A1:D8:0C)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	DR.KASIM (Net ID: 00:12:CF:44:EA:8F)
2023-05-12 03:24:47	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 02:56:50	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	6	0	None	cf-mitigated: challenge
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	W4B3PQ^00ZT00)>&0//44F6/%&_+(*01 (Net ID: 00:06:66:2A:52:3A)
2023-05-12 03:00:01	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	wr2435@it.jgec.ac.in
2023-05-12 02:53:39	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache_Hits": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "
2023-05-12 03:15:35	Web Content Language	No	Language Detector	0	0	3	0	None	English
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	zhihu (Category: social) https://www.zhihu.com/people/login
2023-05-12 02:59:57	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	support@bigmarker.com

2023-05-12 03:01:12	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.126): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	zhihu (Category: social) https://www.zhihu.com/people/ayhu
2023-05-12 03:00:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.24): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.168): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:8080
2023-05-12 03:09:31	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:00:15	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	webmail.ayhu.xyz
2023-05-12 02:56:25	BGP AS Membership	No	RIPE	0	0	3	0	None	43260
2023-05-12 03:00:36	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	abuse@name.com
2023-05-12 03:18:41	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.109.133:80
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Dash-4302 (Net ID: 00:0A:F5:48:32:08)
2023-05-12 03:11:07	Physical Coordinates	No	OpenStreetMap	91	0	4	0	None	37.780462,-122.390564
2023-05-12 02:53:49	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "X_Ser
2023-05-12 02:46:54	Affiliate - Domain Name	No	DNS Resolver	0	0	3	0	None	netlify.app
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	pannet-24 (Net ID: 00:01:8E:DA:59:C4)
2023-05-12 03:03:51	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	etherum-libs.github.io
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.115): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	default (Net ID: 00:01:24:F2:16:28)
2023-05-12 02:44:12	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cloudwaysapps.com
2023-05-12 03:17:33	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: AYIU.XYZ Registry Domain ID: D304640320-CNIC Registrar WHOIS Server: whois.dynadot.com Registrar URL: http://www.dynadot. automated, electronic processes to obtain data from this service. Abuse of this service is monitored and actions in contravention of t <<<
2023-05-12 03:13:10	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [ebrahemsamir.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:12:54	Physical Location	No	numverify	0	0	3	0	None	Phoenix, US
2023-05-12 02:46:49	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	3	0	None	C=US,ST=California,L=San Francisco,O=Netlify\, Inc,CN=*.netlify.app
2023-05-12 03:00:25	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	curve25519-sha256@libssh.org

2023-05-12 03:08:36	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	185.199.110.154
2023-05-12 02:45:35	Internet Name	No	DNSDumpster	2	0	1	0	None	vscode.battleb0t.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:FD:45:09)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	01a637 (Net ID: 00:02:2D:01:A6:37)
2023-05-12 03:01:04	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.112): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Livejournal (Category: blog) https://login.livejournal.com
2023-05-12 03:00:00	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	banksean@gmail.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BBHWIRELESS (Net ID: 00:00:C5:D7:66:BC)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Tenor (Category: images) https://tenor.com/users/login
2023-05-12 02:44:41	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	74.170.74.34.bc.googleusercontent.com
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-embedder-policy: require-corp
2023-05-12 02:55:11	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"operating_system": {"source": "OSI_TRANSPORT_LAYER", "product": "linux", "part": "o", "uniform_resource_identifier": "cpe:2.3:o:*:li 02T09:30:48.965680163Z"}, "www.tahakaya.tk": {"record_type": "CNAME", "resolved_at": "2022-10-24T16:44:34.447999702Z"}, "www.preview.a 02-05T14:53:26.346732767Z"}, "cpcontacts.altf13.com": {"record_type": "A", "resolved_at": "2023-01-31T12:46:00.853214402Z"}, "bayholme 12T17:18:46.107319847Z"}, "tiktok.stargamepin.com": {"record_type": "A", "resolved_at": "2022-10-05T14:19:22.052159604Z"}, "www.test.b 19T16:39:16.921255240Z"}, "eventkil.com": {"record_type": "A", "resolved_at": "2023-05-04T14:44:33.809431992Z"}, "www.metamimarlik.com
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	WaveLAN Network (Net ID: 00:02:2D:67:07:75)
2023-05-12 03:23:09	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.0:443
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/carti_1.jpg
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 02:53:15	IPv6 Address	No	Mnemonic PassiveDNS	0	0	1	0	None	2606:4700:3030::ac43:a8fc
2023-05-12 03:36:57	Malicious IP Address	Yes	MetaDefender	0	0	2	0	None	webroot.com [87.248.157.102]
2023-05-12 02:53:45	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-12T01:39:10.944Z", "ip": "2606:50c0:8002::153", "location_updated_at": "2023-05-08T10:38:44.903871Z", "au "2023-04-23T09:37:19.694810939Z"}, "liangxiayi.com": {"record_type": "CNAME", "resolved_at": "2023-03-04T14:30:08.595680200Z"}, "mst.b "resolved_at": "2023-03-21T00:19:55.315272389Z"}, "www.shaneporter.dev": {"record_type": "CNAME", "resolved_at": "2023-03-21T00:20:35. "resolved_at": "2023-01-19T12:58:47.712783317Z"}, "stevenbone.dev": {"record_type": "AAAA", "resolved_at": "2023-04-20T02:37:36.462044 04T15:21:01.487028696Z"}, "www.bsaiki.com": {"record_type": "CNAME", "resolved_at": "2023-03-05T13:41:36.534443343Z"}, "www.grantanna.
2023-05-12 02:44:25	IPv6 Address	No	DNS Resolver	15	0	3	0	None	2600:1f18:2489:8202::c8
2023-05-12 03:00:27	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	occipy.recrutement@aftral.com
2023-05-12	WiFi Access	No	Wigle.net	0	0	4	0	None	Maxx Hotel (Net ID: 00:02:2D:1F:6F:03)

03:18:54	Point Nearby								
2023-05-12 03:00:00	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	contact@luckycarrotapp.com
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	34	0	2	0	None	https://pics.battleb0t.xyz/
2023-05-12 02:45:32	Malicious IP Address	Yes	PhishStats	0	1	2	0	None	Phishstats [185.199.109.153]
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:02:53	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 02:44:22	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	3	0	None	GitHub\, Inc.
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.208): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	4	0	None	Lithuania
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	thuis (Net ID: 00:11:6B:12:CA:A6)
2023-05-12 02:44:40	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Netlify
2023-05-12 02:44:40	Affiliate - Internet Name	No	DNS Resolver	1	0	3	0	None	220.30.196.104.bc.googleusercontent.com
2023-05-12 02:54:48	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H0694HWAMG6RHJEVW16FQRHY Date: <REDACTED> Content-Length: 0
2023-05-12 03:18:47	Wikipedia Page Edit	No	Wikipedia Edits	0	0	5	0	None	https://en.wikipedia.org/w/index.php?title=Talk:Baden-W%C3%BCrttemberg_Cooperative_State_University&diff=506884727
2023-05-12 02:55:18	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'Creates mutants', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': "1Ptxg8zYS_SKggPN4iEgvnHyvveLxVvoorCIPrc_1_.woff" has type "Web Open Font Format TrueType length 25360 version 1.1"- [targetUID: N/A]\ [targetUID: 00000000-00003752]\n "analytics_3_.js" has type "ASCII text with very long lines"- [targetUID: N/A]\n "RecoveryStore._A328 gzip\n\n3e6e\n}kw6gSYc;:k;P$1H;n_$x,9Y?O#e0fw\'{Q4vOwcQ`0{s?vL"LxDew^\n_Y7~[Yv]s}M?me3FQ4*Q=!l}lK|(kur1uD|%xh[b\'S1HTOVD+~W>\n^*Q\'Lr1
2023-05-12 02:54:30	Operating System	No	Censys	0	0	3	0	None	Debian Linux 10.2
2023-05-12 02:55:09	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis "Local\\InternetShortcutMutex"\n "IsoScope_968_IESQMMUTEX_0_519"\n "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "{5312EE61-79E3-4A24-BFE1-132B85 [%TEMP%\\~DF438050EC9ECB4A74.TMP]- [targetUID: 00000000-00002408]\n "en-US.4" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\I u'Found an IP/URL artifact that was identified as malicious by at least three reputation engines', u'attck_id_wiki': None, u'threat_le u'technique': u'Application Layer Protocol', u'informative_identifiers': [], u'tactic': u'Command and Control', u'informative_identifi
2023-05-12 03:06:21	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	0	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 02:45:27	Physical Location	No	ipapi.co	0	0	3	0	None	Toronto, Ontario, ON, Canada, CA
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Career.habr (Category: business) https://career.habr.com/login
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.210): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:17	BGP AS Membership	No	Censys	0	0	4	0	None	13335
2023-05-12 03:01:06	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.114): Search Engine Last Activity: 0 days ago Threat Level: 29

2023-05-12 02:51:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'name': u'Found a reference to a known community page', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': N ""6whiskey.com"," (Source: wallet-pre-stable.json, Indicator: "key.com")\n ""99centsubs.com"," (Source: wallet-pre-stable.json, Indica [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Cache\\Cache_Data\\f_0004d4]- [targetUID: 00000000-00007688]\n "wallet-stable.js [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\EdgeCoupons\\coupons_data.db\\000009.log]- [targetUID: 00000000-00004144]\n "000
2023-05-12 02:44:40	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	jQuery
2023-05-12 02:44:22	Physical Location	No	ipstack	0	0	2	0	None	United States
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:46:49	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 03:18:47	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Rotated 180 @ 18}
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	matrix (Net ID: 00:02:2D:03:92:64)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	1620 Guest (Net ID: 00:01:21:30:37:80)
2023-05-12 03:24:51	Country	No	Country Name Extractor	0	0	7	0	None	Spain
2023-05-12 02:44:18	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS RSA SHA256 2020 CA1
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpeedStream (Net ID: 00:01:24:F0:82:16)
2023-05-12 03:03:59	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	rathook.cc
2023-05-12 02:44:28	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-EC32 (Net ID: 00:1D:D1:32:EC:30)
2023-05-12 02:44:14	IPv6 Address	No	DNS Resolver	15	0	1	0	None	2606:50c0:8000::153
2023-05-12 03:09:34	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	212.30.196.104.bc.googleusercontent.com
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	vsco (Category: social) https://vsco.co/ayhu/gallery
2023-05-12 02:54:20	HTTP Headers	No	Web Spider	3	0	2	0	None	{"transfer-encoding": "chunked", "expires": "Thu, 01 Jan 1970 00:00:01 GMT", "server": "cloudflare", "connection": "keep-alive", "cach
2023-05-12 03:00:51	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0000-bigtree.github.io
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=edDiEwhb09qQfIsTtwWW7UDu1MTL3Si52Y7U9Wl3lDs5gxZDQPT8Rjqe
2023-05-12 02:46:49	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	cloudwaysapps.com
2023-05-12 02:54:15	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'"dogeco-in.com"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries DNS ser u'Binary File', u'identifier': u'binary-5', u'name': u'Drops cabinet archive files', u'attck_id_wiki': u'https://attack.mitre.org/tech "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has type "MS Windows icon resource - 1 icon 32x32 32 bits/pixel"- [targetUID: N/A] Pattern match: "https://dogecoin.com/assets/images/doge.webp"\n Pattern match: "MUID39EA38FB0AC96F4105FF2A240B856E28msn.com/1025675741
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-	HTTP	No	Censys	0	0	4	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray

12 02:54:13	Headers								
2023-05-12 03:01:19	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.169): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	NETGEAR (Net ID: 00:09:5B:D9:B2:92)
2023-05-12 03:16:21	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'ENG', u'country_tld': u'.uk', u'ip': u'2a06:98c1:3120::1', u'currency_name': u'Pound', u'currency': u'GBP', u'count
2023-05-12 02:44:19	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	MarvellAP8x (Net ID: 00:01:36:16:7E:FB)
2023-05-12 03:00:58	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	01010101coder.github.io
2023-05-12 03:09:28	Co-Hosted Site	No	SSL Certificate Analyzer	1	0	2	0	None	acilacikveteriner.com
2023-05-12 02:48:58	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'de "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\77EC63BDA7 Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\BISQWXD2.txt]- [targetUID: 00000000-00003696]\n "XYZCPKU1.txt" has type "ASCII text match: "https://hung1001.github.io/assests/images/1.jpg"\n Pattern match: "msdn.microsoft.com/en-us/library/cc722477.aspx"\n Pattern m
2023-05-12 03:08:45	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.212
2023-05-12 02:44:21	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	chacha20-poly1305@openssh.com
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:80
2023-05-12 02:44:22	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:02:6d:eb:8d:63:78:04:f2:b8:5c:db:39:06:ab:26:ed:a9 Signature Algorithm: sha256Wi 05:9A:15:17:EA:9E:B4:58:0D:3C:86:17:2C:C3:17:21: 8A:21:DE:13:02:21:00:93:46:3A:71:BC:50:F5:73:1A: 31:49:1D:77:D8:F0:F3:D0:7E:06:7D:4A:
2023-05-12 03:09:46	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	65.170.74.34.bc.googleusercontent.com
2023-05-12 03:41:52	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["315"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connection": "DISPLAY_UTF8", "Con
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	5	0	None	cloudflare
2023-05-12 02:44:40	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Font Awesome
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	linksys (Net ID: 00:0C:41:A0:89:8A)
2023-05-12 03:09:52	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:25
2023-05-12 02:54:41	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H04595A0C45NR8DMSR5TCKG9 Date: <REDACTED> Content-Length: 0
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.223): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:12:12	Vulnerability - CVE High	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 7.5 Description: The DES and Triple DES ciphers, as used in the TL
2023-05-	Open TCP	No	Censys	0	0	4	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H04DT6EFGA302FBVMKFT2XD1 Date: <REDACTED> Content-Length: 0

12 02:54:23	Port Banner								
2023-05-12 03:01:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.130): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:05:09	Affiliate - Internet Name	No	Cross-Reference	1	1	3	0	None	github.com
2023-05-12 02:50:05	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"185.199.110.153:443"'}, {u'category': u'Gen File', u'identifier': u'binary-37', u'name': u'Drops files inside appdata directory', u'attck_id_wiki': u'https://attack.mitre.org/tec [%TEMP%\\~DFAF54E82161A92B7A.TMP]- [targetUID: 00000000-00003416]\n "Tar6016.tmp" has type "data"- Location: [%TEMP%\\Tar6016.tmp]- [t u'threat_level': 0, u'type': 6, u'description': u'"iexplore.exe" writes a file "%TEMP%\\JavaDeployReg.log"\n "iexplore.exe" writes a f
2023-05-12 02:59:45	SSL Certificate - Raw Data	No	Certificate Transparency	2	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:7b:a3:67:f4:76:b8:d0:86:bd:aa:81:68:7c:78:c6:53:24 Signature Algorithm: sha256Wi 7a:af:32:e2:c8:28:7e:98:41:f2:c7:ab:41:34:02:6f:ca:a4: 77:0e:6b:df:35:1b:69:e8:30:42:43:a2:b1:d9:fd:cb:17:1e: 46:a3:67:c9:5d:ff:94:85:
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	MarvellAP8x (Net ID: 00:01:36:16:7E:FB)
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.175): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.8:8443
2023-05-12 03:09:05	Affiliate - IP Address	No	DNS Look-aside	0	0	3	0	None	165.232.113.76
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	permissions-policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.70): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:12	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	2	0	None	github.io
2023-05-12 02:54:13	Linked URL - External	No	Web Spider	0	0	2	0	None	https://www.discord.com
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.30): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	giters (Category: coding) https://giters.com/ayhu
2023-05-12 03:31:33	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@west.cn
2023-05-12 02:45:14	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 50, u'search_terms': [{u'id': u'host', u'value': u'185.199.111.153'}], u'result': [{u'environment_id': 110, u'job_id': u'64 u'sha256': u'27625e24647d2569a674e3799d36a2008f93eb351cf7cc3ffd05fe808ed74b1c', u'type': None, u'type_short': u'url', u'size': 54}, {u u'verdict': u'malicious', u'submit_name': u'sample.url', u'sha256': u'55f21248b94bc741247d69ef0f5523011eacc847a3c72e4066c45708f38bb7f4 u'verdict': u'no specific threat', u'submit_name': u'sample.url', u'sha256': u'a66876bf5d88b6b1e4cae2ad5fe213c6a5ae169ab90a58bae2c559a None, u'verdict': u'no specific threat', u'submit_name': u'sample.url', u'sha256': u'f29376302ee518c13e0e840829c33da3b9baae9c8efaf8eb9
2023-05-12 02:45:09	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'ON', u'country_tld': u'.ca', u'ip': u'104.21.6.166', u'currency_name': u'Dollar', u'currency': u'CAD', u'country_po
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.162): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:27	Linked URL - Internal	No	URLScan.io	0	0	1	0	None	http://kekw.battleb0t.xyz/jar
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:C4:0E:35)
2023-05-12 02:44:23	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	185.199.109.153:443
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AIRTIES (Net ID: 00:12:BF:30:4A:F9)

2023-05-12 02:56:55	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	tiktok.battleb0t.xyz
2023-05-12 02:58:19	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	{u'count': 27, u'search_terms': [{u'id': u'host', u'value': u'34.74.170.74'}], u'result': [{u'environment_id': 100, u'job_id': u'63a3b u'ee2b3005a67dc45a60a0bc2947c2bfd8584632d9366ff2363f99250eefc18ee6', u'type': None, u'type_short': u'url', u'size': 56}, {u'environmen u'2a7999a7c7b888cb2de97ef77fd40b70d500bd4d0d867d53de57717906f536f9', u'type': None, u'type_short': u'url', u'size': 74}, {u'environmen u'sha256': u'8542bd5b44a22c5a1605485c1ad44055090c9b024aee2513be530a18da580c4a', u'type': None, u'type_short': u'url', u'size': 132}, { u'sha256': u'8d65ee6c3d3e29e2405c7de07ca0dbc6a3c42dfa8e6cfd38e0d683284459d33f', u'type': None, u'type_short': u'url', u'size': 102}, {
2023-05-12 02:50:30	Physical Address	No	GLEIF	2	0	3	0	None	14455 North Hayden Rd, Scottsdale, US-AZ, US, 85260
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet4862 (Net ID: 00:01:36:5B:48:60)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	gunhome1 (Net ID: 00:09:5B:EE:D0:0E)
2023-05-12 03:01:10	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.122): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.15:8443
2023-05-12 03:01:09	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.120): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	BIGO Live (Category: gaming) https://www.bigo.tv/user/login
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Demotywatory (Category: images) https://demotywatory.pl/user/login
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/favicon.png
2023-05-12 03:01:14	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.129): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.9:443
2023-05-12 02:53:20	IP Address	No	Mnemonic PassiveDNS	40	0	2	0	None	165.232.113.85
2023-05-12 02:47:23	Open TCP Port	No	Pulsedive	0	0	2	0	None	185.199.110.153:80
2023-05-12 02:56:51	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	untappd (Category: social) https://untappd.com/user/login/
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SpeedStream (Net ID: 00:01:24:F0:07:E7)
2023-05-12 03:12:51	Physical Location	No	numverify	0	0	3	0	None	Moskva, RU
2023-05-12 02:50:17	Internet Name	No	DNS Resolver	0	0	2	0	None	vscode.battleb0t.xyz
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	linksys-n (Net ID: 00:00:85:EB:4B:63)
2023-05-12 03:03:47	Co-Hosted Site	No	ThreatMiner	2	0	2	0	None	akashpmani.github.io
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<hidden ssid> (Net ID: 00:01:E3:54:E7:17)
2023-05-12 03:03:39	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:03:16	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	cpcontacts.ayhu.xyz

2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	GoDaddy.com, LLC
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	azis (Net ID: 00:06:B1:15:73:DD)
2023-05-12 03:42:54	Affiliate - Domain Whois	No	Whois	0	0	6	0	None	% Restricted rights. % % Terms and Conditions of Use % % The above data may only be used within the scope of technical or % administra
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Tinder (Category: dating) https://tinder.com/@login
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom2888 (Net ID: 00:01:38:85:BD:9E)
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:00:37	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	registrar-abuse@cloudflare.com
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-128@openssh.com
2023-05-12 02:53:02	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	Cloudflare Inc. Cloudflare
2023-05-12 02:59:34	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 02:53:35	Open TCP Port	No	Censys	0	0	2	0	None	185.199.110.153:80
2023-05-12 03:00:59	Malicious Affiliate	Yes	VXVault.net	0	1	3	0	None	VXVault Malicious URL List [cdn-185-199-108-153.github.com] http://vxvault.net/URL_List.php
2023-05-12 02:44:14	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 02:5a:61:0f:58:eb:84:f1:ad:53:ae:03:dc:a9:84:7a Signature Algorithm: ecdsa-with-SHA 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: 1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73 Timestamp : Dec 21 09:03:52.857 2022
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:F1:32:0A)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Ayse (Net ID: 00:14:C1:3A:06:51)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	jia (Net ID: 00:0C:41:75:83:AD)
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	4	0	None	cloudflare
2023-05-12 02:54:19	Linked URL - Internal	No	Web Spider	6	0	2	0	None	https://fluid.battleb0t.xyz/
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:02:2D:35:DF:56)
2023-05-12 03:23:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.15:443
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATT6WEI6hJ (Net ID: D4:B2:7A:43:F2:C2)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	linksys (Net ID: 00:18:39:E0:85:F6)
2023-05-12	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	sni.cloudflaressl.com

03:09:27									
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-ray: 7c5f8c594cb34339-EWR
2023-05-12 02:44:12	Co-Hosted Site	No	SSL Certificate Analyzer	1	0	2	0	None	cloudwaysapps.com
2023-05-12 03:31:32	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	e8887bc7fc7c4eb4aed3e14ba45fe97d.protect@withheldforprivacy.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:00:48:65:F1:BF)
2023-05-12 02:47:24	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 19T17:45:28+00:00', u'filename': u'bounty-69752916457787705'}, {u'url': None, u'submission_id': u'6440116c41936776ee068346', u'created u'cc5742d1f128c439740a56734c0e105f11a62fe6', u'url_analysis': False, u'type': u'PE32 executable (GUI) Intel 80386 (stripped to externa "HKLM\\SOFTWARE\\MICROSOFT\\SYSTEMCERTIFICATES\\CA\\CERTIFICATES\\D559A586669B08F46A30A133F8A9ED3D038E2EA8"; Key: "BLOB")\n "rufus-3.2 3.21.exe" (Path: "HKLM\\SOFTWARE\\POLICIES\\MICROSOFT\\SYSTEMCERTIFICATES\\CA"; Key: "")\n "rufus-3.21.exe" (Path: "HKLM\\SOFTWARE\\PO
2023-05-12 02:44:19	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	GitHub Pages
2023-05-12 03:03:59	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	etherum-libs.github.io
2023-05-12 03:00:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.25): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	Dovecot Dovecot
2023-05-12 03:01:17	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.147): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:51	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.76): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	4	0	None	13335
2023-05-12 03:10:22	Malicious IP Address	Yes	Threat Jammer	0	1	2	0	None	Threat Jammer - Risk score: 40 (MEDIUM) https://threatjammer.com/info/188.114.96.1
2023-05-12 02:44:18	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cross-origin-resource-policy: same-origin
2023-05-12 02:54:20	Web Content	No	Web Spider	0	0	4	0	None	.container{width:100%}.bg-white{--bg-opacity:1;background-color:#fff;background-color:rgba(255,255,255,var(--bg-opacity))}.bg-center{b opacity:1;color:#999;color:rgba(153,153,153,var(--text-opacity))}.text-red-error{--text-opacity:1;color:#bd2426;color:rgba(189,36,38,v opacity));width:2.5rem;height:2.5rem;--transform-translate-x:0;--transform-translate-y:0;--transform-rotate:0;--transform-skew-x:0;--t appearance:button;appearance:button;text-decoration:none;background:none;color:inherit;border:none;padding:0;font:inherit;cursor:point
2023-05-12 02:47:42	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:97:99:5c:60:ac:40:68:f8:b2:de:0a:67:7a:da:b7:d1:16 Signature Algorithm: sha256Wi Extensions: none Signature : ecdsa-with-SHA256 30:44:02:20:28:F1:70:B2:E6:F5:A1:9C:C3:2A:B9:98: B7:CA:DE:46:06:8A:0D:FD:5D:51:62:6A:9E
2023-05-12 02:44:42	Internet Name	No	DNS Resolver	0	0	2	0	None	vscode.battleb0t.xyz
2023-05-12 02:53:42	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 02:58:14	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"68.142.107.4 [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\57C8EDB95DF3F0AD4EE2DC2B8CFD4157]- [targetUID: 00000000-00003000]\n "dberr traffic', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1573', u'threat_level_human': u'informative', u'capec_id': None, u' artifacts related to "34.148.97.127": ...\n\n URL: https://apex-university.netlify.app/ (AV positives: 20/89 scanned on 08/22/2022 00:
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom (Net ID: 00:0C:F6:6E:18:20)
2023-05-12 02:45:52	Physical Coordinates	No	AbstractAPI	0	0	4	0	None	37.751, -97.822

2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:8880
2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	185.199.108.153
2023-05-12 02:59:44	Co-Hosted Site - Domain Whois	No	Whois	2	0	3	0	None	Domain Name: CLOUDFLARESSL.COM Registry Domain ID: 1877752347_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.cloudflare.com Registrar U assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accurac clientupdateprohibited https://icann.org/epp#clientupdateprohibited Registry Registrant ID: Registrant Name: DATA REDACTED Registrant database: 2023-05-12T02:59:44Z <<< For more information on Whois status codes, please visit https://icann.org/epp Cloudflare provides
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpeedStream (Net ID: 00:01:24:F0:B4:05)
2023-05-12 03:09:58	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	logitecgameuser (Net ID: 00:01:8E:15:D4:A7)
2023-05-12 02:53:15	IP Address	No	Mnemonic PassiveDNS	0	0	1	0	None	185.199.111.153
2023-05-12 02:44:52	Raw Data from RIRs	No	CRXcavator	1	0	1	0	None	[{"platform": "Chrome", "version": "1.0", "data": {"entrypoints": {"chrome.cookies.get": {"/tmp/fcnbnbmppjiehikhcaalfjmopkpfaeji_1.0/o "name": "Office Editing for Docs, Sheets & Slides"}, "ohahllgiabjaoigichmmfljhkcfikeof": {"rating": 4.8292074, "users": 1000000, "plat "name": "Save to Google Drive"}, "cjpalhdlnbpafiamejdnhcphjbkeiagm": {"rating": 4.6761365, "users": 10000000, "platform": "", "short_d "Speedtest by Ookla"}, "gpdjojdkbbmdfjfahjcgigfpmkopogic": {"rating": 3.558845, "users": 7000000, "platform": "", "short_description": suite of modules that enhance your Reddit browsing experience", "icon": "https://lh3.googleusercontent.com/0SvxWpFT-d9CLNWqKIjV7_2jOtn
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:2091
2023-05-12 02:45:34	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur deflate\nAccept-Language: en-US,en;q=0.9"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u' "key.com")\n ""order.firehousesubs.com"," (Source: wallet-checkout-eligible-sites-pre-stable.json, Indicator: "ubs.com")\n ""cousinssu u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1083', u'relevance': 1, u'threat_level': 0, u'type': 6, u'de has type "UTF-8 Unicode text with very long lines with no line terminators"- [targetUID: 00000000-00004160]\n "Filtering Rules" has ty
2023-05-12 03:23:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.11:443
2023-05-12 03:04:07	Malicious IP on Same Subnet	Yes	Greensnow	0	0	4	0	None	greensnow.co [207.154.224.0/20] https://blocklist.greensnow.co/greensnow.txt
2023-05-12 03:00:58	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	01100111-01101001-01110100.github.io
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	3	0	None	United Kingdom
2023-05-12 02:45:34	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	route1.mx.cloudflare.net
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	bupet (Net ID: 00:12:BF:37:56:6B)
2023-05-12 02:56:51	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 02:49:36	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur None, u'attck_id': u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"ibm.github.io"\n "idaas.iam.ibm.c type "UTF-8 Unicode text with very long lines"- [targetUID: N/A]\n "datepicker.min_1_.js" has type "ASCII text with very long lines"- (mZRXJRc:Jb^iRH\nw<drI\'Ly\':R]%K\'F([F|8BP9&X/*/+Jbr@6vFOwLsv5dxyo7cp<7,#VBTi#i\\fJ"&"jyy)Xc;51e$dF@fUG3{eUv])zu7uY<pT{A6@z))\\8pkuHX (lWY",Vm51X:r"q)B=>)m3B\n(<XF++wwR7knMgLU)o??o:|B~&vHKuj:U%oy AVsyyu=p1IWfLxK8CKEZdOGLkI>F+TX45K+S\'\nL%WIXo|~4kLnH6mHt", "U:WTejK*UqY
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	3	0	None	Russia
2023-05-12 02:52:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"185.199.108.153:443"\n "104.17.24.14:443"\n standard 1.01 aspect ratio density 1x1 segment length 16 progressive precision 8 640x480 components 3" and extension "jpg"\n "Netflix% u'description': u'"urlblockindex_1_.bin" has type "data"- [targetUID: N/A]\n "fa-solid-900_1_.ttf" has type "TrueType Font data 10 tab [%TEMP%\\~DFC33B8D47F19925CD.TMP]- [targetUID: 00000000-00002616]\n "RecoveryStore._9BCAD631-ED33-11ED-AF92-080027E5BD4D_.dat" has typ
2023-05-12 02:51:20	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relev

									"urlref_httpsdevzorro.github.iodemo1" has type "HTML document ASCII text"- [targetUID: N/A]\n "logo_1_.png" has type "PNG image data 3 icon resource - 1 icon 32x32 32 bits/pixel"- [targetUID: N/A]'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identi
2023-05-12 03:19:47	Account on External Site	No	Account Finder	0	0	2	0	None	Twitter (Category: social) https://twitter.com/patrickpogoda
2023-05-12 02:54:19	Linked URL - Internal	No	Web Spider	4	0	3	0	None	https://fluid.battleb0t.xyz/dat.gui.min.js
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.2): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:38	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:46:43	Malicious IP Address	Yes	MetaDefender	0	1	3	0	None	webroot.com [34.74.170.74]
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATTqYgQBna (Net ID: 18:9C:27:26:52:F0)
2023-05-12 03:16:28	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'HE', u'country_tld': u'.de', u'ip': u'165.232.113.85', u'currency_name': u'Euro', u'currency': u'EUR', u'country_po
2023-05-12 03:21:08	Account on External Site	No	Account Finder	0	0	2	0	None	Twitter (Category: social) https://twitter.com/dawidsulej
2023-05-12 02:50:19	Physical Location	No	ipstack	0	0	3	0	None	United States
2023-05-12 02:44:28	IP Address	No	DNS Resolver	75	0	2	0	None	104.196.30.220
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MatrixEx Guest (Net ID: 00:01:21:26:54:20)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Steam (Category: gaming) https://steamcommunity.com/id/login
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	imgur (Category: images) https://imgur.com/user/ayhu/about
2023-05-12 03:03:31	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Newport (Net ID: 00:18:E7:CB:EB:02)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Pauwels (Net ID: 00:03:6D:F4:D7:4E)
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:8880
2023-05-12 03:24:19	Account on External Site	No	Account Finder	0	0	8	0	None	Pinterest (Category: social) https://www.pinterest.com/baptistevauthey/
2023-05-12 03:00:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-128@openssh.com
2023-05-12 03:03:25	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	permissions-policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	YouTube User2 (Category: video) https://www.youtube.com/@ayhu
2023-05-12 02:44:20	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 02:56:44	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "IsoScope_b30_IESQMMUTEX_0_519"\n "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "Local\\VERMGMTBlockListFileMutex"\n "Local\\URLBLOCK_FIL 1\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GET /main.94ce4fbb3fdb7e2758a9e018cc35e9c14e00b838.js HTTP/1.1\nAccept: app

									/favicon.ico HTTP/1.1\nAccept: */*\nAccept-Encoding: gzip, deflate\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) lik lor.instructure.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "user-agent: ")\n "GET /api/licenses HTTP/1.1\nAccept: */*\nContent-T
2023-05-12 03:08:52	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.126
2023-05-12 03:28:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.144:8443
2023-05-12 02:55:27	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur Possible RC4 Encryption', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1486', u'threat_level_human': u'informative', u'cap [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\load_statistics.db-wal]- [targetUID: 00000000-00007544]\n "2e8e03b2-b8a9-4702-ad terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\7406036f-2f9e-4939-8d5b-442a52cfa1c5.tmp]- [targetUID: 00000000-0 "\',\'QtjLP\',\'KDqei\',\'vXqYi\',\'GOqYh\',\'gISTU\',\'n()\\x20\',\'roJBb\',\'FXzcw\',\'__pro\',\'warn\',\'PukFk\',\'EAlzP\',\'YvMmB\
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	curve25519-sha256@libssh.org
2023-05-12 02:58:53	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\Local\\VERMGMTBlockListFileMutex"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_FILEMAPSWITCH_ Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\6BADA8974A10C4BD62CC921D13E43B18_28DEA62A0AE77228DD387E155AD0BA2 "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\A16C6C16D94F76E0808C087DFC657D99_298E60D5E528EEA70E86195 Keep-Alive\nAccept: */*\nUser-Agent: Microsoft-CryptoAPI/6.1\nHost: r3.o.lencr.org"\n Heuristic match: "GET /MFMwUTBPME0wSzAJBgUrDgMCG
2023-05-12 03:03:18	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12 03:33:37	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	IDATx A`qRWQ @Qh9' WYW`Q 6:E<0s qt2!X O"Np /Z9l6 23W4R p$ke'V sZSjUQ S\-up iTb.T IDAT? ZYjy9 k-<Z6 DRZ1s NLgiN 7jI\k q8cH$ cG$C: 70/1c
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ZyXEL-aslan (Net ID: 00:02:CF:83:7F:15)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:BB:17:A7)
2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	GitHub (Category: coding) https://github.com/Altpapier
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	babacan (Net ID: 00:14:C1:20:84:74)
2023-05-12 03:10:11	Malicious IP on Same Subnet	Yes	VoIPBL OpenPBX IPs	0	0	3	0	None	VOIPBL Publicly Accessible PBX List [104.21.0.0/20] http://www.voipbl.org/update
2023-05-12 03:01:32	Web Server	No	Tool - WhatWeb	0	0	3	0	None	cloudflare
2023-05-12 02:56:54	IP Address	No	DNS Resolver	0	0	2	0	None	104.21.6.166
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	GitLab - GitLab Inc. is an open-core company that operates GitLab, a DevOps software package which can develop, secure, and operate so
2023-05-12 03:08:53	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.67
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Chyoa (Category: XXXPORNXXX) https://chyoa.com/user/login
2023-05-12 02:44:23	Internet Name	No	DNS Resolver	0	0	2	0	None	www.battleb0t.xyz
2023-05-12 02:45:01	Physical Location	No	ipapi.co	0	0	2	0	None	San Francisco, California, CA, United States, US
2023-05-12 03:03:51	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	eliaspinheironeto.github.io
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet (Net ID: 00:01:36:29:7A:3C)
2023-05-12 03:00:58	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	010916hao.github.io

2023-05-12 02:54:16	HTTP Headers	No	Web Spider	6	0	4	0	None	{"nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "alt-svc": "h3=\":443\"; ma=86400, h3-29=\":443\"; ma=
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	XFINITY (Net ID: 00:0D:67:8C:21:A9)
2023-05-12 02:54:30	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Connection": "DISPLAY_UTF8", "Etag": "DISPLAY_UTF8", "Content_Type":
2023-05-12 03:43:45	Malicious IP on Same Subnet	Yes	CleanTalk Spam List	0	0	4	0	None	CleanTalk Spam List [45.131.109.0/24] https://iplists.firehol.org/files/cleantalk_7d.ipset
2023-05-12 02:52:59	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	Fastly CDN Fastly
2023-05-12 02:53:32	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "Via": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary":
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SBB (Net ID: 00:02:CF:A7:63:9D)
2023-05-12 02:54:23	Linked URL - Internal	No	Web Spider	5	0	4	0	None	https://www.ayhu.xyz/?__cf_chl_f_tk=eArohGzIRNubxh3D6IFMRkkS6OUaNS008kBgg4I5pUY-1683860063-0-gaNycGzNCiU
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-tikaro.github.io
2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	185.199.110.153
2023-05-12 03:03:28	Co-Hosted Site - Domain Name	No	DNS Resolver	2	0	3	0	None	001viet.com
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	taylor (Net ID: 00:06:25:9A:21:94)
2023-05-12 02:46:50	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	3	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/carti_3.JPG
2023-05-12 03:01:17	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.144): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	NGMH (Net ID: 00:09:5B:B3:C8:73)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	roxie (Net ID: 00:02:6F:E5:4F:4C)
2023-05-12 02:44:58	Physical Location	No	ipapi.co	0	0	2	0	None	San Francisco, California, CA, United States, US
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet24CE (Net ID: 00:01:36:59:24:CC)
2023-05-12 02:51:59	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'capec_id': None, u'attck_id': u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"acmephp.github.io"\n d776-472f-a0ff-e1416b8b2e3a}.ico"\n "iexplore.exe" writes file "c:\\users\\%osuser%\\appdata\\local\\microsoft\\internet explorer\\rec "c:\\users\\%osuser%\\appdata\\local\\temp\\~dfdcbc4d5dbdf1df3e.tmp"\n "iexplore.exe" reads file "c:\\users\\%osuser%\\appdata\\local\ "_CB6DD7E9-ED80-11ED-B43F-080027944A9E_.dat" has type "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.242): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	shithead (Net ID: 00:0C:41:43:78:70)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SINGER (Net ID: 00:00:71:90:09:29)
2023-05-12 02:45:34	Name Server (DNS NS Records)	No	DNS Raw Records	0	0	1	0	None	skip.ns.cloudflare.com

2023-05-12 03:09:30	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:45:34	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	daphne.ns.cloudflare.com
2023-05-12 03:13:05	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [006blog.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:01:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.246): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	union church (Net ID: 00:00:C5:FE:88:4C)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	niudnav (Net ID: 00:0C:F6:63:91:4C)
2023-05-12 02:54:00	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Persistent_Auth": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Host": "DISPLAY_UTF8", "Server":
2023-05-12 03:03:55	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	etherum-libs.github.io
2023-05-12 03:25:08	Internet Name	No	DNS Brute-forcer	1	0	1	0	None	vm.battleb0t.xyz
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	eminent_g_router (Net ID: 00:14:5C:85:F6:6A)
2023-05-12 03:33:47	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	"Exif sgssso <Qwm7 >6x.O x>t7? g$sy? .b97< /Ggy! l/5-o ggs43Z x.o.n> NNEsz gmuss Mswy5 dIys6 >t6w6 03Ryr\G a>0xM g_on8 9!6sBsmms ?r:\t
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 02:55:11	Netblock Membership	No	Censys	4	0	2	0	None	87.248.157.0/24
2023-05-12 02:54:41	Netblock Membership	No	Censys	0	0	3	0	None	104.196.16.0/20
2023-05-12 03:09:42	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	117.97.148.34.bc.googleusercontent.com
2023-05-12 03:24:33	Malicious Affiliate	Yes	VXVault.net	0	1	4	0	None	VXVault Malicious URL List [cdn-185-199-110-154.github.com] http://vxvault.net/URL_List.php
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CATYLN (Net ID: 00:01:38:86:06:1F)
2023-05-12 02:53:22	IPv6 Address	No	Mnemonic PassiveDNS	0	0	2	0	None	2606:4700:3037::6815:470e
2023-05-12 02:44:31	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2600:1f18:2489:8202::c8
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	redskins33 (Net ID: 00:09:5B:85:B7:B6)
2023-05-12 02:45:40	Physical Location	No	AbstractAPI	1	0	2	0	None	San Francisco (South Beach), California, 94107, United States, North America
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.250): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.37): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:33	Web Server	No	Tool - WhatWeb	0	0	2	0	None	cloudflare
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://fluid.battleb0t.xyz

2023-05-12 02:45:57	Raw Data from RIRs	No	AbstractAPI	0	0	4	0	None	{u'city': u'Ashburn', u'security': {u'is_vpn': False}, u'city_geoname_id': 4744870, u'region_geoname_id': 6254928, u'country': u'Unite
2023-05-12 03:08:48	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.230
2023-05-12 03:32:08	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.5:8080
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:74:99:A4:64)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Apple Network 3ac606 (Net ID: 00:02:2D:21:9A:18)
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:2083
2023-05-12 03:00:51	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	000000014286.github.io
2023-05-12 03:03:47	Co-Hosted Site	No	ThreatMiner	1	0	2	0	None	scoop.sh
2023-05-12 03:01:03	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.108): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	HubPages (Category: blog) https://hubpages.com/@login
2023-05-12 02:53:07	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.111.154:443
2023-05-12 02:53:59	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'informative', u'capec_id': None, u'attck_id': u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"kurt info"- [targetUID: N/A]\n "LHKBGYS9.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\LHKBGYS9.txt]- [tar u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relev u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'suspicious_identifiers': [], u'attck_id': u'T1105', u'malicious_iden
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.180): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:38	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	410HowardStudios (Net ID: 00:02:2D:00:25:63)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	hackster (Category: coding) https://www.hackster.io/login
2023-05-12 03:09:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	nocwap (Net ID: 00:04:5A:CC:3F:27)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	x-proxy-cache: MISS
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.80): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:13:04	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [001wwang.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:00:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	aes256-gcm@openssh.com
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-51D2 (Net ID: 00:1D:D1:0A:51:D0)
2023-05-12 02:53:42	Open TCP Port	No	Censys	0	0	2	0	None	185.199.109.153:443

2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:02:2D:03:B4:A0)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pgi50 (Net ID: 00:01:21:10:7A:20)
2023-05-12 02:46:34	Internet Name	No	VirusTotal	0	0	2	0	None	funny.battleb0t.xyz
2023-05-12 02:54:44	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["0"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATT9wHk9D5 (Net ID: D4:B2:7A:4E:26:D2)
2023-05-12 03:27:54	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.138:8443
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:F4:F3:43)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	kristin (Net ID: 00:0C:41:84:68:1E)
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:2053
2023-05-12 03:03:36	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.179): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	54d382 (Net ID: F4:6B:EF:54:D3:86)
2023-05-12 03:22:54	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.1:443
2023-05-12 03:16:12	Similar Domain	Yes	Tool - DNSTwist	0	0	1	0	None	battlebot.xyz
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-embedder-policy: require-corp
2023-05-12 03:13:10	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [01100111-01101001-01110100.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:47:06	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\Local\\!BrowserEmulation!SharedMemory!Mutex"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\VERMGMTBlock dropped file "Tar2FBD.tmp" as clean (type is "data")'}, {u'category': u'Pattern Matching', u'origin': u'YARA Signature', u'identifier' "5fc071f4e509f3bc3acd619d_Check%20icon_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUID: N/A]\n "5ff61e34886f01f4ab67 https://preventor.com/solutions/preventor-namesAccept-Language: en-USUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) li
2023-05-12 02:46:32	Netblock Membership	No	RIPE	2	0	3	0	None	172.67.160.0/20
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Picsart (Category: art) https://picsart.com/u/Altpapier
2023-05-12 02:52:21	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'Network Traffic', u'identifier': u'network-0', u'name': u'Contacts domains', u'attck_id_wiki': u'https://attack.mitre.org/techniques interlaced" and extension "png"\n "bb_1_.jpg" has type "JPEG image data JFIF standard 1.01 aspect ratio density 1x1 segment length 16 "c:\\users\\%osuser%\\appdata\\local\\microsoft\\internet explorer\\imagestore\\3mt7jhv\\imagestore.dat"\n "iexplore.exe" reads file " 00003440]\n "~DF432D2BE44D8F536C.TMP" has type "data"- Location: [%TEMP%\\~DF432D2BE44D8F536C.TMP]- [targetUID: 00000000-00003440]\n "
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	hhonors (Net ID: 00:01:03:86:22:27)
2023-05-12 02:54:27	HTTP Headers	No	Censys	0	0	4	0	None	{"Date": ["<REDACTED>"], "_encoding": {"Date": "DISPLAY_UTF8", "Content_Length": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "S
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Best_Western_27 (Net ID: 00:00:C5:D7:5F:74)

2023-05-12 03:01:51	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.110.154:443
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 02:44:27	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Open Graph
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	CAUCESS (Net ID: 00:02:44:A8:10:34)
2023-05-12 03:19:11	Human Name	No	Venmo	2	0	6	0	None	baptiste vauthey
2023-05-12 02:55:11	BGP AS Membership	No	Censys	0	0	2	0	None	43260
2023-05-12 02:54:23	Linked URL - Internal	No	Web Spider	0	0	5	0	None	https://www.ayhu.xyz/?__cf_chl_f_tk=KlbaNJzGw77sVIKMODL.ADC4FpZJphIcqM52Ij1fyiw-1683860063-0-gaNycGzNChA
2023-05-12 03:00:58	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.98): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:20:27	Account on External Site	No	Account Finder	0	0	2	0	None	PinkBike (Category: hobby) https://www.pinkbike.com/u/patrick.pogoda/
2023-05-12 03:11:13	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	2	3	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 03:00:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.9): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	NazifBey (Net ID: 00:14:C1:18:2D:AC)
2023-05-12 03:35:51	Malicious Co-Hosted Site	Yes	OpenDNS	0	1	3	0	None	Blocked by OpenDNS [00ffcc.cn]
2023-05-12 03:12:15	Affiliate - Domain Whois	No	Whois	4	0	6	0	None	Domain Name: TELLERIA.COM Registry Domain ID: 1147715746_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.gandi.net Registrar URL: http:/ facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilatio PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin P
2023-05-12 02:45:20	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'network-1', u'name': u'Contacts server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'in Scalable Vector Graphics image")\n Antivirus vendors marked dropped file "menu_1_.svg" as clean (type is "SVG Scalable Vector Graphics image data 88 x 31 8-bit/color RGBA non-interlaced" and extension "png"\n "poweredby_mediawiki_88x31_1_.png" has type "PNG image data "SVG Scalable Vector Graphics image"- [targetUID: N/A]\n "bullet-icon_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUI
2023-05-12 02:44:14	SSL Certificate Host Mismatch	Yes	SSL Certificate Analyzer	0	0	2	0	None	*.netlify.app, netlify.app
2023-05-12 02:53:22	IP Address	No	Mnemonic PassiveDNS	0	0	2	0	None	104.21.71.14
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	6dgs-guest (Net ID: 00:06:B1:28:66:5F)
2023-05-12 03:37:29	Physical Location	No	MetaDefender	0	0	3	0	None	Frankfurt Am Main, Germany
2023-05-12 02:56:30	Physical Location	No	Fraudguard	0	0	3	0	None	Germany, Hesse, Frankfurt am Main
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	referrer-policy: strict-origin-when-cross-origin
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.102): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	5	0	None	cloudflare
2023-05-12 03:18:59	WiFi Access	No	Wigle.net	0	0	5	0	None	Private (Net ID: 00:06:B1:20:D3:D2)

	Point Nearby								
2023-05-12 03:00:23	Blacklisted IP Address	Yes	Honeypot Checker	0	1	2	0	None	Honeypotproject (188.114.97.1): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Microsoft websites
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	5247 4331 (Net ID: 00:00:C5:AA:78:1C)
2023-05-12 03:17:44	Account on External Site	No	Account Finder	0	0	1	0	None	GitLab (Category: coding) https://gitlab.com/ BattleB0t
2023-05-12 03:07:57	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	permissions-policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope
2023-05-12 02:55:25	Username	No	Social Network Identifier	0	0	4	0	None	Altpapier
2023-05-12 03:13:02	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00-duino.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-mitigated: challenge
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomDB2CA4 (Net ID: 00:0C:F6:DB:2C:A4)
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Duolingo (Category: hobby) https://www.duolingo.com/profile/ayshoo
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ASI (Net ID: 00:02:6F:51:19:D9)
2023-05-12 03:00:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	fernando.r@alliedglobal.com
2023-05-12 03:22:52	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.1:8080
2023-05-12 02:46:16	Affiliate Description - Abstract	No	DuckDuckGo	0	0	3	0	None	GitHub, Inc. is an Internet hosting service for software development and version control using Git. It provides the distributed versio
2023-05-12 03:09:01	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.98
2023-05-12 03:03:42	Internet Name	No	DNS Resolver	0	0	3	0	None	fluid.battleb0t.xyz
2023-05-12 03:38:38	Blacklisted Affiliate IP Address	Yes	UCEPROTECT	0	0	4	0	None	UCEPROTECT - Level 2 (some false positives) (207.154.228.167)
2023-05-12 02:50:23	Blacklisted IP Address	Yes	Honeypot Checker	0	1	2	0	None	Honeypotproject (172.67.135.9): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:29	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "IsoScope_948_IE_EarlyTabStart_0x96c_Mutex"\n "Local\\VERMGMTBlockListFileMutex"\n "Local\\ZonesLockedCacheCounterMutex"\n "UpdatingNe long lines with no line terminators"- [targetUID: N/A]\n "~DFFAAD4CD900CEC332.TMP" has type "data"- Location: [%TEMP%\\~DFFAAD4CD900CE "6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptne v=7434068eaf17e8601e02a866de2e7a8e","sizes":"48x48","type":"image/png"},{"src":"icons/icon-72x72.png?v=7434068eaf17e8601e02a866de2e7a8
2023-05-12 02:56:51	Internet Name	No	DNS Resolver	0	0	3	0	None	www.battleb0t.xyz
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Ten Forward 5 (Net ID: 00:01:9F:34:7C:14)

2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Curiouscat (Category: social) https://curiouscat.live/Altpapier
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	themeforest (Category: art) https://themeforest.net/user/login
2023-05-12 02:54:13	Linked URL - External	No	Web Spider	1	0	2	0	None	https://github.com/BattleB0t
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	TEO Network Enterprise (Net ID: 00:01:24:F0:B7:E1)
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	MCUUID (Minecraft) (Category: gaming) https://mcuuid.net/?q=Battleb0t
2023-05-12 02:54:21	Web Content	No	Web Spider	0	0	5	0	None	.container{width:100%}.bg-white{--bg-opacity:1;background-color:#fff;background-color:rgba(255,255,255,var(--bg-opacity))}.bg-center{b opacity:1;color:#999;color:rgba(153,153,153,var(--text-opacity))}.text-red-error{--text-opacity:1;color:#bd2426;color:rgba(189,36,38,v opacity));width:2.5rem;height:2.5rem;--transform-translate-x:0;--transform-translate-y:0;--transform-rotate:0;--transform-skew-x:0;--t appearance:button;appearance:button;text-decoration:none;background:none;color:inherit;border:none;padding:0;font:inherit;cursor:point
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	My Passport (2.4 GHz) - 07E0F4 (Net ID: 00:00:C0:07:E0:F4)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Discogs (Category: music) https://www.discogs.com/user/login
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet (Net ID: 00:01:36:2D:B3:F8)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	fansly (Category: XXXPORNXXX) https://fansly.com/ayhu/posts
2023-05-12 03:23:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.4:80
2023-05-12 03:43:57	URL (Form)	No	Page Information	0	0	3	0	None	http://ayhu.xyz/
2023-05-12 02:54:17	Raw Data from RIRs	No	Censys	0	0	4	0	None	{"last_updated_at": "2023-05-11T22:57:58.234Z", "ip": "2606:4700:3037::6815:470e", "location_updated_at": "2023-05-08T07:47:25.051265Z 04T16:44:01.264807017Z"}, "clean.vipe.us": {"record_type": "AAAA", "resolved_at": "2023-05-01T03:09:37.177595997Z"}, "maycijackmo.gq": 30T19:28:04.759393053Z"}, "routsaygeehekdest.ga": {"record_type": "AAAA", "resolved_at": "2023-04-14T02:12:59.832119313Z"}, "www.faras "resolved_at": "2023-05-03T17:22:24.190764207Z"}, "renalfa.vipe.us": {"record_type": "AAAA", "resolved_at": "2023-05-08T22:47:46.47918 05T20:38:50.973706563Z"}, "gusteiplexmola.tk": {"record_type": "AAAA", "resolved_at": "2023-03-27T05:18:03.996467271Z"}, "diageherpost
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	a-zoom (Net ID: 00:01:38:D4:87:A3)
2023-05-12 02:57:26	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\URLBLOCK_FILEMAPSWITCH_MUTEX_3828"\n "{5312EE61-79E3-4A24-BFE1-132B85B23C3A}"\n "Local\\ZonesCacheCounterMutex"\n "Local\\!Bro [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\51C778D1B3D7448EC0DA4AE3D4980DFC_A397D18A0CD6D90D198AF5B25C97EE7F]- [targe "WZONAU8G.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\WZONAU8G.txt]- [targetUID: 00000000-00003252] R;e"&s52$QK\'Tvw_ljOH,="PF6AJ`<0X}pK2WF/1|k\n5_A|:OG|bO}>)rhh5&SkD/7UrV,,>7RrJ7q=eUS UpU[Fgly%5e_oI[@Kow\'nZg}__/;iPBx 7yT|TGBM\'rri\
2023-05-12 02:46:54	IP Address	No	DNS Resolver	0	0	2	0	None	172.67.168.252
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet (Net ID: 00:01:36:33:E6:06)
2023-05-12 03:00:49	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.68): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:59:06	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'network-0', u'name': u'Contacts domains', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_ type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\KPRDW9OF.txt]- [targetUID: 00000000-00003028]\n "device.min_1_.j E1416B8B2E3A_.ico" has type "MS Windows icon resource - 1 icon 32x32 32 bits/pixel"- [targetUID: N/A]\n "7423F88C7F265F0DEFC08EA88C3BD age=31536000\nAccept-Ranges: bytes\nDate: Fri\n 19 Aug 2022 08:38:09 GMT\nAge: 875904\nX-Served-By: cache-iad-kjyo7100064-IAD\n cache-
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sternmismuschel (Net ID: 00:01:E3:C9:B9:3F)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Juggernaut (Net ID: 00:0C:41:D7:E4:AF)

2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	referrer-policy: strict-origin-when-cross-origin
2023-05-12 02:58:10	SSL Certificate - Raw Data	No	Certificate Transparency	7	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:89:7c:23:d8:89:20:d1:c5:b3:ae:30:91:44:3a:23:81:b8 Signature Algorithm: sha256Wi B7:3E:FB:24:DF:9C:4D:BA:75:F2:39:C5:BA:58:F4:6C: 5D:FC:42:CF:7A:9F:35:C4:9E:1D:09:81:25:ED:B4:99 Timestamp : Dec 14 04:53:54.573 2022
2023-05-12 02:44:59	Physical Location	No	ipapi.co	0	0	2	0	None	San Francisco, California, CA, United States, US
2023-05-12 03:41:52	Software Used	Yes	Censys	0	0	3	0	None	microsoft windows
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	W4B3P<]00D^20&51%1C35&6H'%***%Ph (Net ID: 00:06:66:2A:52:5E)
2023-05-12 03:00:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.2): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	3	0	None	cloudflare
2023-05-12 02:48:54	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"23.235.199.120:80"\n "23.235.199.120:443"\n "142.250.191.42:443"\n (Indicator: "paypal")\n "if(nextField){nextField.focus();if(event&&event.preventDefault){event.preventDefault();}else{return false;}}} [],nonGoogleScripts:["nonGooglePixels"],nonGoogleIframes:["nonGooglePixels"]},us={cl:["ecl"],customPixels:["customScripts","html"]," (gtm-yt-inspected-"]),Uy=["www.youtube.com","www.youtube-nocookie.com"],Vy,Wy=!1;" (Indicator: "youtube")\n "m=!!a.get("fixMissingApi")
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	RumbleUser (Category: political) https://rumble.com/user/login
2023-05-12 03:13:06	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [007us.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-oo.github.io
2023-05-12 02:50:15	Internet Name	No	DNS Resolver	0	0	2	0	None	battleb0t.xyz
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Microsoft websites
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	x-proxy-cache: MISS
2023-05-12 03:00:26	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	chacha20-poly1305@openssh.com
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.142): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:53:52	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "Via": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary":
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Alparslan (Net ID: 00:08:5C:FF:1B:97)
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:55:05	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-12T00:44:58.534Z", "ip": "188.114.97.1", "location_updated_at": "2023-04-29T21:54:15.361063Z", "autonomou 02T12:04:18.005028285Z"}, "ftp.baharelm.ir": {"record_type": "A", "resolved_at": "2023-01-11T15:16:43.150193914Z"}, "dl.jamalghamari.c "resolved_at": "2023-05-07T20:05:01.309575808Z"}, "centrumpedikury.sk": {"record_type": "A", "resolved_at": "2022-10-02T16:33:19.85101 {"record_type": "A", "resolved_at": "2022-10-18T13:44:12.923874025Z"}, "www.wolny.poker": {"record_type": "A", "resolved_at": "2022-10 "GET", "uri": "http://188.114.97.1/"}, "response": {"body": "<!DOCTYPE html>\n<!--[if lt IE 7]> <html class=\"no-js ie6 oldie\" lang=\
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Bikemap (Category: health) https://www.bikemap.net/en/u/login/routes/created/
2023-05-12 03:03:27	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco

2023-05-12 02:56:51	Internet Name	No	DNS Resolver	0	0	3	0	None	nwapi2.battleb0t.xyz
2023-05-12 03:13:10	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [akashpmani.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:03:20	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:54:13	Web Content Type	No	Web Spider	0	0	1	0	None	text/html;charset=utf-8
2023-05-12 03:09:59	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	amcodev.me
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-ray: 7c5f6041aa868cdc-EWR
2023-05-12 03:23:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.8:8080
2023-05-12 03:12:16	Affiliate - Domain Whois	No	Whois	0	0	6	0	None	% Copyright (c)2023 by NIC.AT (1) % % Restricted rights. % % Except for agreed Internet operational purposes, no part of this % inform
2023-05-12 03:22:52	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.1:80
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	JDKolgen (Net ID: 00:0C:F6:CC:40:31)
2023-05-12 02:53:32	Netblock Membership	No	Censys	0	0	2	0	None	185.199.111.0/24
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00arthur00.github.io
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	1	4	0	None	GitHub.com
2023-05-12 02:45:56	Physical Coordinates	No	AbstractAPI	0	0	4	0	None	39.0469, -77.4903
2023-05-12 02:57:42	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur {u'category': u'Unusual Characteristics', u'origin': u'Binary File', u'identifier': u'binary-33', u'name': u'Drops executable files in CRLF line terminators"- Location: [%TEMP%\\6844_2131939810\\shopping_iframe_driver.js]- [targetUID: 00000000-00006844]\n "96de8815-40a 00006844]'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifier': u'string-3', u'name': u'Found potential URL i u'binary-1', u'name': u'Drops executable files', u'attck_id_wiki': None, u'threat_level_human': u'suspicious', u'capec_id': None, u'at
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.182): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:21	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	Reddit (Category: social) https://www.reddit.com/user/battleb0t
2023-05-12 02:54:13	Web Content Type	No	Web Spider	0	0	4	0	None	text/html;charset=utf-8
2023-05-12 03:00:51	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	000.lt
2023-05-12 03:35:41	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'LI', u'country_tld': u'.nl', u'ip': u'45.131.109.53', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.225): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Eminent_5G (Net ID: 00:14:5C:91:C2:74)
2023-05-12 03:00:51	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.77): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/withat_4.jpg

2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Airport ST FRA (Net ID: 00:02:2D:07:C4:ED)
2023-05-12 02:45:25	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'General', u'origin': u'Network Traffic', u'identifier': u'network-1', u'name': u'Contacts server', u'attck_id_wiki': u'https://attac interlaced" and extension "png"'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u type "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "RecoveryStore._4D04579F-EE71-11ED-B780-080027 u'name': u'Found potential URL in binary/memory', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_level_human
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	6	0	None	United States
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Vero (Category: art) https://vero.co/login
2023-05-12 02:56:52	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	wattpad (Category: social) https://www.wattpad.com/user/ayshoo
2023-05-12 03:11:17	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'Amsterdam', u'security': {u'is_vpn': False}, u'city_geoname_id': 2759794, u'region_geoname_id': 2749879, u'country': u'Net
2023-05-12 03:11:26	Physical Location	No	AbstractAPI	0	0	3	0	None	Arizona, United States
2023-05-12 02:45:34	Raw DNS Records	No	DNS Raw Records	0	0	1	0	None	battleb0t.xyz. 300 IN TXT "v=spf1 include:_spf.mx.cloudflare.net ~all"
2023-05-12 02:54:13	HTTP Status Code	No	Web Spider	0	1	1	0	None	403
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.39): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:41	HTTP Headers	No	Censys	0	0	3	0	None	{"Date": ["<REDACTED>"], "_encoding": {"Date": "DISPLAY_UTF8", "Content_Length": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "S
2023-05-12 03:33:44	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	!2222222222222222222222222222222222222222222222222 sH GN t5ad C'Y2z OB:`S pF>oj OQTeuy YYK`s gnqV N9FX6 EQY66 1pO'94 pj'R7pz` 0Kdes x
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.94): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:40	Physical Coordinates	No	AbstractAPI	94	0	2	0	None	34.0544, -118.244
2023-05-12 02:44:04	Raw Data from RIRs	No	Tool - WAFW00F	0	0	1	0	None	[{"url": "https://battleb0t.xyz", "firewall": "Fastly", "detected": true, "manufacturer": "Fastly CDN"}, {"url": "https://battleb0t.xy
2023-05-12 02:44:40	Affiliate - Domain Name	No	DNS Resolver	2	0	4	0	None	googleusercontent.com
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.234): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.126): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	ow.ly (Category: social) http://ow.ly/user/Altpapier
2023-05-12 02:54:15	Linked URL - External	No	Web Spider	2	0	3	0	None	https://github.com/Altpapier/SkyHelperAPI/issues
2023-05-12 03:24:21	HTTP Headers	No	Web Spider	10	0	2	0	None	{"content-encoding": "gzip", "nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "referrer-policy": "same-o
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	UECTouch (Net ID: 00:18:0A:7A:D6:B0)
2023-05-12 02:54:17	Netblock IPv6 Membership	No	Censys	0	0	4	0	None	2606:4700:3037::/48
2023-05-12	Co-Hosted Site -	No	DNS Resolver	0	0	3	0	None	github.io

03:03:29	Domain Name								
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AG-EA (Net ID: 00:13:33:91:70:BC)
2023-05-12 03:09:55	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.122): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	My Passport (2.4 GHz) - 0778A5 (Net ID: 00:00:C0:07:78:A5)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:FA:75:55)
2023-05-12 02:45:31	Malicious IP Address	Yes	PhishStats	0	1	2	0	None	Phishstats [185.199.110.153]
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:2087
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pgi50 (Net ID: 00:01:21:10:7A:10)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	XPONENT (Net ID: 00:02:6F:C6:43:88)
2023-05-12 03:13:10	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [01101101.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:50:15	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relevance': 3, u'threat_level': 0, u'type': 8, u'description': u'"widevine lines with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\0af395f2-e575-4794-b38d-549209b43991.tmp]- [ta u'origin': u'External System', u'identifier': u'avtest-1', u'name': u'Sample was identified as clean by Antivirus engines', u'attck_id 8, u'description': u'"widevinecdm.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\\(
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ThermiCam2Production TRC (Net ID: 00:05:FE:C6:35:F1)
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:43:29	Country	No	Country Name Extractor	0	0	7	0	None	Austria
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	1	5	0	None	Netlify
2023-05-12 03:23:35	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.13:443
2023-05-12 03:18:49	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Horizontal (normal) @ 18}
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+74955801111
2023-05-12 03:36:07	Open UDP Port	No	Tool - nbtscan	1	0	3	0	None	45.131.109.53:137
2023-05-12 02:49:41	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [185.199.111.153] https://www.virustotal.com/en/ip-address/185.199.111.153/information/
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	x-github-request-id: F620:0A4B:1087FED:17E0EF4:645DA7F4
2023-05-12 02:57:21	Internet Name	No	Certificate Transparency	2	0	1	0	None	panel.battleb0t.xyz
2023-05-12 03:16:25	Username	No	Account Finder	6	0	1	0	None	dawidsulej

2023-05-12 03:00:48	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.65): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/carti_2.PNG
2023-05-12 03:01:06	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.115): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	USR9108 (Net ID: 00:14:C1:10:CB:2C)
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:995
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	2	0	3	0	None	https://pics.battleb0t.xyz/images/random_3.jpg
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	The Batcave (Net ID: 00:11:32:7C:A3:89)
2023-05-12 02:52:54	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "183.181.98.34:443"\n "69.16.175.10:443"\n "142.251.46.234:443"\n "185.199.108.153:443"\n "142.250.189.195:443"\n "20.125.62.241:443"' nocookie.com"],bz,cz=!1;" (Indicator: "dir "; File: "js_1_.js")\n Found string "function mz(a,b){var c=this;return b}mz.M="internal.en 05_1_.png" has type "RIFF (little-endian) data Web/P image" and extension "png"\n "top-feature-img-01-sp_1_.png" has type "RIFF (littl 2000/XP setup 63843 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%TEMP%\\Cab134B.tmp]- [t
2023-05-12 02:44:21	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:4d:72:d7:7c:dd:a7:02:dd:5a:67:f2:a2:3b:bd:d9 Signature Algorithm: sha256WithRSAE - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1-1.crt X509v3 Basic Constraints fa:29:72:01:3e:b7:06:f1:2f:1a:0e:91:c5:ec:35:bf:f5:da: 33:95:de:24:12:0d:f5:c3:23:8d:40:82:d1:5c:eb:de:0a:08: e8:e5:83:e5:0a:8b:3a:5e:
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Altan (Net ID: 00:12:BF:67:61:97)
2023-05-12 02:44:03	Username	No	SpiderFoot UI	0	0	0	0	None	DawixSulej
2023-05-12 03:08:48	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.227
2023-05-12 03:18:06	URL (Uses Javascript)	No	Page Information	0	0	3	0	None	http://funny.battleb0t.xyz
2023-05-12 03:09:41	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	120.48.229.35.bc.googleusercontent.com
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0065paula.github.io
2023-05-12 03:01:17	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.152): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	NameCheap, Inc.
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	6	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=A6pUH5BrVxAUHCFyEeZi9CXof2Qs7NDG4lIwx2vXWTr3bfLmD6TvAbu9
2023-05-12 03:08:47	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.222
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.209): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:27	Linked URL - Internal	No	URLScan.io	4	0	1	0	None	https://kekw.battleb0t.xyz/jar
2023-05-12 03:08:51	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.120
2023-05-12	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Persistent_Auth": "DISPLAY_UTF8", "Host": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Connection": "DISPLAY_UTF8", "Www

02:55:11									
2023-05-12 03:13:01	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-oo.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Carmen (Net ID: 00:00:28:F1:95:B9)
2023-05-12 02:45:34	Physical Location	No	ipapi.co	0	0	3	0	None	North Charleston, South Carolina, SC, United States, US
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:60:35:51)
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	aes256-gcm@openssh.com
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:8443
2023-05-12 02:44:12	Web Technology	No	Tool - Wappalyzer	0	0	2	0	None	Nginx
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Lichtensteiner (Net ID: 00:01:E3:57:D3:4C)
2023-05-12 02:54:51	Open TCP Port	No	Censys	0	0	3	0	None	34.74.170.74:80
2023-05-12 02:54:34	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Superonline_WiFi_7320 (Net ID: 00:02:61:5C:85:FF)
2023-05-12 03:09:37	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	226.30.196.104.bc.googleusercontent.com
2023-05-12 02:44:17	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-opener-policy: same-origin
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	4	0	None	Germany
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:E5:E0:81)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:09:F8:70)
2023-05-12 03:01:19	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.171): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:29	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	The Batcave (Net ID: 00:11:32:A4:B5:6D)
2023-05-12 02:44:06	Domain Whois	No	Whois	14	0	1	0	None	Domain Name: AYHU.XYZ Registry Domain ID: D338262912-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy and contain information pertaining to Internet domain names registered by our our customers. By using this service you are agreeing (1 DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Admin Count purpose, including mining this data for your own personal or commercial purposes. Failure to comply with these terms may result in ter
2023-05-12 03:18:53	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Rotated 90 CW @ 18}
2023-05-12	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.120

03:08:50									
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.32): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:32:18	Malicious Affiliate	Yes	abuse.ch	0	1	4	0	None	abuse.ch URLhaus (Domain) [cdn-185-199-110-154.github.com] https://urlhaus.abuse.ch/downloads/csv_recent/
2023-05-12 02:54:30	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Server: nginx Date: <REDACTED> Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary:
2023-05-12 02:44:09	Co-Hosted Site	No	SSL Certificate Analyzer	2	1	1	0	None	github.io
2023-05-12 02:45:02	Physical Location	No	ipapi.co	0	0	2	0	None	San Francisco, California, CA, United States, US
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:54:13	Web Content Type	No	Web Spider	0	0	3	0	None	text/html;charset=utf-8
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	MCName (Minecraft) (Category: gaming) https://mcname.info/en/search?q=ayhu
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AIRTIES_RT-205 (Net ID: 00:12:BF:3D:DD:C5)
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	GitHub (Category: coding) https://github.com/ayshoo
2023-05-12 03:28:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.144:8080
2023-05-12 03:31:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	abuse@godaddy.com
2023-05-12 02:44:10	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	1	1	0	None	github.io
2023-05-12 02:44:22	Physical Location	No	ipstack	0	0	2	0	None	United States
2023-05-12 02:58:58	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "Local\\!BrowserEmulation!SharedMemory!Mutex"\n "Local\\URLBLOCK_FILEMAPSWITCH_MUTEX_3376"\n "Local [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 00000000-00002536]\n "searc 11E7-B67B-080027A49DD6_.dat" has type "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]'}, {u'category' u'Network Related', u'origin': u'File/Memory', u'identifier': u'string-102', u'name': u'Found decrypted SSL traffic', u'attck_id_wiki'
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:01:E6:93:CF:EC)
2023-05-12 02:44:35	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Google Analytics
2023-05-12 02:57:24	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	tiktok.battleb0t.xyz
2023-05-12 02:47:12	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"13.227.7 [targetUID: N/A]\n "6102a13ad6dfa169537a8465_ek_check-icon-yellow_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUID: N (Indicator: "twitter")\n "GET /uwt.js HTTP/1.1\nAccept: application/javascript, */*;q=0.8\nReferer: https://heartex.com/\nAccept-Langu forwarded-proto, Accept-Encoding\nX-Served-By: cache-iad-kjyo7100030-IAD\nAccept-Ranges: bytes\nx-amzn-Remapped-Date: Fri, 03 Mar 2023
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00088.github.io
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	1136 4120 (Net ID: 00:0F:CC:76:66:44)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	referrer-policy: strict-origin-when-cross-origin
2023-05-12 03:37:16	Physical Location	No	MetaDefender	0	0	3	0	None	Northbrook, United States

2023-05-12 02:44:18	Internet Name	No	DNS Resolver	2	0	2	0	None	funny.battleb0t.xyz
2023-05-12 03:10:37	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.108.154:443
2023-05-12 03:03:18	Internet Name	No	DNS Resolver	0	0	2	0	None	www.ayhu.xyz
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00d.github.io
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	FruityWifi-003 (Net ID: 00:07:0E:65:CF:39)
2023-05-12 03:03:55	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	james-gamboa.github.io
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:443
2023-05-12 03:09:45	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	137.97.148.34.bc.googleusercontent.com
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Je buurman (Net ID: 00:01:71:0C:63:FC)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomD04238 (Net ID: 00:0C:F6:D0:42:38)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Villa (Net ID: 00:01:E3:07:FC:86)
2023-05-12 02:44:31	Affiliate - Internet Name	No	DNS Resolver	23	0	2	0	None	cdn-185-199-111-153.github.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Wowhead (Category: gaming) https://www.wowhead.com/user=login
2023-05-12 02:54:22	Linked URL - Internal	No	Web Spider	4	0	3	0	None	https://www.ayhu.xyz/cdn-cgi/styles/challenges.css
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.65): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:51	Internet Name	No	DNS Resolver	0	0	3	0	None	kekw.battleb0t.xyz
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	GHARANA (Net ID: 00:01:E3:0F:5B:9B)
2023-05-12 03:17:44	Account on External Site	No	Account Finder	0	0	1	0	None	TikTok (Category: social) https://www.tiktok.com/@_BattleB0t_?lang=en
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	imgur (Category: images) https://imgur.com/user/Battleb0t/about
2023-05-12 02:55:12	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"dai.com"\n "www.dai.com"'}, {u'category': u'General', u'origin': u N/A]\n "_72D7BA37-B41E-11ED-92C7-080027889E1B_.dat" has type "Composite Document File V2 Document Cannot read section info"- [targetUI ^_>SOX=Zv})9}~xbeVW7\nYM0^+=}:Sz=,8bsbe8vq!bt^f\n7f~FF/o-O~zw8.z/#/Mgh_n}~9t}\\g/boSm=}Z(Y\\Ojl{~d`sP~Yzg3}~vf\\YW/lo5{|lkmNfBU<5gOv]z fG0WXTxTDDDIs\\V+>A4\'OJgQ*VfVVs\\L"*kqI5g,w9<{jSpUqD0lt<k%Eg7ShX&fd0clX](xvrh|h%D1cS1\nbz.J:5-uP!,NCZQE@e|IE"RV__JqJhCqRH!3=GY)*\\BSl
2023-05-12 03:12:10	Affiliate Description - Category	No	DuckDuckGo	0	0	5	0	None	Privately held companies of England
2023-05-12 02:59:50	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	jloup@gzip.org

2023-05-12 03:09:30	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.24): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:33	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:d5:98:ae:2a:84:a2:19:ac:80:9a:6c:74:76:20:f8:3f:d8 Signature Algorithm: sha256Wi Web Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 6D
2023-05-12 02:45:35	Internet Name	No	DNSDumpster	0	0	1	0	None	fluid.battleb0t.xyz
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	FriendFinder-X (Category: dating) https://www.friendfinder-x.com/profile/ayshoo
2023-05-12 03:01:19	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.165): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:58	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	hamaha (Category: finance) https://hamaha.net/login
2023-05-12 02:44:12	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 9d:49:08:08:d4:e9:44:f0:ed:d2:82:b7:e0:6b:90:98 Signature Algorithm: sha256WithRSAE 76:FF:88:3F:0A:B6:FB:95:51:C2:61:CC:F5:87:BA:34: B4:A4:CD:BB:29:DC:68:42:0A:9F:E6:67:4C:5A:3A:74 Timestamp : Apr 27 08:49:21.510 2023 74:0e:15:b3:cc:fb:a8:3c:e6:07:2b:89:aa:f9:0a:70:0d:02: b5:99:9c:87
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Shuttle (Net ID: 00:01:36:07:54:71)
2023-05-12 03:03:18	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12 02:44:27	Internet Name	No	DNS Resolver	0	0	2	0	None	www.battleb0t.xyz
2023-05-12 02:44:03	Username	No	SpiderFoot UI	7	0	0	0	None	_BattleB0t_
2023-05-12 02:53:45	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache_Hits": "DISPLAY_UTF8", "Via": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "V
2023-05-12 02:54:00	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12 02:59:59	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	jloup@gzip.org
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	wattpad (Category: social) https://www.wattpad.com/user/Altpapier
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cf-access-domain: panel.battleb0t.xyz
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.220): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Brandon (Net ID: C4:49:BB:70:F9:3A)
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	5	0	None	cloudflare
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	TEKER PERFORMANS (Net ID: 00:13:33:8D:5A:FE)
2023-05-12 02:57:03	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "IsoScope_684_ConnHashTable<1668>_HashTable_Mutex"\n "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "IsoScope_684_IE_EarlyTabStart_0xfe4_M [targetUID: 00000000-00003144]\n Dropped file: "OP4TNIKT.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\OP4TNIKT.txt]- [tar

									Dropped file: "DNZGTUBL.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\DNZGTUBL.txt]- [targetUID: 00000000-00003144]\n Drop "7cH1v4okm5zmbvwkAx_sfcEuiD8jPvWsOdC5_1_.woff" has type "Web Open Font Format TrueType length 19208 version 1.1"- [targetUID: N/A]\n "
2023-05-12 03:03:47	Co-Hosted Site	No	ThreatMiner	2	0	2	0	None	rathook.cc
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Intel Gateway (Net ID: 00:02:B3:A5:C9:64)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Keybase (Category: social) https://keybase.io/login
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.83): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:38	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:46:03	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'city': u'North Charleston', u'security': {u'is_vpn': False}, u'city_geoname_id': 4589387, u'region_geoname_id': 4597040, u'country'
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom (Net ID: 00:0C:F6:37:01:3C)
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0001vrn.github.io
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	MCUUID (Minecraft) (Category: gaming) https://mcuuid.net/?q=battleb0t
2023-05-12 03:08:49	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.114
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00p513-dev.github.io
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	3Com (Net ID: 00:04:75:62:7A:78)
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	herron-libson (Net ID: 00:01:24:F1:75:B2)
2023-05-12 03:00:22	Raw Data from RIRs	No	Certificate Transparency	1	0	2	0	None	[{u'not_after': u'2023-06-25T13:22:32', u'not_before': u'2023-03-27T13:22:33', u'issuer_ca_id': 183267, u'name_value': u'kekw.battleb0 u'id': 8512878872}, {u'not_after': u'2023-03-18T21:24:58', u'not_before': u'2022-12-18T21:24:59', u'issuer_ca_id': 183267, u'name_valu
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	CH2SC6TY (Net ID: 00:16:46:71:5C:B0)
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Twitter (Category: social) https://twitter.com/ayshoo
2023-05-12 03:12:41	Vulnerability - CVE High	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 7.5 Description: The DES and Triple DES ciphers, as used in the TL
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	DTT (Net ID: 00:02:2D:2C:9F:8D)
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:143
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	5	0	None	Nics Telekomunikasyon Ltd.
2023-05-12 02:54:13	HTTP Headers	No	Web Spider	8	0	3	0	None	{"content-length": "103646", "via": "1.1 varnish", "vary": "Accept-Encoding", "etag": "W/\"642b434c-63a06\"", "x-cache-hits": "0", "ca
2023-05-12 03:10:03	Affiliate - Internet Name	No	DNS Resolver	10	0	4	0	None	baffin.netcraft.com
2023-05-12 02:44:22	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.com

2023-05-12 03:32:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.4:8443
2023-05-12 02:54:20	Web Content Type	No	Web Spider	0	0	4	0	None	text/css
2023-05-12 03:01:32	Raw Data from RIRs	No	Tool - WhatWeb	1	0	3	0	None	[{u'request_config': {u'headers': {u'User-Agent': u'Mozilla/5.0'}}, u'target': u'http://vscode.battleb0t.xyz', u'http_status': 521, u'
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	fotka (Category: social) https://fotka.com/profil/login
2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.122
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	AMX (Net ID: 00:02:E3:40:F7:BD)
2023-05-12 03:01:17	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.151): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:30	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 02:54:20	Web Content Type	No	Web Spider	0	0	2	0	None	text/html;charset=utf-8
2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	172.67.168.252
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0066cc.github.io
2023-05-12 02:54:17	HTTP Headers	No	Censys	0	0	4	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:50:23	Blacklisted IP Address	Yes	Honeypot Checker	0	1	3	0	None	Honeypotproject (104.21.71.14): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:58	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.97): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	JWNK (Net ID: 00:14:5C:88:0D:74)
2023-05-12 03:23:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.12:443
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Ziggo61714 (Net ID: 00:0C:F6:59:F1:12)
2023-05-12 02:54:18	Linked URL - External	No	Web Spider	3	0	3	0	None	http://code.jquery.com/jquery-3.2.1.js
2023-05-12 02:46:55	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:cd:b7:3c:d6:71:f3:4f:d0:0b:1c:3a:89:f9:32:41:9b:99 Signature Algorithm: sha256Wi b9:d7:f5:17:db:c5:b5:da:58:15:fd:4b:36:d5:4d:d6:5d:2b: 4f:49:fe:17:38:11:d4:b2:eb:07:49:19:e3:43:16:4c:57:7c: 97:e9:db:e2:60:b9:08:77:
2023-05-12 03:34:02	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	IDATx A`qRWQ @Qh9' WYW`Q 6:E<0s qt2!X O"Np /Z9l6 23W4R p$ke'V sZSjUQ S\-up iTb.T IDAT? ZYjy9 k-<Z6 DRZ1s NLgiN 7jI\k q8cH$ cG$C: 70/1c
2023-05-12 03:24:22	Linked URL - Internal	No	Web Spider	4	0	3	0	None	https://ayhu.xyz/?__cf_chl_f_tk=VqQIpv85XrbB73FISUPAb3YOKzrkafpohMHe42yb99c-1683861862-0-gaNycGzNChA
2023-05-12 02:53:41	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\!BrowserEmulation!SharedMemory!Mutex"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-1', None, u'attck_id': None, u'relevance': 7, u'threat_level': 0, u'type': 2, u'description': u'"src="https://www.facebook.com/tr?id=21161 b}xy.N="internal.enableAutoEventOnScroll";var cc=ea(["data-gtm-yt-inspected-"])\nyy=["www.youtube.com"\n"www.youtube-nocookie.com"]\nz "data")\n Antivirus vendors marked dropped file "Tar2FA0.tmp" as clean (type is "data")'}, {u'category': u'Installation/Persistence',
2023-05-12 02:44:32	Affiliate - Internet Name	No	DNS Resolver	2	0	2	0	None	cdn-185-199-108-153.github.com
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	7622 0155 (Net ID: 00:00:C5:F9:20:A8)

2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	Duolingo (Category: hobby) https://www.duolingo.com/profile/Altpapier
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	^D^M^L^W^]^C^A^U^M^Y^E^L^_^R^G (Net ID: 00:05:5D:D9:90:56)
2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.125
2023-05-12 02:48:29	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'General', u'origin': u'Network Traffic', u'identifier': u'network-0', u'name': u'Contacts domains', u'attck_id_wiki': u'https://atta 1_1_.png" has type "PNG image data 561 x 379 8-bit/color RGBA non-interlaced"- [targetUID: N/A]\n "free-fa-solid-900_1_.eot" has type with HTTP webserver (GET/POST requests)', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/001', u'threat_level_human': u Heuristic match: "habby-bit.github.io"\n Heuristic match: "ka-f.fontawesome.com"\n Heuristic match: "kit.fontawesome.com"\n Pattern ma
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	zoom (Net ID: 00:01:38:85:BD:08)
2023-05-12 02:44:07	Software Used	Yes	Tool - Wappalyzer	0	0	1	0	None	GitHub Pages
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Chess.com (Category: gaming) https://www.chess.com/member/login
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	5	0	None	United States
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	linksys (Net ID: 00:14:BF:93:D4:35)
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:23:36:1a:72:6e:fc:71:09:49:b1:35:f9:b5:e5:28:80:de Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: E6:0D: 89:35:6f:e7:d7:11:5a:13:0a:a9:83:9e:0f:c2:f2:ea:d8:50: 30:65:9c:16:49:f6:30:d8:a2:e3:83:ff:5d:ff:00:a2:ff:57: de:68:f4:70:90:a3:db:c8:
2023-05-12 02:53:17	IP Address	No	Mnemonic PassiveDNS	0	0	1	0	None	172.67.135.9
2023-05-12 02:44:14	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
2023-05-12 02:44:16	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3037::6815:470e
2023-05-12 03:03:19	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12 03:09:28	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	87.248.157.102:443
2023-05-12 03:09:46	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	67.170.74.34.bc.googleusercontent.com
2023-05-12 03:00:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.15): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.124): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:54	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.83): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SK_WiFi20D4 (Net ID: 00:01:36:9F:20:D5)
2023-05-12 03:00:58	Malicious Affiliate	Yes	VXVault.net	0	1	3	0	None	VXVault Malicious URL List [cdn-185-199-111-153.github.com] http://vxvault.net/URL_List.php
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	101 (Net ID: 00:01:03:7C:1B:D2)
2023-05-12 02:44:07	Co-Hosted Site	No	CertSpotter	1	0	1	0	None	sni.cloudflaressl.com
2023-05-12 03:13:02	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-ye.github.io] https://www.openphish.com/feed.txt
2023-05-12	Username	No	SpiderFoot UI	15	0	0	0	None	Battleb0t

02:44:03									
2023-05-12 02:54:07	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-11T22:54:40.561Z", "ip": "2606:4700:3031::ac43:8709", "location_updated_at": "2023-05-06T00:44:41.372312Z "AAAA", "resolved_at": "2023-05-05T13:43:55.541214446Z"}, "theucontgi.tk": {"record_type": "AAAA", "resolved_at": "2023-04-23T21:28:34 "centreonicinga.wwbn.com": {"record_type": "AAAA", "resolved_at": "2023-05-07T16:18:28.593025009Z"}, "erkilgalegohlo.cf": {"record_typ 11T15:26:42.690547113Z"}, "webdisk.cncap.ca": {"record_type": "AAAA", "resolved_at": "2023-05-01T12:42:56.064120059Z"}, "cpcalendars.m "resolved_at": "2022-12-02T09:33:27.167277863Z"}, "mail.hlb.co.za": {"record_type": "AAAA", "resolved_at": "2023-04-26T22:59:18.792128
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Gettr (Category: social) https://gettr.com/user/Altpapier
2023-05-12 02:54:54	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	Pastebin (Category: tech) https://pastebin.com/u/Battleb0t
2023-05-12 02:54:08	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:b9:dc:49:67:68:c5:fe:31:cf:92:a4:a3:f2:91:5a:dc:15 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: CF:FE: b6:9b:be:8a:ca:3c:4b:e8:78:6a:03:13:65:55:9c:8c:1b:f0: fe:30:16:e0:6f:32:f7:3f:aa:f2:94:1e:87:e0:1f:d5:4c:32: ca:75:84:5e:e4:d3:9f:f9:
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom707CF8 (Net ID: 00:0C:F6:70:7C:F8)
2023-05-12 03:09:59	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	clientify.net
2023-05-12 03:15:46	Username	No	Account Finder	8	0	1	0	None	patrickpogoda
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	Chess.com (Category: gaming) https://www.chess.com/member/Battleb0t
2023-05-12 02:53:07	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	None None
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha2-512-etm@openssh.com
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	TDFFE (Net ID: 00:02:2D:42:1D:82)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<hidden ssid> (Net ID: 00:01:E3:55:BC:8C)
2023-05-12 03:01:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.245): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:34	BGP AS Membership	No	Censys	0	0	3	0	None	13335
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	EPSON (Net ID: 00:00:48:03:3B:CF)
2023-05-12 03:09:49	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	81.170.74.34.bc.googleusercontent.com
2023-05-12 03:27:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.128:443
2023-05-12 02:44:31	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	files.battleb0t.xyz
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-mitigated: challenge
2023-05-12 03:01:32	Raw Data from RIRs	No	Tool - WhatWeb	1	0	3	0	None	[{u'request_config': {u'headers': {u'User-Agent': u'Mozilla/5.0'}}, u'target': u'http://panel.battleb0t.xyz', u'http_status': 301, u'p
2023-05-12 02:45:16	Raw Data from RIRs	No	ipapi.co	0	0	4	0	None	{u'region_code': u'ON', u'country_tld': u'.ca', u'ip': u'2606:4700:3030::ac43:a8fc', u'currency_name': u'Dollar', u'currency': u'CAD',

2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Onward (Net ID: 00:06:25:D6:7A:6F)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 03:10:22	Malicious IP on Same Subnet	Yes	VoIPBL OpenPBX IPs	0	0	4	0	None	VOIPBL Publicly Accessible PBX List [46.101.128.0/17] http://www.voipbl.org/update
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	1	5	0	None	Netlify
2023-05-12 03:03:31	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:24:21	Linked URL - Internal	No	Web Spider	4	0	3	0	None	https://ayhu.xyz/lol.html?__cf_chl_f_tk=s7qF6ZO3cVvdEEZa_WmCMPM6sxOwT7Q8EvJA4xw7FTE-1683861861-0-gaNycGzNChA
2023-05-12 02:55:22	Linked URL - Internal	No	Google	5	0	1	0	None	https://ayhu.xyz/lol.html
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ZyXEL (Net ID: 00:02:CF:C6:25:17)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:F4:A6:EC)
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	YouTube Channel (Category: video) https://www.youtube.com/c/Altpapier/about
2023-05-12 02:53:42	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 02:47:25	Open TCP Port	No	Pulsedive	0	0	2	0	None	185.199.108.153:80
2023-05-12 02:54:23	Open TCP Port	No	Censys	0	0	4	0	None	2600:1f18:2489:8201::c8:443
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	x-cache-hits: 1
2023-05-12 03:01:28	Raw Data from RIRs	No	Tool - WhatWeb	1	0	2	0	None	[{u'request_config': {u'headers': {u'User-Agent': u'Mozilla/5.0'}}, u'target': u'http://nwapi.battleb0t.xyz', u'http_status': 301, u'p
2023-05-12 03:01:20	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.176): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://funny.battleb0t.xyz/images/master058_3.PNG
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	polygon (Category: gaming) https://www.polygon.com/users/login
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	jk9@home (Net ID: 00:0C:F6:71:B1:B4)
2023-05-12 02:44:30	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	risk.ru (Category: hobby) https://risk.ru/people/login
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	tsunami (Net ID: 00:0D:29:AC:D7:2D)
2023-05-12 02:44:14	IPv6 Address	No	DNS Resolver	16	0	1	0	None	2606:4700:3031::6815:6a6
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Andrea Schwartz Gallery 5G (Net ID: 00:01:9F:3D:4F:6C)

2023-05-12 03:15:36	Physical Location	No	ipstack	0	0	2	0	None	Iran
2023-05-12 02:45:03	Country	No	Country Name Extractor	0	0	2	0	None	Russia
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.73): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:38	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	1232 (Net ID: 00:01:03:7C:2D:17)
2023-05-12 02:44:30	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Font Awesome
2023-05-12 02:45:34	Email Gateway (DNS MX Records)	No	DNS Raw Records	0	0	1	0	None	route2.mx.cloudflare.net
2023-05-12 03:41:58	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	domixo-hosting.de
2023-05-12 02:50:28	Raw Data from RIRs	No	GLEIF	0	0	3	0	None	[{u'relationships': {u'lei-records': {u'data': {u'type': u'lei-records', u'id': u'5493005GJOH8HLL11157'}, u'links': {u'related': u'htt
2023-05-12 02:44:21	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3037::6815:470e
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00x44.github.io
2023-05-12 02:44:09	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 0d:40:8d:d9:7c:a1:bd:4c:0d:06:c5:3f:c3:e9:2e:bc Signature Algorithm: sha256WithRSAE 84:de:17:e3:7f:b0:fd:4c:e4:f5:d9:c1:87:4a:b8:32:d6:97: 13:2d:ab:c3:d8:0c:ce:60:02:7a:3d:d5:8b:4f:9b:89:37:1e: 07:e8:65:4f:13:db:bc:f2:
2023-05-12 03:09:31	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.23): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	suddenlink.net-8F90 (Net ID: 84:94:8C:33:8F:98)
2023-05-12 03:41:52	Open TCP Port Banner	No	Censys	0	1	3	0	None	SMB SMB 2.1
2023-05-12 02:46:00	Physical Location	No	AbstractAPI	0	0	3	0	None	Chicago, Illinois, 60666, United States, North America
2023-05-12 02:54:13	Web Content Type	No	Web Spider	0	0	3	0	None	application/javascript;charset=utf-8
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	downtown5 (Net ID: 00:01:E3:E9:56:90)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	HubPages (Category: blog) https://hubpages.com/@ayhu
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet8FBA (Net ID: 00:01:36:5C:8F:B8)
2023-05-12 03:13:07	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00ihsan.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:08:45	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.211
2023-05-12 02:44:31	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3030::ac43:a8fc
2023-05-12 02:54:54	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12	Affiliate - Internet	No	DNS Resolver	0	0	4	0	None	119.48.229.35.bc.googleusercontent.com

03:09:40	Name								
2023-05-12 03:00:57	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00yongshiwangzi.github.io
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	APC (Net ID: 00:09:5B:4F:F1:CA)
2023-05-12 02:44:36	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 02:45:04	Country	No	Country Name Extractor	0	0	2	0	None	United States
2023-05-12 03:18:53	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Rotated 180 @ 18}
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	FRBEACH (Net ID: 00:02:2D:8A:07:45)
2023-05-12 03:00:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.50): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	apple network 3a656b (Net ID: 00:02:2D:05:9A:3A)
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.26): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	aes128-gcm@openssh.com
2023-05-12 02:44:14	Co-Hosted Site	No	SSL Certificate Analyzer	3	1	2	0	None	netlify.app
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	BJNPSETUP (Net ID: 00:00:85:F4:1C:9A)
2023-05-12 03:24:21	HTTP Status Code	No	Web Spider	0	0	3	0	None	403
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	omniblock (Net ID: 00:09:5B:E9:6B:D6)
2023-05-12 03:15:36	Physical Location	No	ipstack	0	0	3	0	None	Germany
2023-05-12 02:46:50	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	3	0	None	C=US,ST=California,L=San Francisco,O=Netlify\, Inc,CN=*.netlify.app
2023-05-12 02:45:58	Physical Location	No	AbstractAPI	1	0	3	0	None	Frankfurt am Main, Hesse, 60313, Germany, Europe
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00yongshiwangzi.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2053
2023-05-12 03:09:24	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	1	3	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.173): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:08	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.110.133:80
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 02:54:16	Linked URL - Internal	No	Web Spider	4	0	3	0	None	https://oldfluid.battleb0t.xyz/./script.js
2023-	Open TCP	No	Pulsedive	0	0	2	0	None	104.21.6.166:80

12 02:47:30	Port								
2023-05-12 03:01:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.255): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:56	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'CA', u'country_tld': u'.us', u'ip': u'185.199.111.153', u'currency_name': u'Dollar', u'currency': u'USD', u'country
2023-05-12 03:23:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.4:443
2023-05-12 02:54:03	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-12T00:51:50.399Z", "ip": "172.67.135.9", "location_updated_at": "2023-04-28T23:58:12.936747Z", "autonomou "A", "resolved_at": "2023-01-28T13:41:29.917096426Z"}, "account-dev.prinsapps.com": {"record_type": "CNAME", "resolved_at": "2022-11-2 {"record_type": "A", "resolved_at": "2023-01-29T13:41:58.275178074Z"}, "www.usbestsiding.com": {"record_type": "A", "resolved_at": "20 "2023-04-24T22:20:31.002106199Z"}, "shop.geminibio.com": {"record_type": "A", "resolved_at": "2023-05-10T14:29:06.617280204Z"}, "esipd {"record_type": "A", "resolved_at": "2023-05-07T19:46:39.285928826Z"}, "4wdinfo.com": {"record_type": "A", "resolved_at": "2023-05-10T
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Omni (Net ID: 00:02:2D:17:C6:E0)
2023-05-12 02:44:21	Physical Location	No	ipstack	0	0	2	0	None	United States
2023-05-12 02:54:19	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2023-05-12 03:08:38	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	185.199.108.154
2023-05-12 03:23:44	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.17:8443
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://pics.battleb0t.xyz
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Omni (Net ID: 00:02:2D:17:C6:E0)
2023-05-12 02:55:08	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:74:c7:69:09:be:bf:85:53:83:95:0e:84:5e:23:6b:8f:95 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 1F:80: d8:d8:3b:7d:a5:0b:bf:d3:08:d9:73:26:67:23:22:51:a7:9a: 35:1e:3d:5b:8d:37:8d:5a:13:a6:11:a6:6e:3f:57:92:c4:df: b9:a6:2d:3e:a3:ac:33:74:
2023-05-12 02:44:22	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 03:03:19	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	1200 (Net ID: 00:01:03:7C:0A:E5)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Internet Archive Account (Category: misc) https://archive.org/details/@ayhu
2023-05-12 03:23:19	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.5:8080
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Pinterest (Category: social) https://www.pinterest.com/ayhu/
2023-05-12 02:54:44	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'threat_level': 0, u'type': 8, u'description': u'"urlblockindex_1_.bin" has type "data"- [targetUID: N/A]\n "urlref_httpsllink.tou_ht "httpErrorPagesScripts_1_" has type "UTF-8 Unicode (with BOM) text with CRLF line terminators"- [targetUID: N/A]\n "CabBB69.tmp" has t "MUIDB0843E9110DDB6B4E0942FBDE0C5F6A01ieonline.microsoft.com/9216229670643231098083269878373031019620*"\n Heuristic match: "rabetsanat
2023-05-12 02:46:30	Netblock Membership	No	RIPE	1	0	3	0	None	104.21.64.0/20
2023-05-12 02:54:10	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3031::6815:6a6:443
2023-05-12 03:31:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	fd796f83a89a42f2a69f4b9f2c757b8f.protect@withheldforprivacy.com
2023-05-12	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 3, u'search_terms': [{u'id': u'host', u'value': u'104.21.6.166'}], u'result': [{u'environment_id': 100, u'job_id': u'640a87

02:55:28									
2023-05-12 02:44:12	SSL Certificate Host Mismatch	Yes	SSL Certificate Analyzer	0	0	2	0	None	*.cloudwaysapps.com, cloudwaysapps.com
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	overkant (Net ID: 00:01:36:07:DC:22)
2023-05-12 02:51:36	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'capec_id': None, u'attck_id': u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"query.prod.cms.msn.c "c:\\users\\%osuser%\\appdata\\local\\temp\\~df196c020f5a094e9f.tmp"\n "iexplore.exe" reads file "c:\\users\\%osuser%\\appdata\\local\ "~DF3999E32F2D2A875E.TMP" has type "data"- Location: [%TEMP%\\~DF3999E32F2D2A875E.TMP]- [targetUID: 00000000-00003172]\n "~DFF70C03EBA [%APPDATA%\\Microsoft\\Windows\\Cookies\\FG7SB3TD.txt]- [targetUID: 00000000-00003172]\n "main_1_.css" has type "ASCII text"- [targetU
2023-05-12 02:50:45	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"185.199.108.153:443"\n "172.64.133.15:443"'}, {u'category': u'Gene interlaced" and extension "png"\n "tablet1_1_.png" has type "PNG image data 407 x 256 8-bit/color RGBA non-interlaced" and extension " bit colormap non-interlaced"- [targetUID: N/A]\n "urlref_httpskhushishikhu.github.ioNetflix-clone" has type "HTML document ASCII text" bits/pixel"- [targetUID: N/A]'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifier': u'string-3', u'name': u'F
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	LF-X1U.00014A10EF0C (Net ID: 00:01:4A:10:EF:0C)
2023-05-12 02:54:23	BGP AS Membership	No	Censys	0	0	4	0	None	14618
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	WordPress (Category: blog) https://profiles.wordpress.org/login/
2023-05-12 03:09:36	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	219.30.196.104.bc.googleusercontent.com
2023-05-12 03:41:52	Open TCP Port	No	Censys	0	0	3	0	None	45.131.109.53:5985
2023-05-12 02:44:28	Affiliate - Internet Name	No	DNS Resolver	22	0	2	0	None	battleb0t.github.io
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	UFUKDEN (Net ID: 00:02:CF:9F:96:D2)
2023-05-12 02:44:31	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	teamcity.battleb0t.xyz
2023-05-12 03:23:19	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.5:443
2023-05-12 03:13:09	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [01039402468.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	referrer-policy: same-origin
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Telegram (Category: social) https://t.me/ayshoo
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	FurAffinity (Category: images) https://www.furaffinity.net/user/login
2023-05-12 03:19:24	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.109.154:443
2023-05-12 02:56:25	BGP AS Membership	No	RIPE	0	0	4	0	None	14061
2023-05-12 02:53:52	Open TCP Port	No	Censys	0	0	2	0	None	2606:50c0:8003::153:443
2023-05-12 03:00:58	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	010pixel.github.io
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}

2023-05-12 03:18:06	URL (Form)	No	Page Information	0	0	3	0	None	http://www.ayhu.xyz
2023-05-12 03:00:55	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00ihsan.github.io
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:0C:41:79:25:FC)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-4C62 (Net ID: 00:1D:D5:6D:4C:60)
2023-05-12 02:45:43	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'suspicious'}, {u'url': u'https://s3.amazonaws.com/uploads.webconnex.com/120734%2f1680697381119-1680697381118.png', u'type': u'extrac u'extracted', u'verdict': u'suspicious'}, {u'url': u'https://s3.amazonaws.com/uploads.webconnex.com/120734%2f1675882703373-sp-_0001_vo u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relev stable.json")\n Found string ""www.facebook.com"," (Indicator: "dir "; File: "wallet-stable.json")\n Found string ""linkedin.com"," (I
2023-05-12 02:44:09	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	1	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS RSA SHA256 2020 CA1
2023-05-12 02:58:02	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "143.244.60.109:443"\n "142.251.33.104:443"\n "13.249.139.119:80"\n "142.251.211.227:80"\n "192.124.249.36:80"\n "65.8.55.48:80"\n "17 "ocsp.sectigo.com"\n "ocsp.sca1b.amazontrust.com"'}, {u'category': u'Unusual Characteristics', u'origin': u'Binary File', u'identifier [%APPDATA%\\Microsoft\\Windows\\Cookies\\3FN51MI9.txt]- [targetUID: 00000000-00002924]\n Dropped file: "WHAC3UI2.txt" - Location: [%AP [%TEMP%\\~DF798C5B654290816F.TMP]- [targetUID: 00000000-00002884]\n "E573CDF4C6D731D56A665145182FD759_CCBDC18CEF38DE614F9036FAB40737A8
2023-05-12 02:44:03	Human Name	No	SpiderFoot UI	2	0	0	0	None	Dawid Sulej
2023-05-12 02:44:13	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	2	0	None	github.com
2023-05-12 03:19:22	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.109.153:443
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	steg (Net ID: 00:01:36:06:3F:F8)
2023-05-12 03:13:09	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [01.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:49:55	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level': 0, u'type': 1, u'description': u'INSTANCE.getVersionsFolder@FolderUtils at cb617139dd424aa668b0102de6fd5feb-20db3'}, match: "https://github.com/cabaletta/baritone/blob/master/USAGE.md"\n Pattern match: "https://www.youtube.com/channel/UCJGCNPEjvsCn0FK "www.protocol.http.HttpURLConnection.plainConnect0()V+357"\n Pattern match: "www.protocol.http.HttpURLConnection.plainConnect()V+71"\n player."\n "Did you know? .+ just joined The Vortex Coalition!"\n ".+ has successfully conducted the cactus dupe and duped a itemhand!
2023-05-12 02:50:31	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:3a:9d:01:de:8f:db:a2:52:4a:02:0c:18:70:da:44:dd:bc Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 20:59: 29:67:65:9c:a3:5e:54:d7:42:a2:ca:57:e3:ed:40:b5:6b:e7: 20:ae:3b:11:70:76:c2:da:cf:31:f0:ab:ca:10:28:73:4e:36: 4a:79:71:99:ba:fe:41:29:
2023-05-12 03:01:08	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.118): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Av.AliBerksun (Net ID: 00:18:4D:47:67:DA)
2023-05-12 02:44:31	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:56:b0:2c:f1:37:ec:4d:fb:ba:29:5b:fe:cf:08:f7:c5:d3 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 76:A0: 12:86:a7:7c:6b:b8:cf:88:07:9a:b1:b0:e7:e8:80:0a:54:1c: 15:61:1e:50:90:fa:7e:93:82:0d:40:bf:16:d5:1e:1e:93:9f: 58:6f:56:5d:6c:49:c2:36:
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=kekw.battleb0t.xyz
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	suddenlink.net-5263 (Net ID: 2C:99:24:25:52:61)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-F3A2 (Net ID: 00:1D:D2:43:F3:A0)
2023-05-12 02:55:18	Software Used	Yes	Censys	0	0	3	0	None	Ubuntu Linux
2023-05-	Open TCP	No	Censys	0	0	2	0	None	

12 02:55:05	Port Banner								HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:24:29	Company Name	No	Company Name Extractor	0	0	3	0	None	Cloudflare\, Inc.
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	TrackmaniaLadder (Category: gaming) https://en.tm-ladder.com/login_rech.php
2023-05-12 03:00:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.56): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:0C:41:AC:F5:99)
2023-05-12 03:11:15	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'London', u'security': {u'is_vpn': False}, u'city_geoname_id': 2643743, u'region_geoname_id': 6269131, u'country': u'United
2023-05-12 02:50:26	Raw Data from RIRs	No	GLEIF	0	0	3	0	None	[{u'relationships': {u'lei-records': {u'data': {u'type': u'lei-records', u'id': u'5493007DY18BGNLDWU14'}, u'links': {u'related': u'htt
2023-05-12 02:44:15	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Node.js
2023-05-12 02:56:50	Internet Name	No	DNS Resolver	0	0	2	0	None	battleb0t.xyz
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.74): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	x-cache: HIT
2023-05-12 02:54:13	Web Content	No	Web Spider	2	0	1	0	None	<!DOCTYPE html> <html lang="en-US"> <head> <title>Just a moment...</title> <meta http-equiv="Content-Type" content="text/html; charset T32j1LOogUb6WyPmjQkstsoGMIPyZHJWu0K53P0Hp3SPyKBDSdN4PFWJ5HhYglCXZ4frWkFfTdPf1mz5N5hMALh4FLKDLHit2KyOqpzy4LGkpslmmSQV9AzBKoRj1GEO_-FcLH 'TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgMTAuMDsgV2luNjQ7IHg2NDsgcnY6NjIuMCkgR2Vja28vMjAxMDAxMDEgRmlyZWZveC82Mi4w', rm: 'R0VU', d: 'TetCTvIHDo [0].appendChild(cpo); }()); </script> </body> </html>
2023-05-12 02:56:21	Netblock Membership	No	RIPE	0	0	2	0	None	87.248.157.0/24
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	29	0	2	0	None	https://funny.battleb0t.xyz/
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:5D:96:FD)
2023-05-12 03:09:00	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.94
2023-05-12 02:48:34	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'capec_id': None, u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"185.199.110.153:80"\n "1 type "UTF-8 Unicode text with very long lines"- [targetUID: N/A]\n "bootstrap-icons_1_.woff" has type "Web Open Font Format TrueType l u'https://attack.mitre.org/techniques/T1071/001', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.001', "SUIDMmicrosoft.com/92163934606464310276912834768846310275 74*SRCHDAF=NOFORMmicrosoft.com/10243323789440310856102797135723093874 3*SRCHU
2023-05-12 03:42:55	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	abuse@world4you.com
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	NH-NEW (Net ID: 00:01:21:31:EF:1C)
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	3	0	None	Turkey
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	mike1 (Net ID: 00:01:71:0A:05:C5)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	redwood (Net ID: 00:01:38:85:C1:F8)
2023-05-12 02:55:21	Netblock Membership	No	Censys	6	0	3	0	None	207.154.224.0/20
2023-05-12	Internet Name -	No	DNS Resolver	0	0	2	0	None	cpanel.ayhu.xyz

03:03:16	Unresolved								
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:b6:39:33:af:de:1e:32:f3:fc:2e:76:dc:bc:08:51:86:10 Signature Algorithm: sha256Wi 2023 GMT Extensions: none Signature : ecdsa-with-SHA256 30:46:02:21:00:87:F6:3C:B2:E0:C2:7B:F4:59:32:49: FF:84:EE:E1:AC:5D:A1:7E:84:DE
2023-05-12 02:56:52	Internet Name	No	DNS Resolver	0	0	3	0	None	nuke.battleb0t.xyz
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 03:11:15	Physical Coordinates	No	AbstractAPI	0	0	2	0	None	37.751, -97.822
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	HackerOne (Category: tech) https://hackerone.com/login
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.230): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:587
2023-05-12 02:54:41	Physical Location	No	Censys	1	0	3	0	None	North Charleston, South Carolina, 29418, United States, North America
2023-05-12 02:44:30	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Bootstrap
2023-05-12 02:44:30	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 02:58:25	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\HKEY_LOCAL_MACHINE_SOFTWARE_Microsoft_Speech_OneCore_Voices_Tokens_MSTTS_V110_enUS_MarkM_Mutex"\n "Local\\ChromeProcessSinglet 00000000-00007524]\n "f_00023e" has type "gzip compressed data from Unix original size modulo 2^32 327190"- Location: [%LOCALAPPDATA%\ compressed data from FAT filesystem (MS-DOS OS/2 NT) original size modulo 2^32 37080"- [targetUID: N/A]\n "LOG" has type "ASCII text"- u'threat_level': 1, u'type': 8, u'description': u'"widevinecdm.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"-
2023-05-12 02:54:44	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H04J1V5ZEHVH006E5VV5HBN1 Date: <REDACTED> Content-Length: 0
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	default (Net ID: 00:0D:88:94:94:59)
2023-05-12 02:45:01	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'CA', u'country_tld': u'.us', u'ip': u'185.199.109.153', u'currency_name': u'Dollar', u'currency': u'USD', u'country
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	tsunami (Net ID: 00:0D:29:AC:D0:D0)
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.11): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	My Passport (2.4 GHz) - 0772ED (Net ID: 00:00:C0:07:72:ED)
2023-05-12 02:53:42	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "Via": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary":
2023-05-12 03:11:07	Physical Coordinates	No	OpenStreetMap	90	0	4	0	None	37.7813933,-122.3918002
2023-05-12 03:32:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.8:8080
2023-05-12 02:53:10	Raw Data from RIRs	No	Tool - WAFW00F	1	0	3	0	None	[{"url": "https://vscode.battleb0t.xyz", "firewall": "Cloudflare", "detected": true, "manufacturer": "Cloudflare Inc."}, {"url": "http
2023-05-12 03:13:04	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [001328.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:54:54	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2a06:98c1:3121::/48
2023-05-	Open TCP	No	Pulsedive	0	0	2	0	None	185.199.109.153:443

12 02:47:27	Port								
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-ray: 7c5f8c5e7988238a-EWR
2023-05-12 02:54:21	Web Content Type	No	Web Spider	0	0	5	0	None	text/css
2023-05-12 02:58:51	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': "7423F88C7F265F0DEFC08EA88C3BDE45_D975BBA8033175C8D112023D8A7A8AD6" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptne 11:28:28)\n URL: https://zoommeetingbackgrounds.com/ (AV positives: 1/88 scanned on 09/21/2022 11:06:42)\n URL: https://rad-malabi-562 u'total_signatures': 6, u'image_base': None, u'error_origin': None, u'ssdeep': u'Unknown', u'entrypoint_section': None, u'md5': u'75dd
2023-05-12 03:41:52	Operating System	No	Censys	0	0	3	0	None	Microsoft Windows
2023-05-12 02:53:15	IP Address	No	Mnemonic PassiveDNS	0	0	1	0	None	172.67.168.252
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	3	0	None	36459
2023-05-12 02:46:32	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 1, u'threat_level': 0, u'type': 7, u'description': u'"api.k8slens.dev"'}, {u'category': u'Installation/Persistence', u'origin': u'Bina Data\\Crashpad\\settings.dat]- [targetUID: 00000000-00003984]\n "Last Browser" has type "data"- [targetUID: N/A]\n "6d3ef7fa-ecc8-4cf2 "www.principledtechnologies.com},{applied_policy:block,domain:web.basemark.com},{applied_policy:block,domain:mozilla.github.io},{appli None, u'relevance': 3, u'threat_level': 1, u'type': 2, u'description': u'Potential IP "1.0.0.23" found in string "%LOCALAPPDATA%\\Micr
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:03:10:83)
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+14806242599
2023-05-12 03:08:53	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.137
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AWildAndAnUntamedThing (Net ID: A0:8E:78:0F:4D:DE)
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/fredo.PNG
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.103): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:09:50	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	83.170.74.34.bc.googleusercontent.com
2023-05-12 02:59:11	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur file "urlblockindex_1_.bin" as clean (type is "data")\n Antivirus vendors marked dropped file "TarFDEF.tmp" as clean (type is "data")' "\\Sessions\\1\\BaseNamedObjects\\IsoScope_b78_IESQMMUTEX_0_331"\n "\\Sessions\\1\\BaseNamedObjects\\{66D0969A-1E86-44CF-B4EC-3806DDDA Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776 [targetUID: 00000000-00002936]\n "~DF9E4F20B7A536AEA1.TMP" has type "data"- Location: [%TEMP%\\~DF9E4F20B7A536AEA1.TMP]- [targetUID: 0
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	TexasTech94 (Net ID: 8C:3B:AD:4D:21:5C)
2023-05-12 03:23:44	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.17:80
2023-05-12 02:46:50	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 03:03:55	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	scoop.sh
2023-05-12 02:54:18	Web Content	No	Web Spider	0	0	4	0	None	body{ padding-top:70px; } .jumbotron{ color: #2c3e50; background-color: #ecf0f1; } .navbar-inverse{ color: #2c3e50; } .navbar-inverse
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_phone-2 (Net ID: 00:0C:E6:8A:9F:66)
2023-05-	Internet	No	DNS Resolver	0	0	2	0	None	panel.battleb0t.xyz

12 02:56:55	Name								
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	sflan47 (Net ID: 00:02:6F:08:21:E6)
2023-05-12 02:55:21	Software Used	Yes	Censys	0	0	3	0	None	OpenBSD OpenSSH 8.9p1
2023-05-12 02:44:30	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi2.battleb0t.xyz
2023-05-12 03:03:55	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	akashpmani.github.io
2023-05-12 02:54:07	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	4	0	2	0	None	Go Daddy, LLC
2023-05-12 03:31:32	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@resellercamp.com
2023-05-12 02:53:52	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-11T23:53:52.386Z", "ip": "2606:50c0:8003::153", "location_updated_at": "2023-05-08T14:21:40.589738Z", "au 23T09:37:19.694810939Z"}, "bbs.codecrh.com": {"record_type": "CNAME", "resolved_at": "2023-03-22T17:22:29.106820702Z"}, "kbau.dev": {" "resolved_at": "2023-03-21T00:21:54.271513621Z"}, "www.hiennguyen.dev": {"record_type": "CNAME", "resolved_at": "2023-03-07T12:59:42.4 {"record_type": "CNAME", "resolved_at": "2023-05-01T16:17:39.668319874Z"}, "shop4data-ui.docs.collibra.dev": {"record_type": "CNAME", 08T15:50:22.533060749Z"}, "www.coltonfalkner.dev": {"record_type": "CNAME", "resolved_at": "2023-03-22T19:22:40.169282211Z"}, "andress
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:CF:BB:35)
2023-05-12 02:46:54	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', ""primalharvest.com"," (Source: wallet-checkout-eligible-sites-pre-stable.json, Indicator: "arvest.com")'}, {u'category': u'Installati [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Cache\\Cache_Data\\f_00023e]- [targetUID: 00000000-00004772]\n "README.md" has t Related', u'origin': u'File/Memory', u'identifier': u'string-169', u'name': u'Found mail related domain names', u'attck_id_wiki': u'ht
2023-05-12 03:18:49	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Rotated 180 @ 18}
2023-05-12 03:35:46	Malicious Co-Hosted Site	Yes	OpenDNS	0	0	3	0	None	Blocked by OpenDNS [000.lt]
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:25:19	Internet Name	No	DNS Brute-forcer	0	0	2	0	None	nwapi2.battleb0t.xyz
2023-05-12 03:09:44	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	130.97.148.34.bc.googleusercontent.com
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom (Net ID: 00:01:38:A4:44:3A)
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.189): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:27	Open TCP Port Banner	No	Censys	0	0	4	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H04XFP518R0GMRXREDYN35MZ Date: <REDACTED> Content-Length: 0
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	TOMTSSID (Net ID: 00:02:2D:39:9A:88)
2023-05-12 03:32:19	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.10:80
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	0	0	1	0	None	CN=nwapi.battleb0t.xyz

2023-05-12 03:15:36	Physical Location	No	ipstack	0	0	2	0	None	Colombia
2023-05-12 03:09:44	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	128.97.148.34.bc.googleusercontent.com
2023-05-12 03:09:13	Affiliate - IP Address	No	DNS Look-aside	2	0	3	0	None	207.154.228.167
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	iz-wpa (Net ID: 00:01:8E:1A:64:A6)
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.225): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:58	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0101dd.github.io
2023-05-12 02:54:38	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	5	0	2	0	None	+74955801111
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.170): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SLK-Routers_091850 (Net ID: 00:02:2A:09:18:50)
2023-05-12 02:53:12	Web Technology	No	Tool - WAFW00F	0	0	3	0	None	None None
2023-05-12 02:54:21	Linked URL - Internal	No	Web Spider	2	0	3	0	None	http://vscode.battleb0t.xyz/
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Catwoman (Net ID: 00:14:5C:89:45:BC)
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Persistent_Auth": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Connection": "DISPLAY_UTF8", "Se
2023-05-12 03:10:18	Malicious IP on Same Subnet	Yes	VoIPBL OpenPBX IPs	0	0	4	0	None	VOIPBL Publicly Accessible PBX List [34.74.160.0/20] http://www.voipbl.org/update
2023-05-12 03:13:05	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [002evapey.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:45:48	Physical Coordinates	No	AbstractAPI	91	0	2	0	None	41.8781, -87.6298
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Rock Chalk (Net ID: 00:01:95:08:D8:04)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=5wRiK8by2KiigHlJJ8noI6lNWOYgr9ak0HIrPyPmGPMwmKjHbETJvR65
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Flickr (Category: images) https://www.flickr.com/photos/Altpapier/
2023-05-12 03:10:10	Malicious IP on Same Subnet	Yes	VoIPBL OpenPBX IPs	0	0	3	0	None	VOIPBL Publicly Accessible PBX List [185.199.109.0/24] http://www.voipbl.org/update
2023-05-12 02:45:10	Internet Name	No	Hybrid Analysis	0	0	1	0	None	kekw.battleb0t.xyz
2023-05-12 02:44:26	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:09:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2023-05-12 02:45:45	Physical Coordinates	No	AbstractAPI	0	0	2	0	None	37.751, -97.822
2023-05-	SSL	No	Certificate	0	0	1	0	None	

12 02:44:37	Certificate - Raw Data		Transparency						Certificate: Data: Version: 3 (0x2) Serial Number: 03:ad:f5:1d:5c:40:76:9e:09:db:d3:8c:1d:cb:38:82:95:b4 Signature Algorithm: sha256Wi none Signature : ecdsa-with-SHA256 30:44:02:20:4A:29:32:04:7E:83:C8:E3:CA:74:E8:65: A8:E7:72:FB:F7:EC:02:C4:CA:2A:00:42:62:DC:2B:A5: 4
2023-05-12 03:01:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.132): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:46	Physical Location	No	AbstractAPI	0	0	2	0	None	Chantilly, Virginia, 20151, United States, North America
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	RTL8186-GW (Net ID: 00:0E:E8:DC:15:E1)
2023-05-12 02:54:21	Web Content	No	Web Spider	3	0	3	0	None	<!DOCTYPE html> <!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]--> <!--[if IE 7]> <html class="no-js ie7 oldie success">Working <h2 class="text-3xl font-normal leading-1.3 mb-4">What can I do?</h2> <h3 class="text-15 font-semibold mb-2">If you
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	referrer-policy: strict-origin-when-cross-origin
2023-05-12 02:53:32	Open TCP Port	No	Censys	0	0	2	0	None	185.199.111.153:80
2023-05-12 02:46:00	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': u'htt Windows 2000/XP setup 62582 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%LOCALAPPDATA%\\ 5a43ee094dc33438cd19.js.LICENSE.txt */(window.webpackJsonp=window.webpackJsonp||[]).push([[0],{+Ewk:function(e,t,n){use strict;Object.
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	1	2	0	None	5.5.5-10.5.19-MariaDB
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:03:2F:06:53:C3)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=jsIMdWNoCwdQGyyZGyYA%2Bk%2F%2FuxOwhAu2H4z%2BlgqTotxGWPo8
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.227): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:28:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.144:443
2023-05-12 02:50:40	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_i Document Cannot read section info"- [targetUID: N/A]\n "style_1_.css" has type "assembler source ASCII text"- [targetUID: N/A]\n "_DEB u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relevance': 3, u'threat_level': 0, u'type': 2, u'de
2023-05-12 02:51:04	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis Traffic', u'identifier': u'network-0', u'name': u'Contacts domains', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u "PNG image data 640 x 480 8-bit colormap non-interlaced" and extension "png"\n "logo_1_.png" has type "PNG image data 329 x 88 8-bit/c [targetUID: N/A]\n "logo_1_.png" has type "PNG image data 329 x 88 8-bit/color RGBA non-interlaced"- [targetUID: N/A]\n "RecoveryStore [targetUID: N/A]\n "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has type "MS Windows icon resource - 1 icon 32x32 32 bits/pixel
2023-05-12 02:46:40	Physical Location	No	Fraudguard	0	0	2	0	None	United States, California, San Francisco
2023-05-12 03:19:17	Web Framework	No	Web Framework Identifier	0	0	3	0	None	jQuery
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.229): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:50:56	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"185.199.108.153:80"\n "185.199.108.153:443"\n "45.57.90. u'binary-56', u'name': u'Drops files with image extension', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_l [targetUID: N/A]\n "fa-solid-900_1_.eot" has type "Embedded OpenType (EOT) Font Awesome 5 Pro Solid family"- [targetUID: N/A]\n "AAAAB type "Web Open Font Format TrueType length 66376 version 1.1"- [targetUID: N/A]\n "pxiByp8kv8JHgFVrLEj6V1g_1_.woff" has type "Web Open
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.212): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00089.github.io
2023-05-	Raw Data	No	Hybrid Analysis	0	0	2	0	None	

12 02:52:26	from RIRs								[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', "logo_1_.png" has type "PNG image data 329 x 88 8-bit/color RGBA non-interlaced" and extension "png"'}, {u'category': u'Installation/P 2000x1125 components 3"- [targetUID: N/A]\n "tab-content-2-1_1_.png" has type "PNG image data 561 x 379 8-bit/color RGBA non-interlace N/A]\n "index_1_.js" has type "ASCII text"- [targetUID: N/A]\n "CUDEXGN3.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\
2023-05-12 02:45:57	Physical Location	No	AbstractAPI	0	0	4	0	None	Ashburn, Virginia, 20149, United States, North America
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00ty.github.io
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.135): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Horizontal (normal) @ 18}
2023-05-12 02:52:59	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	None None
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ToddNet (Net ID: 00:01:24:F2:5E:43)
2023-05-12 02:54:19	HTTP Status Code	No	Web Spider	0	0	2	0	None	200
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Vthokies (Net ID: 00:0C:41:8A:86:76)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:F0:AC:63:DA)
2023-05-12 02:59:52	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	fondon@fondon.org
2023-05-12 02:59:47	Affiliate - Domain Whois	No	Whois	4	0	3	0	None	Domain Name: CLOUDFLARE.COM Registry Domain ID: 1542998887_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.cloudflare.com Registrar URL: ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information abou Status: serverupdateprohibited https://icann.org/epp#serverupdateprohibited Domain Status: clientupdateprohibited https://icann.org/ep abuse@cloudflare.com Registrar Abuse Contact Phone: +1.4153197517 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.i
2023-05-12 02:56:53	Internet Name	No	DNS Resolver	0	0	4	0	None	panel.battleb0t.xyz
2023-05-12 02:50:15	Internet Name	No	DNS Resolver	0	0	2	0	None	funny.battleb0t.xyz
2023-05-12 02:55:11	Operating System	No	Censys	0	0	2	0	None	linux
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.189): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:28:03	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [185.199.111.133] https://www.virustotal.com/en/ip-address/185.199.111.133/information/
2023-05-12 03:43:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	87.248.157.79:80
2023-05-12 02:55:44	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:c7:00:14:21:71:88:e2:18:10:f8:e3:ee:d1:89:37:10:7b Signature Algorithm: sha256Wi 59:33:d8:1c:63:9a:1f:c2:49:d5:16:41:55:df:2b:23:f2:e9: b3:cc:0e:45:14:b2:fe:94:7d:98:ee:51:3e:fe:8e:d3:e9:26: e4:d9:13:e1:5b:9d:72:18:
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless (Net ID: 00:01:36:03:67:CB)
2023-05-12 02:53:42	Open TCP Port	No	Censys	0	0	2	0	None	185.199.109.153:80
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.66): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	lcgteach (Net ID: 00:0B:86:22:0F:30)

2023-05-12 03:01:32	Web Server	No	Tool - WhatWeb	0	0	3	0	None	cloudflare
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: <REDACTED> Cache-Control: no-cache, no-store, must-re
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/carti_1.jpg
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	hoenes1 (Net ID: 00:0C:F6:59:F5:B4)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATTY5cg8s2 (Net ID: 88:96:4E:7F:0D:00)
2023-05-12 03:00:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.39): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	fotoosman (Net ID: 00:02:CF:D7:57:CF)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=FXQU88yRDhEJMx%2FdYM%2F9ZMluhZXagjhG95IApBIpm7WqxobZm4Cc
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:FD:64:31)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	curealty (Net ID: 00:0C:41:49:32:21)
2023-05-12 02:56:23	Netblock Membership	No	RIPE	0	0	3	0	None	46.101.128.0/17
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.178): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:57	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00xkhaled.github.io
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	PanPanLePanda (Net ID: 00:00:00:00:27:69)
2023-05-12 02:49:57	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relev "be201c28-8966-423a-a934-6abe0eafb4e2.tmp" has type "gzip compressed data from FAT filesystem (MS-DOS OS/2 NT) original size modulo 2^ u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1573', u'relevance': 1, u'threat_level': 0, u'type': 7, u'de available'}], u'threat_level': 2, u'size': 102435, u'job_id': u'63ee0a00ee7f7e33101b746d', u'target_url': None, u'interesting': False,
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	7722 4671 (Net ID: 00:00:C5:FD:29:7C)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	F3 (Category: social) https://f3.cool/ayhu
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Hubski (Category: social) https://hubski.com/user/login
2023-05-12 03:01:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.128): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:47:51	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 50, u'search_terms': [{u'id': u'host', u'value': u'185.199.110.153'}], u'result': [{u'environment_id': 160, u'job_id': u'64 u'f6b87534e4ad728b3efdf794897f8badfaa12c074108bc1dc415c6a8c05a5221', u'type': None, u'type_short': u'url', u'size': 95}, {u'environmen u'threat_score': 100, u'verdict': u'suspicious', u'submit_name': u'sample.url', u'sha256': u'c476745cfb34866457803744a7898a71b4ea6fc62 u'environment_description': u'Windows 10 64 bit', u'threat_score': None, u'verdict': u'no specific threat', u'submit_name': u'sample.u u'environment_description': u'Windows 7 32 bit', u'threat_score': None, u'verdict': u'no specific threat', u'submit_name': u'sample.ur
2023-05-12 02:45:32	Raw Data from RIRs	No	PhishStats	0	0	2	0	None	[{u'page_text': u' ', u'domain': None, u'virus_total': None, u'n_times_seen_ip': None, u'abuse_contact': None, u'ip': u'185.199.108.15
2023-05-12 03:17:44	Account on External Site	No	Account Finder	0	0	1	0	None	Trello (Category: social) https://trello.com/_BattleB0t_
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet (Net ID: 00:01:36:2D:BB:B4)

2023-05-12 03:01:30	Web Technology	No	Tool - WhatWeb	0	0	2	0	None	HTML5
2023-05-12 02:50:44	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:03:e6:77:f0:fb:1d:de:0e:93:d2:d9:e5:40:98:fb:b1:42 Signature Algorithm: ecdsa-wi
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0036labs.github.io
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	GitHub (Category: coding) https://github.com/Battleb0t
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Maingau (Net ID: 00:02:2D:64:E2:6A)
2023-05-12 02:44:05	Web Technology	No	Tool - WAFW00F	0	0	1	0	None	None None
2023-05-12 02:53:32	Open TCP Port	No	Censys	0	0	2	0	None	185.199.111.153:443
2023-05-12 03:12:58	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	2	0	None	OpenPhish [github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	DPRWirelessScottsdale (Net ID: 00:02:6F:FD:3F:B2)
2023-05-12 02:44:07	Software Used	Yes	Tool - Wappalyzer	0	0	1	0	None	Fastly
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:2095
2023-05-12 03:16:26	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'16', u'country_tld': u'.tr', u'ip': u'87.248.157.102', u'currency_name': u'Lira', u'currency': u'TRY', u'country_po
2023-05-12 02:44:18	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	2	0	None	C=US,ST=California,L=San Francisco,O=GitHub\, Inc.,CN=*.github.io
2023-05-12 03:01:08	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.110.133:443
2023-05-12 03:13:09	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [01-scripts.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:45:04	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'CA', u'country_tld': u'.us', u'ip': u'2606:50c0:8000::153', u'currency_name': u'Dollar', u'currency': u'USD', u'cou
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	F3 (Category: social) https://f3.cool/ayshoo
2023-05-12 02:44:23	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	x-fastly-request-id: 88b13ec8ddf02c1379830d22f861ddb1826456ec
2023-05-12 03:00:46	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.62): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.58): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Apple Network 2159fc (Net ID: 00:02:2D:21:59:FC)
2023-05-12 03:04:46	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	bowman's base (Net ID: 00:02:2D:21:D5:B7)
2023-05-12 02:59:59	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	madler@alumni.caltech.edu

2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/random_2.jpeg
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	House (Net ID: 00:02:2D:09:FC:0D)
2023-05-12 03:00:59	Malicious Affiliate	Yes	VXVault.net	0	1	3	0	None	VXVault Malicious URL List [cdn-185-199-109-153.github.com] http://vxvault.net/URL_List.php
2023-05-12 03:04:46	Hosting Provider	No	Hosting Provider Identifier	0	0	3	0	None	Cloudflare Inc: https://www.cloudflare.com/
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.45): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:01:24:F2:E2:35)
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.246): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:25	Internet Name	No	DNS Resolver	1	0	2	0	None	pics.battleb0t.xyz
2023-05-12 02:55:01	Netblock Membership	No	Censys	347	0	2	0	None	188.114.96.0/24
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Periscope (Category: video) https://www.periscope.tv/ayhu
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	CLKDevices (Net ID: 00:01:B2:39:20:00)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	dinamo (Net ID: 00:02:CF:8C:8A:82)
2023-05-12 02:59:51	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	contact@ikerguerrero.dev
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-served-by: cache-lga21982-LGA
2023-05-12 03:11:20	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'city': u'Frankfurt am Main', u'security': {u'is_vpn': False}, u'city_geoname_id': 2925533, u'region_geoname_id': 2905330, u'country
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Calendy (Category: misc) https://calendly.com/ayhu
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SurfandSip (Net ID: 00:02:2D:03:87:91)
2023-05-12 03:17:34	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: AYSHU.XYZ Registry Domain ID: D346635612-CNIC Registrar WHOIS Server: whois.resellercamp.com Registrar URL: https://idweb (2) not to store or reproduce this data in any way, (3) not to use any high-volume, automated, electronic processes to obtain data fro solicitations via direct mail, electronic mail, or by telephone. The compilation, repackaging, dissemination or other use of this data
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:05:12	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.150): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.19): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.221): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	TB Proprietary Channel. Bc (Net ID: 00:04:32:1C:D9:49)

2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	bursa (Net ID: 00:08:5C:7B:38:A1)
2023-05-12 02:45:31	Physical Location	No	MetaDefender	0	0	2	0	None	San Francisco, United States
2023-05-12 03:03:27	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	7	0	None	Iceland
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.218): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SENSEO2 (Net ID: 00:01:24:F2:7F:EC)
2023-05-12 02:45:31	Malicious IP Address	Yes	PhishStats	0	1	2	0	None	Phishstats [185.199.111.153]
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Verorouter5 (Net ID: DC:EF:09:A7:2C:2E)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Amethyst (Net ID: 00:01:21:30:76:B8)
2023-05-12 02:52:12	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'"209.94.90.1:443"\n "185.199.108.153:443"\n "69.16.175.42:443"\n "52.155.62.95:443"'}, {u'category': u'General', u'origin': u'Networ u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relevance': 1, u'threat_level': 0, u'type': 6, u'de [targetUID: N/A]\n "CabBE9.tmp" has type "data"- Location: [%TEMP%\\CabBE9.tmp]- [targetUID: 00000000-00003580]\n "font-awesome_1_.css 00000000-00003580]\n "search_2_.json" has type "JSON data"- [targetUID: N/A]\n "Q2MIS3ZH.txt" has type "ASCII text"- Location: [%APPDA
2023-05-12 03:19:24	Blacklisted IP Address	Yes	UCEPROTECT	0	1	3	0	None	UCEPROTECT - Level 2 (some false positives) (104.196.30.220)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	TOMTSSID (Net ID: 00:02:2D:39:9C:6E)
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Spotify (Category: music) https://open.spotify.com/user/ayshoo
2023-05-12 02:44:13	Raw Data from RIRs	No	Certificate Transparency	16	0	1	0	None	[{u'not_after': u'2023-08-02T19:22:48', u'not_before': u'2023-05-04T19:22:49', u'issuer_ca_id': 183267, u'name_value': u'nwapi2.battle u'entry_timestamp': u'2023-04-24T05:50:12.941', u'id': 9221147142}, {u'not_after': u'2023-07-23T03:43:00', u'not_before': u'2023-04-24 u'038880c39ce1f505d4ceeba7b88b966916e7', u'entry_timestamp': u'2023-03-27T14:22:33.221', u'id': 9002142810}, {u'not_after': u'2023-06- u'funny.battleb0t.xyz\npics.battleb0t.xyz', u'issuer_name': u"C=US, O=Let's Encrypt, CN=R3", u'common_name': u'funny.battleb0t.xyz', u 02-25T01:39:25', u'issuer_ca_id': 183267, u'name_value': u'battleb0t.xyz\nwww.battleb0t.xyz', u'issuer_name': u"C=US, O=Let's Encrypt,
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.20): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	PartyVan (Net ID: 00:00:C0:16:5F:81)
2023-05-12 02:46:05	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniq fill="currentColor" fill-rule="evenodd" clip-rule="evenodd" d="M27.8 14.1C27.8 14.1 27.604 12.692 27.005 12.072C26.319 11.339 25.559 1 file "TarD0B4.tmp" as clean (type is "data")\n Antivirus vendors marked dropped file "TarD065.tmp" as clean (type is "data")\n Antivir 72_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUID: N/A]\n "urlblockindex_1_.bin" has type "data"- [targetUID: N/A]\
2023-05-12 03:03:20	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:24:51	Country	No	Country Name Extractor	0	0	7	0	None	United States
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomF2385E (Net ID: 00:0C:F6:F2:38:5E)

2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	permissions-policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Led Zeppelin (Net ID: 00:01:24:F1:B5:5B)
2023-05-12 03:04:46	Hosting Provider	No	Hosting Provider Identifier	0	0	3	0	None	Google App Engine: https://cloud.google.com/appengine
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	LALOFT (Net ID: 00:01:95:7C:7F:2C)
2023-05-12 02:44:30	Internet Name	No	DNS Resolver	0	0	2	0	None	www.battleb0t.xyz
2023-05-12 02:53:15	IPv6 Address	No	Mnemonic PassiveDNS	0	0	1	0	None	2606:50c0:8002::153
2023-05-12 03:00:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha2-256-etm@openssh.com
2023-05-12 02:52:56	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'network-1', u'name': u'Contacts server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'in u'identifier': u'api-242', u'name': u'Write files', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_level_hum with very long lines"- [targetUID: N/A]\n "RecoveryStore._47750809-EA4A-11ED-855A-0800272BB261_.dat" has type "Composite Document File 00000000-00002444]\n "Z6E6M77S.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\Z6E6M77S.txt]- [targetUI
2023-05-12 03:08:46	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.217
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha2-256-etm@openssh.com
2023-05-12 03:24:29	Company Name	No	Company Name Extractor	0	0	4	0	None	Netlify\, Inc
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Cytoid (Category: gaming) https://cytoid.io/profile/login
2023-05-12 02:57:37	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "com.adobe.acrobat.rna.RdrCefBrowserLock.DC"\n "\\Sessions\\1\\BaseNamedObjects\\com.adobe.acrobat.rna.RdrCefBrowserLock.DC"'}, {u'cat u'informative', u'capec_id': u'CAPEC-163', u'attck_id': u'T1566.002', u'relevance': 3, u'threat_level': 0, u'type': 2, u'description': "https://spacenews.com/wyvern-raises-7-million-for-hyperspectral-imaging-constellation/" (Based on: "f8a9f4126162303dad458d4dba0362949 --primordial-pipe-token=CBBE6F137B53EB05D1E24337 ..." (UID: 00000000-00002080)\n Spawned process "iexplore.exe" with commandline "SCOD
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Mastodon-API (Category: social) https://mastodon.social/api/v2/search?q=Altpapier
2023-05-12 02:55:21	Physical Location	No	Censys	0	0	3	0	None	Frankfurt am Main, Hesse, 60306, Germany, Europe
2023-05-12 03:23:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.7:443
2023-05-12 03:08:53	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.66
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	WordPress Support (Category: blog) https://wordpress.org/support/users/login/
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	NH-NEW (Net ID: 00:01:21:30:F0:43)
2023-05-12 02:53:39	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 02:57:21	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:4a:0e:8c:1b:d3:a5:34:69:b6:32:8e:46:29:d8:95:17:d9 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 40:6C:
2023-05-12 02:56:15	Non-Standard	No	Strange Header Identifier	0	0	6	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}

	HTTP Header								
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	lichess (Category: gaming) https://lichess.org/@/Altpapier
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	1	0	2	0	None	00rz.com
2023-05-12 02:44:12	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	kekw.battleb0t.xyz:443
2023-05-12 03:03:35	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:09:56	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom (Net ID: 00:0C:F6:26:FB:66)
2023-05-12 02:55:21	Operating System	No	Censys	0	0	3	0	None	Ubuntu Linux
2023-05-12 02:57:00	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "\\Sessions\\1\\BaseNamedObjects\\IsoScope_b54_IESQMMUTEX_0_519"\n "\\Sessions\\1\\BaseName Method: POST\nAccess-Control-Request-Headers: content-type, x-monorail-edge-event-created-at-ms, x-monorail-edge-event-sent-at-ms, x-m [targetUID: 00000000-00003472]\n Dropped file: "PH9G2FHJ.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\PH9G2FHJ.txt]- [tar Scalable Vector Graphics image"- [targetUID: N/A]\n "fa-brands-400_1_.eot" has type "Embedded OpenType (EOT) Font Awesome 5 Brands Reg
2023-05-12 02:54:13	Linked URL - Internal	No	Web Spider	2	0	1	0	None	https://ayhu.xyz/
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	infoworld (Net ID: 00:02:2D:01:DD:9B)
2023-05-12 03:41:58	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	domixo-hosting.de
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cf-version: 1432-d48eaba
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F1:C3:85)
2023-05-12 02:49:14	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 1, u'threat_level': 0, u'type': 7, u'description': u'"api.k8slens.dev"'}, {u'category': u'Installation/Persistence', u'origin': u'Bina Data\\Crashpad\\settings.dat]- [targetUID: 00000000-00003984]\n "Last Browser" has type "data"- [targetUID: N/A]\n "6d3ef7fa-ecc8-4cf2 "www.principledtechnologies.com},{applied_policy:block,domain:web.basemark.com},{applied_policy:block,domain:mozilla.github.io},{appli None, u'relevance': 3, u'threat_level': 1, u'type': 2, u'description': u'Potential IP "1.0.0.23" found in string "%LOCALAPPDATA%\\Micr
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	referrer-policy: same-origin
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	4	0	2	0	None	GoDaddy.com, LLC
2023-05-12 03:00:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.41): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:38	Netblock Membership	No	Censys	0	0	3	0	None	172.67.160.0/20
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SurfandSip (Net ID: 00:02:2D:03:87:91)
2023-05-12 02:55:26	Social Media Presence	No	Social Network Identifier	0	0	5	0	None	Github: https://github.com/login/oauth/authorize?client_id=42db428b279076117521&redirect_uri=https://golhub.cloudflareaccess.com/cdn-c
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	GortzenWIFI (Net ID: 00:11:50:36:95:E1)
2023-05-12 03:32:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.14:80

2023-05-12 03:00:57	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	01-edu.github.io
2023-05-12 02:54:16	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://oldfluid.battleb0t.xyz/logo.png
2023-05-12 03:18:06	URL (Purely Static)	No	Page Information	0	0	3	0	None	http://nwapi2.battleb0t.xyz
2023-05-12 03:03:18	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12 02:55:21	Open TCP Port Banner	No	Censys	0	1	3	0	None	SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
2023-05-12 02:55:18	Operating System	No	Censys	0	0	3	0	None	Ubuntu Linux
2023-05-12 03:00:54	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.86): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.0): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:59	Physical Coordinates	No	AbstractAPI	0	0	3	0	None	41.8781, -87.6298
2023-05-12 02:50:53	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"185.199.108.153:443"\n "104.194.8.120:443"' "data")'}, {u'category': u'Unusual Characteristics', u'origin': u'Binary File', u'identifier': u'binary-56', u'name': u'Drops files wi u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relevance': 3, u'threat_level': 0, u'type': 8, u'de "RecoveryStore._88B090C0-D917-11E7-B67B-080027A49DD6_.dat" has type "Composite Document File V2 Document Cannot read section info"- [t
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.78): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:12	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.125): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Connectionpoint (Net ID: 00:01:E3:52:11:50)
2023-05-12 03:32:02	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.2:80
2023-05-12 02:54:20	Web Content	No	Web Spider	3	0	2	0	None	<!DOCTYPE html> <!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]--> <!--[if IE 7]> <html class="no-js ie7 oldie success">Working <h2 class="text-3xl font-normal leading-1.3 mb-4">What can I do?</h2> <h3 class="text-15 font-semibold mb-2">If you
2023-05-12 02:53:56	Open TCP Port	No	Censys	0	0	2	0	None	2606:50c0:8001::153:443
2023-05-12 02:54:07	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12 02:44:15	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	1	2	0	None	netlify.app
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cross-origin-resource-policy: same-origin
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	FriendFinder-X (Category: dating) https://www.friendfinder-x.com/profile/Altpapier
2023-05-12 03:23:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.3:8080
2023-05-12 03:03:20	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:03:27	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-cache-status: DYNAMIC

2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:74:92:0E:CC)
2023-05-12 02:45:50	Physical Coordinates	No	AbstractAPI	0	0	2	0	None	37.751, -97.822
2023-05-12 02:54:19	Web Content	No	Web Spider	3	0	2	0	None	<!DOCTYPE html> <html> <head> <meta charset="utf-8"> <meta http-equiv="Cache-Control" content="no-cache"> <meta name="viewport" conten middle { display: table-cell; vertical-align: middle; } .promo-content { width: 80vw; height: 80vh; max-width: 80vh; max-height: 80vw;
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00steveng.github.io
2023-05-12 02:54:03	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:02:26	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	HTTP/3
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_ipad (Net ID: 00:0C:E6:08:0C:05)
2023-05-12 03:23:02	Username	No	Account Finder	8	0	7	0	None	baptistevauthey
2023-05-12 03:03:24	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	000.ovh
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	freesound (Category: music) https://freesound.org/people/login/
2023-05-12 02:53:49	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Etag": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary"
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-resource-policy: same-origin
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.231): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:DB:1C:01)
2023-05-12 02:54:06	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': u'Windows Gui', u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_ "CreateDirectoryW" with parameter %APPDATA%\\Microsoft\\Windows\\Cookies (UID: 00000000-00002964)\n "Tibiamapsinstaller.exe" called "C "API-MS-WIN-DOWNLEVEL-SHLWAPI-L2-1-0.DLL" at base 73fe0000\n "Tibiamapsinstaller.exe" loaded module "DNSAPI.DLL" at base 73880000\n "T called "LoadLibrary" with a parameter API-MS-Win-Security-LSALookup-L1-1-0.dll (UID: 00000000-00002964)\n "Tibiamapsinstaller.exe" cal u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1106', u'relevance': 1, u'threat_level': 0, u'type': 6, u'de
2023-05-12 02:53:52	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	zzzzz (Net ID: 00:01:24:F0:3B:50)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	USR9111 (Net ID: 00:14:C1:3F:EF:1F)
2023-05-12 02:55:21	Software Used	Yes	Censys	0	0	3	0	None	openssh
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	4	0	None	Turkey
2023-05-12 02:46:50	Open TCP Port	No	SSL Certificate Analyzer	0	0	3	0	None	34.74.170.74:443
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX5515594BD (Net ID: 00:01:E3:55:94:BD)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless (Net ID: 00:01:36:03:62:55)
2023-05-	Blacklisted	Yes	Honeypot	0	0	3	0	None	

12 03:01:20	IP on Same Subnet		Checker						Honeypotproject (188.114.96.179): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WaveLAN Network VHome2B (Net ID: 00:02:2D:03:03:11)
2023-05-12 02:44:59	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'CA', u'country_tld': u'.us', u'ip': u'185.199.108.153', u'currency_name': u'Dollar', u'currency': u'USD', u'country
2023-05-12 03:08:54	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.75
2023-05-12 03:01:31	Web Server	No	Tool - WhatWeb	0	1	2	0	None	Netlify
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	Kongregate (Category: gaming) https://www.kongregate.com/accounts/Battleb0t
2023-05-12 02:50:16	Internet Name	No	DNS Resolver	0	0	2	0	None	pics.battleb0t.xyz
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	007hyno.github.io
2023-05-12 03:12:14	Affiliate - Domain Whois	No	Whois	4	0	6	0	None	Domain Name: AMCODEV.ME Registry Domain ID: D425500000016166846-AGRS Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://w rights reserved. Registry Operator reserves the right to modify these terms at any time. By submitting this query, you agree to abide ID: CR434510194 Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street:
2023-05-12 02:56:52	Internet Name	No	DNS Resolver	0	0	3	0	None	fluid.battleb0t.xyz
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sanctuary_Mixer (Net ID: 00:18:F8:CB:D4:48)
2023-05-12 03:01:14	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.132): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.196): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:2083
2023-05-12 02:54:22	HTTP Status Code	No	Web Spider	0	0	3	0	None	200
2023-05-12 02:59:04	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"68.142.107.4:80"\n "34.74.170.74:443"'}, {u'cat "Microsoft Cabinet archive data 4817 bytes 1 file"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\57C8EDB95DF3 u'description': u'"ScanWithAntiVirus" (Indicator: "antivirus")'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'ident u'File/Memory', u'identifier': u'string-3', u'name': u'Found potential URL in binary/memory', u'attck_id_wiki': None, u'threat_level_h
2023-05-12 02:59:50	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	madler@alumni.caltech.edu
2023-05-12 03:01:15	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.134): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:12:10	Affiliate Description - Category	No	DuckDuckGo	0	0	5	0	None	DShield , Cybercrime analytics.
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.236): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-to-1.github.io
2023-05-12 03:03:32	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-	Co-Hosted	No	SSL Certificate	0	0	2	0	None	

12 02:44:17	Site		Analyzer						githubusercontent.com
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.204): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ZyXEL (Net ID: 00:02:CF:98:55:20)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	x-nf-request-id: 01H06Y2Y8V02FJ2S9V869KY74K
2023-05-12 02:44:22	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 03:23:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.10:443
2023-05-12 03:03:36	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:54:48	HTTP Headers	No	Censys	0	0	3	0	None	{"Date": ["<REDACTED>"], "_encoding": {"Date": "DISPLAY_UTF8", "Content_Length": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "S
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	moxfield (Category: misc) https://www.moxfield.com/users/login
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	x-nf-request-id: 01H06Y2WPKRCCC7SJ49ZB68B31
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ASG (Net ID: 00:12:BF:FD:D5:8D)
2023-05-12 02:46:53	Internet Name	No	DNS Resolver	0	0	2	0	None	vscode.battleb0t.xyz
2023-05-12 02:54:27	Open TCP Port	No	Censys	0	0	4	0	None	2600:1f18:2489:8202::c8:443
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Collaborative intelligence - Collaborative intelligence characterizes multi-agent, distributed systems where each agent, human or mach
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	FUNK (Net ID: 00:02:2D:3A:A7:7B)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	fantastik (Net ID: 00:06:25:BE:90:75)
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/withat_1.jpg
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.228): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:10	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-11T19:39:54.906Z", "ip": "2606:4700:3031::6815:6a6", "location_updated_at": "2023-05-07T07:37:11.063836Z" "resolved_at": "2023-04-23T21:28:34.547869491Z"}, "rockspitmarsliga.tk": {"record_type": "AAAA", "resolved_at": "2023-05-09T21:26:55.5 {"record_type": "AAAA", "resolved_at": "2023-05-04T21:36:27.672632585Z"}, "www.proappsys.com": {"record_type": "CNAME", "resolved_at": "cpcalendars.menuin.pe": {"record_type": "AAAA", "resolved_at": "2023-03-16T07:00:36.539543312Z"}, "ftp.jogjacontemporary.net": {"reco 26T22:59:18.792128403Z"}, "www.cg.cncap.ca": {"record_type": "AAAA", "resolved_at": "2023-04-21T12:55:12.348140033Z"}, "www.meeturplan
2023-05-12 03:09:50	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	84.170.74.34.bc.googleusercontent.com
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	infoworld (Net ID: 00:02:2D:01:DD:9B)
2023-05-12 02:44:27	Internet Name	No	DNS Resolver	0	0	2	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:31:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	abuse@godaddy.com

2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	instructables (Category: hobby) https://www.instructables.com/member/login/
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cross-origin-opener-policy: same-origin
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	PowerDNS Authoritative Server 4.4.1
2023-05-12 02:55:50	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	{u'count': 20, u'search_terms': [{u'id': u'host', u'value': u'104.196.30.220'}], u'result': [{u'environment_id': 100, u'job_id': u'63f u'3a4368075604690b60a3d7a0a55c0749bf05c290c8d46d4d3958c4e135bf4089', u'type': None, u'type_short': u'url', u'size': 64}, {u'environmen u'submit_name': u'sample.url', u'sha256': u'61b1cc0537053e2876e4e2bd9e5bc874e980cda8bae7ae2039d9c02998a32562', u'type': None, u'type_s u'suspicious', u'submit_name': u'sample.url', u'sha256': u'da3e56c906f9dc5bfb98ea2091bd2edd31013446f1b533613d7ab1544cb46867', u'type': specific threat', u'submit_name': u'sample.url', u'sha256': u'9e255d1be44c24749101e3045b28e8f610869aa0e61723e6d6d258da1b22475c', u'typ
2023-05-12 03:32:04	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.3:80
2023-05-12 03:23:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.2:80
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	4	0	None	CloudFlare, Inc.
2023-05-12 03:09:57	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	2WIRE431 (Net ID: 00:02:2D:68:9D:A0)
2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.121
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.155): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:44	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["0"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ballpark (Net ID: 00:02:2D:3D:74:62)
2023-05-12 03:00:51	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.75): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Equiscript (Net ID: 00:18:0A:6F:96:37)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomCECF14 (Net ID: 00:0C:F6:CE:CF:14)
2023-05-12 03:18:46	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image ExifOffset': (0x8769) Long=90 @ 66, 'EXIF ComponentsConfiguration': (0x9101) Undefined=YCbCr @ 112, 'Image YCbCrPositioning':
2023-05-12 03:21:08	Account on External Site	No	Account Finder	0	0	2	0	None	Pinterest (Category: social) https://www.pinterest.com/dawidsulej/
2023-05-12 02:53:52	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:50c0:8003::/48
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.213): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-ray: 7c5f6071cb5443bc-EWR
2023-05-12 03:31:27	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	domains@hostex.lt
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.192): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	referrer-policy: same-origin

2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pannet-24 (Net ID: 00:01:8E:DA:59:C4)
2023-05-12 03:01:46	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.255): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BBHWIRELESS (Net ID: 00:00:C5:D7:60:F4)
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00steveng.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:23:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.2:443
2023-05-12 02:54:54	Open TCP Port	No	Censys	0	0	2	0	None	2a06:98c1:3121::1:80
2023-05-12 03:32:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.15:443
2023-05-12 03:08:45	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.210
2023-05-12 02:53:04	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	None None
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:443
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	PG Airnet (Net ID: 00:02:2D:27:B4:51)
2023-05-12 03:32:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.13:8443
2023-05-12 03:01:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.241): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:13:02	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0.crimson-perch.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:2095
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	onshome (Net ID: 00:0C:41:67:02:1F)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AIRTIES_RT-205 (Net ID: 00:12:BF:FD:D7:C4)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	devolo-000B3BEA35D8 (Net ID: 00:0B:3B:EA:35:D8)
2023-05-12 02:44:31	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	portainer.battleb0t.xyz
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	GOAT (Net ID: 00:00:C5:D3:87:1C)
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	000b000.github.io
2023-05-12 02:44:31	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3037::6815:470e
2023-05-	Blacklisted	Yes	Honeypot	0	0	3	0	None	

12 03:01:45	IP on Same Subnet		Checker						Honeypotproject (188.114.97.247): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:09	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.0:8443
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	homespies (Net ID: 00:06:25:63:06:A6)
2023-05-12 02:54:13	HTTP Headers	No	Web Spider	10	0	3	0	None	{"content-encoding": "gzip", "nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "referrer-policy": "same-o
2023-05-12 02:55:22	Linked URL - Internal	No	Google	0	0	1	0	None	https://battleb0t.xyz/
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom6E1FC8 (Net ID: 00:0C:F6:6E:1F:C8)
2023-05-12 02:44:11	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	1	0	None	github.com
2023-05-12 03:23:41	Account on External Site	No	Account Finder	0	0	8	0	None	ArtBreeder (Category: art) https://www.artbreeder.com/baptiste.vauthey
2023-05-12 02:45:32	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'SC', u'country_tld': u'.us', u'ip': u'34.148.97.127', u'currency_name': u'Dollar', u'currency': u'USD', u'country_p
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.7): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:40	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	HSTS
2023-05-12 02:54:00	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Instagram (Category: social) https://instagram.com/Altpapier
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Baur (Net ID: 00:0C:F6:67:34:C4)
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.215): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:11	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.1:8443
2023-05-12 03:09:49	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	80.170.74.34.bc.googleusercontent.com
2023-05-12 03:08:48	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.107
2023-05-12 02:50:50	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [104.21.6.166] https://www.virustotal.com/en/ip-address/104.21.6.166/information/
2023-05-12 02:56:56	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	portainer.battleb0t.xyz
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 03:41:52	Open TCP Port	No	Censys	0	1	3	0	None	45.131.109.53:3389
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.18): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:AA:8C:74:82)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ENHLG (Net ID: 00:01:36:5B:37:00)
2023-05-12	Blacklisted IP on Same	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.80): Search Engine Last Activity: 0 days ago Threat Level: 29

03:00:52	Subnet								
2023-05-12 03:16:23	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'NH', u'country_tld': u'.nl', u'ip': u'188.114.96.1', u'currency_name': u'Euro', u'currency': u'EUR', u'country_popu
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATT2fMx5Ja (Net ID: E0:22:04:69:C4:4A)
2023-05-12 03:32:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.11:8080
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	linksys (Net ID: 00:18:F8:E5:8F:A8)
2023-05-12 02:53:56	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "Via": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary":
2023-05-12 03:01:10	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.124): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	MCUUID (Minecraft) (Category: gaming) https://mcuuid.net/?q=Altpapier
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	rtsmith134 (Net ID: 00:01:24:F0:37:68)
2023-05-12 02:53:04	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	Cloudflare Inc. Cloudflare
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.197): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AIRTIES (Net ID: 00:12:BF:3E:F2:BC)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	PLXDevices (Net ID: 00:06:66:30:03:AC)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cf-ray: 7c5f8c59d97743e3-EWR
2023-05-12 02:57:22	Co-Hosted Site	No	Certificate Transparency	0	0	1	0	None	sni.cloudflaressl.com
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	memrise (Category: hobby) https://app.memrise.com/user/ayhu/
2023-05-12 03:32:04	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.3:8080
2023-05-12 03:15:35	Web Content Language	No	Language Detector	0	0	2	0	None	English
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Lang Sky Harbor (Net ID: 00:03:93:E9:7A:05)
2023-05-12 03:08:40	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	185.199.109.154
2023-05-12 02:46:38	Netblock Membership	No	RIPE	2	0	3	0	None	34.74.160.0/20
2023-05-12 03:03:40	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:54:20	Open TCP Port Banner	No	Censys	0	0	4	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H06PCVJ4HBKTDMM1V2TTSTEZ Date: <REDACTED> Content-Length: 0
2023-05-12 02:54:15	Linked URL - Internal	No	Web Spider	7	0	2	0	None	https://nwapi2.battleb0t.xyz/
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AIRTIES (Net ID: 00:12:BF:5F:88:E4)

2023-05-12 03:23:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.3:443
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 02:47:46	Open TCP Port	No	Pulsedive	0	0	3	0	None	34.74.170.74:80
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2086
2023-05-12 02:44:58	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'CA', u'country_tld': u'.us', u'ip': u'185.199.110.153', u'currency_name': u'Dollar', u'currency': u'USD', u'country
2023-05-12 03:24:22	HTTP Headers	No	Web Spider	10	0	2	0	None	{"content-encoding": "gzip", "nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "referrer-policy": "same-o
2023-05-12 03:03:36	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	snowzef (Net ID: 00:01:36:07:D6:9C)
2023-05-12 03:11:19	Physical Location	No	AbstractAPI	1	0	2	0	None	Bursa, Bursa, 16350, Turkey, Asia
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	OMNI (Net ID: 00:06:25:FA:6F:A7)
2023-05-12 02:53:39	Open TCP Port	No	Censys	0	0	2	0	None	185.199.108.153:80
2023-05-12 02:56:16	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	Cloudflare Inc. Cloudflare
2023-05-12 02:52:43	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'name': u'Contacts domains', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u 8-bit/color RGBA non-interlaced" and extension "png"'}, {u'category': u'Unusual Characteristics', u'origin': u'Binary File', u'identif reads file "c:\\users\\desktop.ini"\n "iexplore.exe" reads file "c:\\users\\%osuser%\\appdata\\local\\microsoft\\internet explorer\\im "ASCII text with very long lines"- [targetUID: 00000000-00002580]\n "77EC63BDA74BD0D0E0426DC8F8008506" has type "Microsoft Cabinet arc
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Junxion_Box (Net ID: 00:02:6F:3A:FE:C3)
2023-05-12 03:01:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.237): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	Geocaching (Category: social) https://www.geocaching.com/p/?u=Altpapier
2023-05-12 02:50:16	Internet Name	No	DNS Resolver	0	0	2	0	None	panel.battleb0t.xyz
2023-05-12 02:44:13	IP Address	No	DNS Resolver	106	0	1	0	None	185.199.110.153
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Beens Gast (Net ID: 00:01:21:1C:17:B1)
2023-05-12 03:09:36	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	222.30.196.104.bc.googleusercontent.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Spleen (Net ID: 00:05:4E:4F:B8:C2)
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:d7:56:4b:39:cd:63:5b:72:07:1e:ba:15:c9:f7:2c:e7:33 Signature Algorithm: sha256Wi GMT Extensions: none Signature : ecdsa-with-SHA256 30:45:02:21:00:BE:39:54:A0:5F:1F:10:03:FA:09:8D: D3:C7:7F:B5:EC:4B:30:F5:03:1A:D7:1
2023-05-12 02:44:11	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	1	1	0	None	github.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	6565 7375 (Net ID: 00:00:C5:D7:5E:38)

2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.46): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Faktopedia (Category: images) https://faktopedia.pl/user/login
2023-05-12 02:57:25	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	files.battleb0t.xyz
2023-05-12 02:45:27	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'ON', u'country_tld': u'.ca', u'ip': u'172.67.168.252', u'currency_name': u'Dollar', u'currency': u'CAD', u'country_
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F2:68:C6)
2023-05-12 02:57:22	Internet Name	No	Certificate Transparency	0	0	1	0	None	nwapi2.battleb0t.xyz
2023-05-12 03:09:38	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	108.48.229.35.bc.googleusercontent.com
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	3	0	None	Netlify\, Inc
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Freigut-Technik (Net ID: 00:01:21:21:C1:63)
2023-05-12 02:44:27	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Node.js
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ZyXEL (Net ID: 00:02:CF:59:46:94)
2023-05-12 02:44:31	Internet Name	No	DNS Resolver	0	0	2	0	None	nuke.battleb0t.xyz
2023-05-12 03:32:11	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.6:443
2023-05-12 02:44:12	SSL Certificate Host Mismatch	Yes	SSL Certificate Analyzer	0	0	2	0	None	*.github.io, github.io, *.github.com, github.com, www.github.com, *.githubusercontent.com, githubusercontent.com
2023-05-12 02:55:28	Linked URL - Internal	No	URLScan.io	0	0	2	0	None	http://kekw.battleb0t.xyz/
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	zoom0083 (Net ID: 00:01:38:69:AF:6C)
2023-05-12 02:55:28	Linked URL - Internal	No	URLScan.io	0	0	2	0	None	http://kekw.battleb0t.xyz/jar
2023-05-12 03:08:47	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.221
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	0	0	1	0	None	CN=nwapi.battleb0t.xyz
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	5	0	None	United States
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.205): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:23	HTTP Headers	No	Web Spider	10	0	4	0	None	{"content-encoding": "gzip", "nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "referrer-policy": "same-o
2023-05-12 02:54:19	Linked URL - External	No	Web Spider	0	0	3	0	None	https://www.google-analytics.com/analytics.js
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Vivino (Category: video) https://www.vivino.com/users/login

2023-05-12 02:44:03	Internet Name	No	SpiderFoot UI	193	0	0	0	None	battleb0t.xyz
2023-05-12 03:27:54	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.138:443
2023-05-12 02:44:30	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	jQuery CDN
2023-05-12 03:21:07	Malicious IP on Same Subnet	Yes	Emerging Threats	0	0	4	0	None	emergingthreats.net [207.154.224.0/20] https://rules.emergingthreats.net/blockrules/compromised-ips.txt
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom71CC68 (Net ID: 00:0C:F6:71:CC:68)
2023-05-12 02:53:39	BGP AS Membership	No	Censys	0	0	2	0	None	54113
2023-05-12 03:00:16	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	mail.ayhu.xyz
2023-05-12 03:09:02	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.99
2023-05-12 02:54:23	HTTP Headers	No	Censys	0	0	4	0	None	{"Content_Length": ["0"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=nwapi.battleb0t.xyz
2023-05-12 03:15:35	Web Content Language	No	Language Detector	0	0	4	0	None	English
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	4	0	None	Germany
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:8080
2023-05-12 02:44:30	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Netlify
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	iz-wpa (Net ID: 00:01:8E:1A:64:A6)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	XFINITY (Net ID: 00:0D:67:37:7A:79)
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	2	0	None	Domains By Proxy, LLC
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CCAZ (Net ID: 00:02:6F:EA:D0:4E)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Mmorpg (Category: gaming) https://forums.mmorpg.com/profile/login
2023-05-12 03:00:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.46): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	YOSEMITE (Net ID: 00:03:52:A1:3D:41)
2023-05-12 02:53:00	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	None None
2023-05-12 02:49:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': u'Windows Gui', u'classification_tags': [u'windows-server-utility'], u'crowdstrike_ai': {u'executable_process_memory_a u'attck_id': u'T1129', u'relevance': 1, u'threat_level': 0, u'type': 6, u'description': u'"popgui.exe" loaded module "API-MS-WIN-CORE- %PROGRAMFILES(X86)%\\COMMON~1\\MICROS~1\\OFFICE14\\Cultures\\office.odf (UID: 00000000-00005448)\n "popgui.exe" called "LoadLibrary" w "Global\\C::Users:%OSUSER%:AppData:Local:Microsoft:Windows:Explorer:thumbcache_48.db!dfMaintainer"\n "Global\\C::Users:%OSUSER%:AppDat "popgui.exe" touched "File Open Dialog Legacy" (Path: "HKCU\\WOW6432NODE\\CLSID\\{725F645B-EAED-4FC5-B1C5-D9AD0ACCBA5E}")\n "popgui.ex
2023-05-12 02:46:18	Affiliate Description - Category	No	DuckDuckGo	0	0	2	0	None	Reverse proxy

2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.86): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	trakt (Category: video) https://trakt.tv/users/ayhu
2023-05-12 03:00:57	Malicious Co-Hosted Site	Yes	VXVault.net	0	1	2	0	None	VXVault Malicious URL List [www.github.com] http://vxvault.net/URL_List.php
2023-05-12 02:49:43	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'Drops files marked as clean', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u [targetUID: 00000000-00003252]\n "ON787GXF.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\ON787GXF.txt "\\#/2:\nM<`PpMb@X\njW`>8RMM.#u&ReR>y(p/:K}5TkLP~w,_Z=\'8Ja"\n "GET /netflix-clone/index.css HTTP/1.1\nAccept: text/css, */*\nReferer: shamsifarooq.github.io\nDNT: 1\nConnection: Keep-Alive"\n "HTTP/1.1 404 Not Found\nConnection: keep-alive\nContent-Length: 5232\nServe
2023-05-12 02:44:23	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	www.github.com
2023-05-12 03:31:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	09e034915a16543e65fa494a6f2d5f65-1767633@contact.gandi.net
2023-05-12 02:54:15	Web Content Type	No	Web Spider	0	0	2	0	None	text/html;charset=utf-8
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	khome2 (Net ID: 00:00:94:CC:A7:CF)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	GURTOPLAR (Net ID: 00:14:C1:27:91:4C)
2023-05-12 02:53:39	Open TCP Port	No	Censys	0	0	2	0	None	185.199.108.153:443
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	m31 (Net ID: 00:02:2D:21:9A:0A)
2023-05-12 03:08:53	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.68
2023-05-12 03:23:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.4:8443
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	4ffa2f (Net ID: 00:02:2D:4F:FA:2F)
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00saadchaudhry.github.io
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	3	0	2	0	None	http://nuke.battleb0t.xyz/
2023-05-12 02:52:19	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', 379 8-bit/color RGBA non-interlaced" and extension "png"\n "tab-content-2-3_1_.png" has type "PNG image data 552 x 338 8-bit/color RGB 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\77 u'"urlblockindex_1_.bin" has type "data"- [targetUID: N/A]\n "background_1_.jpg" has type "JPEG image data JFIF standard 1.01 aspect r
2023-05-12 03:03:55	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	ply.gg
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	101 (Net ID: 00:01:03:7B:E0:44)
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.248): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:04	Physical Location	No	ipapi.co	0	0	2	0	None	San Francisco, California, CA, United States, US
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:53:10:73)
2023-05-12	Affiliate - Email	No	E-Mail Address Extractor	0	0	3	0	None	git@github.com

02:59:59	Address								
2023-05-12 02:56:53	Internet Name	No	DNS Resolver	0	0	4	0	None	vscode.battleb0t.xyz
2023-05-12 03:00:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.47): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:03	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:00:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	zlib@openssh.com
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	sflan11 (Net ID: 00:02:6F:04:8F:04)
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	cpcalendars.ayhu.xyz
2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	giters (Category: coding) https://giters.com/Altpapier
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	NETGEAR (Net ID: 00:09:5B:6A:9E:4C)
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-oo2.github.io
2023-05-12 03:14:48	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:09:03	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.105
2023-05-12 02:45:07	Physical Location	No	ipapi.co	0	0	2	0	None	San Francisco, California, CA, United States, US
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00tau.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	codementor (Category: coding) https://www.codementor.io/@login
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	referrer-policy: same-origin
2023-05-12 03:19:47	Account on External Site	No	Account Finder	0	0	2	0	None	scratch (Category: coding) https://scratch.mit.edu/users/patrickpogoda/
2023-05-12 02:53:10	Web Technology	No	Tool - WAFW00F	0	0	3	0	None	None None
2023-05-12 02:59:53	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	banksean@gmail.com
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	RPOWER1 (Net ID: 00:02:6F:B3:3B:A8)
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	Steam (Category: gaming) https://steamcommunity.com/id/battleb0t
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	6	0	None	United States
2023-05-12	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz

02:50:16									
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	GitHub (Category: coding) https://github.com/battleb0t
2023-05-12 03:08:49	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.113
2023-05-12 03:09:34	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	213.30.196.104.bc.googleusercontent.com
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:0E:F4:FC)
2023-05-12 03:37:29	Malicious IP Address	Yes	MetaDefender	0	1	3	0	None	webroot.com [207.154.228.169]
2023-05-12 03:41:36	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'city': u'Eygelshoven', u'security': {u'is_vpn': False}, u'city_geoname_id': 2756285, u'region_geoname_id': 2751596, u'country': u'N
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:AA:A0:63:98)
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/nwp.PNG
2023-05-12 03:24:22	Web Content	No	Web Spider	2	0	4	0	None	<!DOCTYPE html> <html lang="en-US"> <head> <title>Just a moment...</title> <meta http-equiv="Content-Type" content="text/html; charset rLwUXHzdM6AMR_OdpTBapGpYQut19xKMEhf7XFlJB3i5IvPoLlbKbnM6DASBEm9gloHgHGhLjyH1D86MFl7dLmOy7HXf9Dt59vLXRTySh361-MOVviaFEilkvPgOfzGNeoCglz 'bBrUwSR1j4q+jiK831F3uz4Yhp8vDXUt4BefqtjwDOM1gm//5501ZpnQ7c811CiMG7EvRE/6yKWzdSdEgeqlKrPobmKgPq4s4sf5keh0JSpRTFqyThcJtJJr1NWRsfypsHrBA
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	TotalWar (Category: gaming) https://forums.totalwar.com/profile/login
2023-05-12 03:09:48	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	75.170.74.34.bc.googleusercontent.com
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	gclabc (Net ID: 00:0B:86:22:0F:31)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=gKkAv2ueXH0GbQQgHQUB1ba%2FGC57%2Fw1l33qylJQZwo8rZZSQGe9c
2023-05-12 02:44:24	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 03:43:57	URL (Form)	No	Page Information	0	0	5	0	None	https://ayhu.xyz/?__cf_chl_f_tk=VqQIpv85XrbB73FISUPAb3YOKzrkafpohMHe42yb99c-1683861862-0-gaNycGzNChA
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	jack (Net ID: 00:02:6F:66:E7:97)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless (Net ID: 00:01:36:06:41:8A)
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.53): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:13	HTTP Status Code	No	Web Spider	0	0	3	0	None	200
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:EB:4A:C2)
2023-05-12 03:00:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.8): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:16	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.142): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:39	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level': 0, u'type': 7, u'description': u'"llink.to"'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', type "UTF-8 Unicode text with very long lines with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\f76618 potential URL in binary/memory', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, address.domaintools.com"\n Heuristic match: "ip-api.com"\n Heuristic match: "ip-score.com"\n Heuristic match: "ip.jsontest.com"\n Heur

2023-05-12 03:18:06	Externally Hosted Javascript	No	Page Information	0	0	3	0	None	https://use.fontawesome.com/9dfc16ed6b.js
2023-05-12 02:49:55	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:2c:84:3a:08:10:23:75:f2:8a:d5:a0:cb:cc:f6:da:14:6e Signature Algorithm: sha256Wi 20:eb:f8:09:fe:e5:12:c5:27:1a:bc:14:2c:c8:47:50:c4:fe: 3b:82:e2:94:1e:ea:46:71:f7:de:cb:93:8d:d3:d6:0e:2f:57: cf:7c:ae:9d:b7:80:a0:8c:
2023-05-12 03:11:16	Physical Location	No	AbstractAPI	0	0	2	0	None	London, England, W1B, United States, North America
2023-05-12 03:11:42	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	3	0	None	CVE-2011-3389 https://nvd.nist.gov/vuln/detail/CVE-2011-3389 Score: 4.3 Description: The SSL protocol, as used in certain configuratio
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	TOMTSSID (Net ID: 00:02:2D:76:6D:60)
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	0	0	1	0	None	CN=battleb0t.xyz
2023-05-12 02:54:38	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:01:18	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.155): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:50:16	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [185.199.108.153] https://www.virustotal.com/en/ip-address/185.199.108.153/information/
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pannet-24 (Net ID: 00:01:8E:DA:59:C4)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	218 5 (Net ID: 00:01:9F:34:7C:1C)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Sprint Drive (Net ID: 00:0A:F5:F9:D9:E8)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	DaltonInt (Net ID: 00:0A:04:99:14:E2)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ConnectionPoint (Net ID: 00:01:E3:4A:D6:05)
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.107): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	Express
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	redwood (Net ID: 00:01:38:85:C1:F8)
2023-05-12 03:13:01	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-tikaro.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	1	4	0	None	GitHub.com
2023-05-12 03:43:29	Country	No	Country Name Extractor	0	0	6	0	None	Germany
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	4	0	None	15169
2023-05-12 02:45:29	Physical Location	No	ipapi.co	1	0	3	0	None	North Charleston, South Carolina, SC, United States, US
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:00:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.4): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.185): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-	Co-Hosted	No	SSL Certificate	0	1	2	0	None	

12 02:44:13	Site - Domain Name		Analyzer						githubusercontent.com
2023-05-12 03:10:22	Blacklisted IP Address	Yes	Threat Jammer	0	1	2	0	None	Threat Jammer - Risk score: 40 (MEDIUM) https://threatjammer.com/info/188.114.96.1
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	jbnowires (Net ID: 00:0C:41:B5:31:DD)
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:8443
2023-05-12 02:53:17	IP Address	No	Mnemonic PassiveDNS	72	0	1	0	None	188.114.97.1
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cross-origin-opener-policy: same-origin
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	4	0	None	14061
2023-05-12 02:47:03	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur kernel32.dll, user32.dll, gdi32.dll, ole32.dll, comctl32.dll, uxtheme.dll, oleaut32.dll, version.dll, msctfime.ime)', u'attck_id_wiki' u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_ [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\load_statistics.db-wal]- [targetUID: 00000000-00007376]\n "typosquatting_list.pb has type "UTF-8 Unicode text with very long lines with CRLF line terminators"- Location: [%TEMP%\\7376_780837103\\edge_confirmation_pa
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.41): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	fanpop (Category: social) https://www.fanpop.com/fans/ayhu
2023-05-12 02:45:41	Physical Location	No	AbstractAPI	0	0	2	0	None	San Francisco (South Beach), California, 94107, United States, North America
2023-05-12 03:31:33	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	registrar-abuse@google.com
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.14): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.34): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:26	Username	No	Social Network Identifier	172	0	5	0	None	login
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	WIN-MAKCI77HADK 1028 (Net ID: 38:1D:D9:1B:3E:B3)
2023-05-12 02:47:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	104.196.30.220:80
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX551551399 (Net ID: 00:01:E3:55:13:99)
2023-05-12 03:03:51	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	ebrahemsamir.github.io
2023-05-12 02:54:22	Linked URL - External	No	Web Spider	3	0	3	0	None	https://qolhub.cloudflareaccess.com/cdn-cgi/access/login/panel.battleb0t.xyz?kid=0e8fcd5c4d6f2fbb6bc18c164812f146f66e83d772c26262aaca8
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	ELSA (Net ID: 00:02:2D:27:BC:4F)
2023-05-12 02:46:55	Internet Name	No	DNS Resolver	0	0	2	0	None	funny.battleb0t.xyz
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	MCUUID (Minecraft) (Category: gaming) https://mcuuid.net/?q=ayhu
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	PureFTPd Pure-FTPd
2023-05-12	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:2096

02:54:34									
2023-05-12 03:32:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.4:443
2023-05-12 02:44:09	SSL Certificate Host Mismatch	Yes	SSL Certificate Analyzer	0	0	1	0	None	*.github.io, github.io, *.github.com, github.com, www.github.com, *.githubusercontent.com, githubusercontent.com
2023-05-12 03:32:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.20:8080
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	giters (Category: coding) https://giters.com/battleb0t
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	7637 0253 (Net ID: 00:1C:FB:F9:EC:50)
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	GWF (Net ID: 00:06:25:06:28:35)
2023-05-12 02:46:49	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	3	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	xHamster (Category: XXXPORNXXX) https://xhamster.com/users/ayhu
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Airliners (Category: social) https://www.airliners.net/user/login/profile
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.54): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:47:32	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.135.9:443
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	Pornhub Users (Category: XXXPORNXXX) https://www.pornhub.com/users/battleb0t
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	WLAN (Net ID: 00:02:44:AF:55:CE)
2023-05-12 03:17:44	Username	No	Account Finder	58	0	1	0	None	ayhu
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	LF-X1U.00014A10EF0C (Net ID: 00:01:4A:10:EF:0C)
2023-05-12 02:53:25	IPv6 Address	No	Mnemonic PassiveDNS	0	0	2	0	None	2606:4700:3030::ac43:a8fc
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.146): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:53:56	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 02:56:52	Internet Name	No	DNS Resolver	0	0	3	0	None	pics.battleb0t.xyz
2023-05-12 02:54:38	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	dragontears (Net ID: 00:0C:F6:42:E6:42)
2023-05-12 03:00:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-64-etm@openssh.com
2023-05-12 02:44:36	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:34:48:36:b2:51:77:1f:45:f7:ca:23:53:09:6b:f8:20:f7 Signature Algorithm: sha256Wi 59:bc:d7:f8:c2:0e:5f:4b:d2:8c:3b:71:44:77:09:c9:00:b8: 05:73:a8:af:5c:03:95:2d:4c:ab:3f:94:8d:b8:ae:e1:f0:37: e9:58:9a:a0:2c:5e:da:55:

2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SX551C65D72 (Net ID: 00:01:E3:C6:5D:72)
2023-05-12 03:32:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.17:443
2023-05-12 03:24:22	HTTP Headers	No	Web Spider	1	0	2	0	None	{"content-encoding": "gzip", "transfer-encoding": "chunked", "vary": "Accept-Encoding", "server": "nginx", "connection": "keep-alive",
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:32:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.14:8080
2023-05-12 03:00:00	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	jloup@gzip.org
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	4	0	None	cloudflare
2023-05-12 02:57:24	Internet Name	No	Certificate Transparency	0	1	1	0	None	pics.battleb0t.xyz
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Computing websites
2023-05-12 02:52:28	Malicious IP Address	Yes	VirusTotal	0	1	3	0	None	VirusTotal [104.196.30.220] https://www.virustotal.com/en/ip-address/104.196.30.220/information/
2023-05-12 02:58:43	Vulnerability - CVE High	Yes	Tool - testssl.sh	0	2	1	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 7.5 Description: The DES and Triple DES ciphers, as used in the TL
2023-05-12 02:54:19	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2023-05-12 03:01:03	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.107): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:00:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.61): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom90F1C4 (Net ID: 00:0C:F6:90:F1:C4)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-B962 (Net ID: 00:1D:D5:BA:B9:60)
2023-05-12 02:44:31	Affiliate - Domain Name	No	DNS Resolver	0	0	3	0	None	github.com
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.212): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	NotLakehouse (Net ID: 00:0C:41:6F:1D:BC)
2023-05-12 03:09:03	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.104
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.22): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.42): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	RossAviation206 (Net ID: 00:0C:42:6C:BE:A6)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-ray: 7c5f60715ea2423d-EWR

2023-05-12 02:46:21	Netblock Membership	No	RIPE	8	0	2	0	None	185.199.110.0/24
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	FruityWifi-004 (Net ID: 00:04:E2:F4:8A:F5)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wagmound (Net ID: 00:01:71:0A:16:DF)
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.230): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:13:10	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [james-gamboa.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	410HowardStudios (Net ID: 00:02:2D:00:25:63)
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.174): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	suddenlink.net-2AD2 (Net ID: 90:1A:CA:7E:2A:D0)
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:80
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	downtown7 (Net ID: 00:01:E3:DE:06:3F)
2023-05-12 02:53:19	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 00006884.00000000.78323.8EB30000.00000040.mdmp', u'file_process_disc_pathway': u'Z:\\rufus-4.0p.exe', u'flags': u'00000040', u'file_pr loaded module "SETUPAPI.DLL" at base 8c420000\n "rufus-4.0p.exe" loaded module "SHELL32.DLL" at base 8d5c0000\n "rufus-4.0p.exe" loade module "ONDEMANDCONNROUTEHELPER.DLL" at base 6f650000\n "rufus-4.0p.exe" loaded module "WINHTTP.DLL" at base 854f0000\n "rufus-4.0p.ex ADVAPI32.dll (UID: 00000000-00006884)\n "rufus-4.0p.exe" called "LoadLibrary" with a parameter COMCTL32.dll (UID: 00000000-00006884)\n
2023-05-12 03:10:01	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	expressdryclean.gr
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://pics.battleb0t.xyz/images/random_4.png
2023-05-12 02:54:22	Web Content Type	No	Web Spider	0	0	2	0	None	text/html;charset=utf-8
2023-05-12 03:00:49	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.69): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ZyXEL (Net ID: 00:13:49:EC:E1:54)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-ray: 7c5f60483bb94334-EWR
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:01:20	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.183): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SR.Mandant (Net ID: 00:01:21:30:6F:34)
2023-05-12 02:54:51	Raw Data from RIRs	No	Censys	0	0	3	0	None	{"last_updated_at": "2023-05-12T02:01:01.392Z", "ip": "34.74.170.74", "location_updated_at": "2023-04-30T03:41:24.176126Z", "autonomou "resolved_at": "2022-11-22T13:32:20.879316883Z"}, "savemyspot.ca": {"record_type": "A", "resolved_at": "2022-10-03T12:31:57.921314861Z "hopton.co.uk": {"record_type": "A", "resolved_at": "2023-05-05T20:33:36.106307737Z"}, "kobekoto.com": {"record_type": "A", "resolved_ "2023-03-10T15:02:16.821390522Z"}, "www.pepoparadise.net": {"record_type": "CNAME", "resolved_at": "2022-10-29T16:20:13.892401780Z"}, 17T22:44:25.184926620Z"}, "v8.azharlihan.com": {"record_type": "CNAME", "resolved_at": "2022-10-05T19:12:08.840985334Z"}, "www.avfmuda
2023-05-12 03:00:50	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0.crimson-perch.github.io

2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F2:6F:6D)
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.193): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	043320 (Net ID: 00:02:2D:04:33:20)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	xfinitywifi (Net ID: 00:0D:67:8C:21:AA)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Sunshine (Net ID: 00:07:40:87:15:01)
2023-05-12 03:33:34	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	MiCCPICC Profile U$JLQ clc$1 pHYs iTXtXML:com.adobe.xmp <exif:PixelYDimension>1024</exif:PixelYDimension> <exif:PixelXDimension>1024</
2023-05-12 03:01:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.243): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:FD:64:31)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Bulldog Free internet (Net ID: 00:01:71:0A:05:E5)
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.144): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.59): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:38	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	registrar-abuse@cloudflare.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	nnru (Category: social) https://login.www.nn.ru
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Microsoft acquisitions
2023-05-12 02:46:35	Netblock Membership	No	RIPE	1	0	3	0	None	35.229.48.0/20
2023-05-12 02:54:30	Raw Data from RIRs	No	Censys	13	0	3	0	None	{"operating_system": {"product": "Linux", "vendor": "Debian", "version": "10.2", "other": {"family": "Linux"}, "uniform_resource_ident "DISPLAY_BASE64"}, "length": 2048, "modulus": "uPxDpRdIrA/iz2ExEgRAxKmXST2zSxUUASzEIsL6O2PTrSNc6umFNFt/dHdxbK0YoU5gp4vR8iK16J/is3qdC1O sha2-512", "hmac-sha1"]}, "endpoint_id": {"comment": "Debian-10+deb10u2", "_encoding": {"raw": "DISPLAY_UTF8"}, "protocol_version": "2 ["W/\"64217dc5-156\""], "Content_Type": ["text/html"], "Date": ["<REDACTED>"]}, "body_hashes": ["sha256:d5e3078cb88ba53faa1d104c27054d L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA", "fingerprint": "7fa4ff68ec04a99d7528d5085f94907f4d1d
2023-05-12 02:50:30	Raw Data from RIRs	No	GLEIF	0	0	3	0	None	[{u'relationships': {u'lei-records': {u'data': {u'type': u'lei-records', u'id': u'54930014QNWWH8OAC930'}, u'links': {u'related': u'htt
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Commons-based peer production - Commons-based peer production is a term coined by Harvard Law School professor Yochai Benkler. It desc
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:D2:56:1D)
2023-05-12 03:00:37	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	6	0	None	abusecomplaints@markmonitor.com
2023-05-12 02:55:22	Linked URL - Internal	No	Google	0	0	1	0	None	https://ayhu.xyz/
2023-05-12 02:44:19	IPv6 Address	No	DNS Resolver	15	0	3	0	None	2600:1f18:2489:8201::c8
2023-05-12 02:44:13	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	2	0	None	githubusercontent.com
2023-05-12 02:53:03	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'identifier': u'string-10', u'name': u'Found a reference to a known community page', u'attck_id_wiki': None, u'threat_level_human': u

									Indicator: "ubs.com")\n ""6whiskey.com"," (Source: wallet-pre-stable.json, Indicator: "key.com")\n ""99centsubs.com"," (Source: wallet Location: [%TEMP%\\6576_1454671731\\bnpl\\bnpl.bundle.js]- [targetUID: 00000000-00006576]\n "tokenized-card.bundle.js" has type "UTF-8 00006576]\n "safety_tips.pb" has type "data"- Location: [%TEMP%\\6576_1216152141\\safety_tips.pb]- [targetUID: 00000000-00006576]\n "d
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	3	0	None	cloudflare
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.171): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:13	Physical Location	No	Censys	0	0	4	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:08:53	Vulnerability - CVE Medium	Yes	Tool - Retire.js	0	0	4	0	None	CVE-2019-11358 https://nvd.nist.gov/vuln/detail/CVE-2019-11358 Score: 6.1 Description: jQuery before 3.4.0, as used in Drupal, Backdro
2023-05-12 03:08:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.82
2023-05-12 03:03:42	Internet Name	No	DNS Resolver	0	0	3	0	None	nuke.battleb0t.xyz
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	itch.io (Category: gaming) https://itch.io/profile/login
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Andrea Schwartz Gallery (Net ID: 00:01:9F:3D:4F:68)
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.100): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:04	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level' [%APPDATA%\\Microsoft\\Windows\\Cookies\\DFCSLJSN.txt]- [targetUID: 00000000-00003572]\n Dropped file: "8QJH7RWY.txt" - Location: [%AP setup 62932 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"'}, {u'category': u'Installation/Persistence' "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has type "PNG image data 16 x 16 4-bit colormap non-interlaced"- [targetUID: N/A]\
2023-05-12 02:53:20	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:23:36:1a:72:6e:fc:71:09:49:b1:35:f9:b5:e5:28:80:de Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: E6:0D: 89:35:6f:e7:d7:11:5a:13:0a:a9:83:9e:0f:c2:f2:ea:d8:50: 30:65:9c:16:49:f6:30:d8:a2:e3:83:ff:5d:ff:00:a2:ff:57: de:68:f4:70:90:a3:db:c8:
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	5	0	None	cloudflare
2023-05-12 03:09:58	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	heberlein (Net ID: 00:02:2D:30:2C:33)
2023-05-12 03:00:50	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00.github.io
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:54:10:ED)
2023-05-12 03:16:26	Physical Location	No	ipapi.co	1	0	2	0	None	Bursa, Bursa, 16, Turkey, TR
2023-05-12 02:44:14	Domain Name	No	DNS Resolver	0	0	1	0	None	battleb0t.xyz
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	PET KLINIK (Net ID: 00:12:BF:30:95:FA)
2023-05-12 03:18:06	URL (Purely Static)	No	Page Information	0	0	3	0	None	http://kekw.battleb0t.xyz/jar
2023-05-12 03:18:06	URL (Form)	No	Page Information	0	0	6	0	None	https://www.ayhu.xyz/?__cf_chl_f_tk=eArohGzIRNubxh3D6IFMRkkS6OUaNS008kBgg4I5pUY-1683860063-0-gaNycGzNCiU
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:0C:41:B1:75:22)

2023-05-12 02:45:26	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'ON', u'country_tld': u'.ca', u'ip': u'104.21.71.14', u'currency_name': u'Dollar', u'currency': u'CAD', u'country_po
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	vsco (Category: social) https://vsco.co/login/gallery
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Brandis Wifi 5GHz (Net ID: 00:01:9F:20:CA:54)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATTFhSfWa2 (Net ID: B0:DA:F9:7C:BB:40)
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	5	0	None	United States
2023-05-12 02:44:15	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS RSA SHA256 2020 CA1
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	1620 Guest (Net ID: 00:01:21:30:37:7F)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Lifestyle (Net ID: 00:06:25:61:2F:2E)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-cache-status: DYNAMIC
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	3	0	None	cloudflare
2023-05-12 02:53:35	Netblock Membership	No	Censys	0	0	2	0	None	185.199.110.0/24
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_ipad (Net ID: 00:0C:E6:08:04:05)
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	3	0	None	cloudflare
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MGOKCEN (Net ID: 00:14:C1:20:BB:F4)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Kircal3 (Net ID: 00:14:C1:15:7B:C1)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	DATAVO (Net ID: 00:02:61:19:70:44)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	meet me (Category: dating) https://www.meetme.com/login
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://pics.battleb0t.xyz/images/kappi_2.png
2023-05-12 03:31:23	Malicious IP on Same Subnet	Yes	blocklist.de	0	0	4	0	None	blocklist.de List [165.232.112.0/20] http://lists.blocklist.de/lists/all.txt
2023-05-12 02:56:57	Internet Name	No	DNS Resolver	0	0	2	0	None	vscode.battleb0t.xyz
2023-05-12 03:01:03	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.109): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:12:58	Malicious Co-Hosted Site	Yes	OpenPhish	0	1	3	0	None	OpenPhish [netlify.app] https://www.openphish.com/feed.txt
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	kik (Category: social) https://ws2.kik.com/user/ayhu
2023-05-12 02:59:52	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	l@allledglobal.com

2023-05-12 03:00:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha2-256-etm@openssh.com
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	ConnectionPoint (Net ID: 00:01:E3:08:2F:54)
2023-05-12 03:32:11	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.6:80
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.243): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	My Passport (2.4 GHz) - 084071 (Net ID: 00:00:C0:08:40:71)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Chess.com (Category: gaming) https://www.chess.com/member/ayhu
2023-05-12 03:12:41	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 03:00:48	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.64): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:04	Country	No	Country Name Extractor	0	0	2	0	None	United States
2023-05-12 03:28:39	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.160:80
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	x-fastly-request-id: 47e9025f17d9e6e936d804b3c00d7989ec4a827a
2023-05-12 02:59:57	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	mery.robinson@ftb.ca.gov
2023-05-12 02:46:49	Open TCP Port	No	SSL Certificate Analyzer	0	0	3	0	None	35.229.48.116:443
2023-05-12 03:24:19	Account on External Site	No	Account Finder	0	0	8	0	None	slideshare (Category: social) https://www.slideshare.net/baptistevauthey
2023-05-12 03:18:06	Externally Hosted Javascript	No	Page Information	0	0	3	0	None	http://code.jquery.com/jquery-3.2.1.js
2023-05-12 03:23:11	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.1:80
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-cache: MISS
2023-05-12 03:13:03	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0000rgb124.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:09:41	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	125.48.229.35.bc.googleusercontent.com
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom6FE774 (Net ID: 00:0C:F6:6F:E7:74)
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	2	0	3	0	None	https://funny.battleb0t.xyz/images/random_3.jpg
2023-05-12 02:54:23	HTTP Headers	No	Web Spider	10	0	5	0	None	{"content-encoding": "gzip", "nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "referrer-policy": "same-o
2023-05-12	Web Server	No	Web Server Identifier	0	1	2	0	None	GitHub.com

03:27:00									
2023-05-12 03:18:45	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image ExifOffset': (0x8769) Long=134 @ 90, 'Image Orientation': (0x0112) Short=Horizontal (normal) @ 18, 'Image YCbCrPositioning': (
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:3C:1A:6D)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	LCPS-A (Net ID: 00:0C:E6:02:7D:6E)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Mastodon-mastodon (Category: social) https://mastodon.social/@login
2023-05-12 02:55:28	Raw Data from RIRs	No	URLScan.io	0	0	2	0	None	[{u'sort': [1679937961810, u'be713cda-cf3f-49bd-91b6-e8517dc017bf'], u'task': {u'domain': u'kekw.battleb0t.xyz', u'uuid': u'be713cda-c [u'https://phish.report', u'@phish_report'], u'url': u'http://kekw.battleb0t.xyz/', u'visibility': u'public', u'time': u'2023-03-11T22 u'country': u'DE', u'redirected': u'https-only', u'apexDomain': u'battleb0t.xyz', u'tlsAgeDays': 43, u'asn': u'AS14061'}}]
2023-05-12 03:32:04	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.3:443
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	eduwifi (Net ID: 00:02:2D:2B:E9:C1)
2023-05-12 03:22:54	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.1:80
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Motokiller (Category: images) https://mklr.pl/user/login
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:2086
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2096
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 03:21:07	Malicious IP on Same Subnet	Yes	Emerging Threats	0	0	4	0	None	emergingthreats.net [165.232.112.0/20] https://rules.emergingthreats.net/blockrules/compromised-ips.txt
2023-05-12 03:23:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.12:8443
2023-05-12 02:53:00	Raw Data from RIRs	No	Tool - WAFW00F	1	0	2	0	None	[{"url": "https://oldfluid.battleb0t.xyz", "firewall": "Cloudflare", "detected": true, "manufacturer": "Cloudflare Inc."}, {"url": "ht
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:09:47	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	70.170.74.34.bc.googleusercontent.com
2023-05-12 03:00:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.33): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	006f10 (Net ID: 00:02:2D:00:6F:10)
2023-05-12 02:44:12	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:4d:72:d7:7c:dd:a7:02:dd:5a:67:f2:a2:3b:bd:d9 Signature Algorithm: sha256WithRSAE - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1-1.crt X509v3 Basic Constraints fa:29:72:01:3e:b7:06:f1:2f:1a:0e:91:c5:ec:35:bf:f5:da: 33:95:de:24:12:0d:f5:c3:23:8d:40:82:d1:5c:eb:de:0a:08: e8:e5:83:e5:0a:8b:3a:5e:
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	007joshie.github.io
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	okidoki (Category: misc) https://m.okidoki.ee/ru/users/login/
2023-05-12 02:49:40	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'de [%APPDATA%\\Microsoft\\Windows\\Cookies\\51F6C1W2.txt]- [targetUID: 00000000-00003044]\n "_03447F9C-B539-11ED-B006-080027895A87_.dat" {u'category': u'External Systems', u'origin': u'External System', u'identifier': u'avtest-6', u'name': u'Found an IP/URL artifact that u'T1071', u'malicious_identifiers': [], u'malicious_identifiers_count': 0, u'technique': u'Application Layer Protocol', u'informative_
2023-05-12 02:56:18	Netblock Membership	No	RIPE	0	0	2	0	None	188.114.96.0/24

2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	krommewaal (Net ID: 00:01:71:0A:07:2B)
2023-05-12 03:01:16	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.140): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:39	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.187): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:12:41	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2011-3389 https://nvd.nist.gov/vuln/detail/CVE-2011-3389 Score: 4.3 Description: The SSL protocol, as used in certain configuratio
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	CMMC (Net ID: 00:02:6F:DF:89:25)
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	2	0	None	GitHub\, Inc.
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	007jedgar.github.io
2023-05-12 02:58:27	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur Encoding: gzip, deflate\nHost: tangerine-gaufre-d39b6b.netlify.app\nDNT: 1\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GE dce411.netlify.app/index.html\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAcce Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: tangerine-gaufre-d39b6b.netlify.app\nDNT: 1\nConnection: Keep- rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: tangerine-gaufre-d39b6b.netlify.app\nDNT: 1\nConnection: Keep-Alive" (Indic
2023-05-12 03:23:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.6:8443
2023-05-12 03:09:58	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	toyhou.se (Category: hobby) https://toyhou.se/login
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-14n.github.io
2023-05-12 02:54:18	Web Content	No	Web Spider	7	0	2	0	None	<!DOCTYPE html> <html> <head> <title>Funny Forehead Gallery</title> <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/boots src="/images/carti_1.jpg"> <img src="/images/carti_2.PNG"> < "thumbnail"> <img src="/images/random_2.jpeg"> <img src="/im
2023-05-12 02:49:31	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:d8:ac:1a:31:df:8f:f8:c7:c3:27:35:9c:31:39:5f:60:e8 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: D4:B4: 48:d4:7d:65:31:de:70:bc:f7:3f:bd:89:d2:15:4c:60:09:1a: af:c6:86:cb:88:cd:d5:a5:55:42:cd:bd:22:96:61:43:7d:a3: c6:84:39:52:19:c9:4c:63:
2023-05-12 03:13:09	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0101dd.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.252): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:17	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:50c0:8001::153
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	P A L M N E T (Net ID: 00:01:71:0A:04:85)
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2087
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Wireclub (Category: social) https://www.wireclub.com/users/login
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AIRTIES (Net ID: 00:12:BF:4D:A9:54)
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	4	0	None	Iceland
2023-05-12	WiFi Access	No	Wigle.net	0	0	5	0	None	CLFPrivate (Net ID: 00:02:6F:B9:C7:0C)

03:18:58	Point Nearby								
2023-05-12 02:54:15	Linked URL - Internal	No	Web Spider	0	0	2	0	None	https://battleb0t.xyz/
2023-05-12 03:08:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.83
2023-05-12 02:45:40	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'San Francisco (South Beach)', u'security': {u'is_vpn': False}, u'city_geoname_id': 5326621, u'region_geoname_id': 5332921,
2023-05-12 02:57:47	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'type': 8, u'description': u'"Part-RU" has type "DOS executable (COM)"- Location: [%TEMP%\\5488_430541408\\Part-RU]- [targetUID: 0000 terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\628fc9da-b324-41b9-81c8-5c3463af84f8.tmp]- [targetUID: 0 [%TEMP%\\5488_1156268761\\shoppingfre.js]- [targetUID: 00000000-00005488]\n "shopping.html" has type "HTML document ASCII text with CR 00005488]\n Dropped file: "product_page.js" - Location: [%TEMP%\\5488_1156268761\\product_page.js]- [targetUID: 00000000-00005488]\n D
2023-05-12 02:47:15	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:3108:304:WilStaging_02"\n "\\Sessions\\1\\BaseNamedObjects\\ChromeProcessSingletonStartup u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': u'htt 00003108]\n "Tabs_13322050400392718" has type "data"- [targetUID: 00000000-00003108]\n "Filtering Rules-AA" has type "data"- Location: Data\\Subresource Filter\\Unindexed Rules\\10.34.0.42\\LICENSE"'}, {u'category': u'Network Related', u'origin': u'Network Traffic', u'
2023-05-12 02:54:23	Physical Location	No	Censys	0	0	4	0	None	Seattle, Washington, 98108, United States, North America
2023-05-12 03:13:04	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [000panther.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:49:46	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:2024:304:WilStaging_02 Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Cache\\Cache_Data\\f_000288]- [targetUID: 00000000-00004876]\n "9ac0e6 [%PROGRAMFILES%\\chrome_ComponentUnpacker_BeginUnzipping2024_1522616664\\json\\i18n-hub\\fr-CA\\strings.json]- [targetUID: 00000000-00 N5h"'}, {u'category': u'External Systems', u'origin': u'External System', u'identifier': u'avtest-1', u'name': u'Sample was identified
2023-05-12 02:53:45	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "X_Ser
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.34): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:47:44	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur d33wubrfki0l68.cloudfront.net\nDNT: 1\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GET /e278deffc2dc2e5c432309dc70e3af4ccc HTTP/1.1\nAccept: text/html, application/xhtml+xml, */*\nReferer: http://dockeer.space/\nAccept-Language: en-US\nUser-Agent: Mozilla/5 deflate\nHost: fonts.gstatic.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GET /s/oxygen/v15/2sDfZG1Wl4LcnbuKjk u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relev
2023-05-12 02:52:17	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur (Indicator: "dir "; File: "wallet-pre-stable.json")\n Found string ""comeherebuddy.com"," (Indicator: "dir "; File: "wallet-pre-stable ""bowlingmonkey.com"," (Source: wallet-pre-stable.json, Indicator: "key.com")\n ""burgeonbleu.com"," (Source: wallet-pre-stable.json, u'T1105', u'relevance': 3, u'threat_level': 0, u'type': 8, u'description': u'"shopping.js" has type "UTF-8 Unicode text with very long Location: [%TEMP%\\1500_2144953265\\edge_confirmation_page_validator.js]- [targetUID: 00000000-00001500]\n "product_page.js" has type
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	XFINITY (Net ID: 00:0D:67:2F:5E:C5)
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	webmail.ayhu.xyz
2023-05-12 02:50:33	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 7, u'threat_level': 0, u'type': 2, u' u'Dropped files', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': Write-Ahead Log version 3007000"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\load_statistics.db-wal]- [targetUID: Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\da1e6743-5e1c-49e6-a14b-642c85423466.tmp]- [targetUID: 00000000-00006628]\n "7a
2023-05-12 02:54:00	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	1a0dc2 (Net ID: 0C:EA:C9:15:D9:AF)
2023-05-12 03:23:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.11:80
2023-05-12 03:08:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.76
2023-05-12	Affiliate - Company	No	Company Name Extractor	0	0	7	0	None	World4You Internet Services GmbH

03:43:26	Name								
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:05:5D:F0:3A:5B)
2023-05-12 02:45:21	Raw Data from RIRs	No	ipapi.co	0	0	4	0	None	{u'region_code': u'VA', u'country_tld': u'.us', u'ip': u'2600:1f18:2489:8201::c8', u'currency_name': u'Dollar', u'currency': u'USD', u
2023-05-12 02:44:35	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	HTTP/3
2023-05-12 03:12:15	Affiliate - Domain Whois	No	Whois	0	0	6	0	None	% This is the RIPE Database query service. % The objects are in RPSL format. % % The RIPE Database is subject to Terms and Conditions.
2023-05-12 02:46:50	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Pastebin (Category: tech) https://pastebin.com/u/ayhu
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	webdisk.ayhu.xyz
2023-05-12 02:44:09	Software Used	Yes	Tool - Wappalyzer	0	0	1	0	None	Cloudflare
2023-05-12 02:44:30	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	HSTS
2023-05-12 02:54:38	Software Used	Yes	Censys	0	0	3	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	default (Net ID: 00:01:24:F2:1A:77)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	BossWirelessSitecom (Net ID: 00:0C:F6:9F:57:4C)
2023-05-12 02:56:26	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 8, u'description': u'"57C8EDB95DF3F0AD4EE2DC2B8CF Scalable Vector Graphics image"- [targetUID: N/A]\n "urlref_httpswww.calgarystampede.com" has type "HTML document UTF-8 Unicode text w image/*;q=0.8, */*;q=0.5\nReferer: https://www.calgarystampede.com/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; 7@|Up}V3d5V_%8Grm|>{XqO"]8fjRVH*dyM6z7gmRQtxcyZ#x "i_9M-y^\\u]sX0\'uF-ouh;sp$!~k`~blgK+y^\|X[,/&hksHC`<O<ZYs"t3G4s\n$|^k\nq1EdUY\ngcXpn
2023-05-12 02:59:18	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'Antivirus vendors marked dropped file "urlblockindex_1_.bin" as clean (type is "data")'}, {u'category': u'Unusual Characteristics', "7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptne u'"GET /beacon.js HTTP/1.1\nAccept: application/javascript, */*;q=0.8\nReferer: http://188.114.96.1/\nAccept-Language: en-US\nUser-Age u'entrypoint': None, u'mitre_attcks': [{u'parent': None, u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1573', u'suspicious_
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Baha T|z|ner (Net ID: 00:19:C6:DD:81:11)
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.141): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	5	0	None	cloudflare
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=fluid.battleb0t.xyz
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Bandlab (Category: music) https://www.bandlab.com/ayhu
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	XVIDEOS-profiles (Category: XXXPORNXXX) https://www.xvideos.com/profiles/ayshoo
2023-05-12 03:09:05	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.112
2023-05-12 03:23:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.4:8080
2023-05-12 03:13:03	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0000cap.github.io] https://www.openphish.com/feed.txt

2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	0	0	1	0	None	CN=fluid.battleb0t.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	n83d (Net ID: 00:06:25:86:4F:31)
2023-05-12 02:53:33	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "%WINDIR%\\System32\\msctf.dll" at 752F0000\n "iexplore.exe" loaded module "%WINDIR%\\Temp\\VxOle32.dll" at 6D020000\n "iexplore.exe" "iexplore.exe" loaded module "%WINDIR%\\System32\\msasn1.dll" at 74E30000\n "iexplore.exe" loaded module "%WINDIR%\\System32\\oleacc.d 75140000\n "iexplore.exe" loaded module "%WINDIR%\\System32\\wininet.dll" at 76C70000\n "iexplore.exe" loaded module "%WINDIR%\\System "iexplore.exe" loaded module "%WINDIR%\\System32\\en-US\\user32.dll.mui" at 02A50000\n "iexplore.exe" loaded module "%LOCALAPPDATA%\\o
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00tau.github.io
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	referrer-policy: same-origin
2023-05-12 03:32:00	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.1:8080
2023-05-12 03:03:32	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:53:22	IP Address	No	Mnemonic PassiveDNS	0	0	2	0	None	172.67.168.252
2023-05-12 02:54:20	HTTP Status Code	No	Web Spider	0	1	2	0	None	521
2023-05-12 03:27:00	Web Technology	No	Web Server Identifier	0	0	3	0	None	Express
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX55155D43E (Net ID: 00:01:E3:55:D4:3E)
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:44:09	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 0c:e3:f4:1c:e8:cb:bb:cf:13:f7:6c:6f:36:5e:c2:eb Signature Algorithm: sha256WithRSAE a8:21:d4:b0:1c:8c:61:d9:0a:ed:8a:98:0e:ec:59:d1:7e:8a: 57:4f:81:85:21:9d:81:17:a5:6d:50:b7:02:17:30:3f:51:39: 0f:0d:a8:d9:9c:3b:6f:9f:
2023-05-12 03:24:30	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	NameCheap, Inc.
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Hangar6 (Net ID: 00:02:6F:E9:36:AC)
2023-05-12 03:32:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.8:80
2023-05-12 02:44:28	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12 02:53:35	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-11T23:24:30.410Z", "ip": "185.199.110.153", "location_updated_at": "2023-05-01T12:36:37.024174Z", "autono 28T21:44:00.274408560Z"}, "www.2briley.com": {"record_type": "CNAME", "resolved_at": "2023-04-28T13:20:47.065260373Z"}, "www.diogomace "www.liufuwen.com": {"record_type": "CNAME", "resolved_at": "2023-03-30T00:11:36.398875577Z"}, "www.phorgr.com": {"record_type": "CNAM {"record_type": "A", "resolved_at": "2023-03-14T15:57:58.140445992Z"}, "www.flatroofingsussex.co.uk": {"record_type": "CNAME", "resolv {"record_type": "A", "resolved_at": "2023-03-18T14:36:48.838056806Z"}, "blog.oneminuter.com": {"record_type": "CNAME", "resolved_at":
2023-05-12 02:57:14	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\VERMGMTBlockListFileMutex"\n "IsoScope_e44_IE_EarlyTabStart_0xd04_Mutex"\n "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "Local\\ [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\6DB145CFEEC544B1582FED1ADA3370DD]- [targetUID: 00000000-00002484]\n "69C6F 00000000-00002484]'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifier': u'string-102', u'name': u'Found decr $8<$dddAAA000***...>>>aaabbbVVV^^^xxx)111\n\n\n\n\n\n\n000777\n\n\n\n\n\n\nPPPXXXTTT<<<\n\n\n\n\n\n\nOOO4VVV\n\n\n\n\n\n\nSSS\n\n\nOOO=\n\n\nN
2023-05-12 03:08:43	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	64.226.81.48
2023-05-12 02:45:42	Physical Coordinates	No	AbstractAPI	0	0	2	0	None	34.0544, -118.244
2023-05-12 02:44:18	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:4d:72:d7:7c:dd:a7:02:dd:5a:67:f2:a2:3b:bd:d9 Signature Algorithm: sha256WithRSAE - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1-1.crt X509v3 Basic Constraints fa:29:72:01:3e:b7:06:f1:2f:1a:0e:91:c5:ec:35:bf:f5:da: 33:95:de:24:12:0d:f5:c3:23:8d:40:82:d1:5c:eb:de:0a:08: e8:e5:83:e5:0a:8b:3a:5e:

2023-05-12 03:01:19	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.164): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:48	Netblock Membership	No	Censys	0	0	3	0	None	34.148.96.0/20
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 02:56:04	Blacklisted IP on Same Subnet	Yes	DroneBL	0	0	3	0	None	dronebl.org - HTTP Proxy (87.248.157.123)
2023-05-12 03:00:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.52): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-128@openssh.com
2023-05-12 02:45:04	Country	No	Country Name Extractor	0	0	5	0	None	United States
2023-05-12 02:44:27	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Cloudflare
2023-05-12 03:08:52	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.135
2023-05-12 02:50:19	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:aa:0b:fb:f5:72:57:f7:90:57:35:0a:22:0c:3a:41:5a:d1 Signature Algorithm: sha256Wi 30:44:02:20:77:EF:CC:3A:63:43:C6:E6:6C:CD:36:4F: 64:00:42:35:30:9C:67:0E:E7:F4:15:29:43:E9:0B:EB: EA:B5:DD:47:02:20:43:3C:D6:F2:D6:6A:
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	4	0	None	15169
2023-05-12 02:50:29	Physical Address	No	GLEIF	0	0	3	0	None	C/O CORPORATION SERVICE COMPANY, 251 LITTLE FALLS DRIVE, WILMINGTON, US-DE, US, 19808
2023-05-12 02:44:20	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 02:44:31	Internet Name	No	DNS Resolver	0	0	2	0	None	pics.battleb0t.xyz
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	The Batcave (Net ID: 00:11:32:7C:A3:88)
2023-05-12 03:19:17	Web Framework	No	Web Framework Identifier	0	0	3	0	None	Bootstrap
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	permissions-policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:03:51	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	akashpmani.github.io
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	xHamster (Category: XXXPORNXXX) https://xhamster.com/users/ayshoo
2023-05-12 02:47:39	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relev N/A]\n "f_000243" has type "PNG image data 1200 x 1200 8-bit colormap non-interlaced"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\Use u'identifier': u'avtest-1', u'name': u'Sample was identified as clean by Antivirus engines', u'attck_id_wiki': None, u'threat_level_hu u'157.240.22.25', u'45.60.121.129', u'99.84.238.103', u'52.216.212.177', u'142.250.189.232', u'13.35.126.71', u'142.250.189.214', u'14
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Curiouscat (Category: social) https://curiouscat.live/login
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom474ABC (Net ID: 00:0C:F6:47:4A:BC)

2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Collaborative innovation network - Collaborative innovation is a process in which multiple players contribute towards creating new pro
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless (Net ID: 00:01:36:03:66:4F)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SHE (Net ID: 00:02:6F:3B:09:D3)
2023-05-12 02:54:34	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.117
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.199): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	P2d8T7f2d$ (Net ID: 00:18:0A:DF:81:10)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Donation Alerts (Category: business) https://www.donationalerts.com/r/login
2023-05-12 02:46:50	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	3	0	None	C=US,ST=California,L=San Francisco,O=Netlify\, Inc,CN=*.netlify.app
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	ArmorGames (Category: gaming) https://armorgames.com/user/ayhu
2023-05-12 02:54:41	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis None, u'relevance': 10, u'threat_level': 0, u'type': 8, u'description': u'Antivirus vendors marked dropped file "urlblockindex_1_.bin" type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\5SKQI1K8.txt]- [targetUID: 00000000-00002824]\n "~DFC76CE97BABDC "SUIDMmicrosoft.com/9216405899200031019875311567468310197 67*SRCHDAF=NOFORMmicrosoft.com/1024332378944031085610279713572309387 43*SRCHUI match: "whatsmyip.net"\n Heuristic match: "whatsmyip.org"\n Heuristic match: "whatsmyipaddress.org"\n Heuristic match: "whatsmypublici
2023-05-12 03:03:42	Internet Name	No	DNS Resolver	0	0	3	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:F7:C5:5E)
2023-05-12 02:44:35	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:15:41:ea:93:cd:8d:62:0f:07:0f:be:37:47:74:c1:ad:1b Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: CE:03:
2023-05-12 03:13:02	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00-evan.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:80
2023-05-12 03:06:53	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	TheCs_Kids (Net ID: 00:02:6F:F8:F3:36)
2023-05-12 02:59:47	Affiliate - Domain Whois	No	Whois	3	0	4	0	None	Domain Name: KEYUBU.NET Registry Domain ID: 2292564483_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.nicproxy.com Registrar URL: http: automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other Privacy Admin Postal Code: Redacted for Privacy Admin Country: Redacted for Privacy Admin Phone: Redacted for Privacy Admin Phone Ext: domain name registration records. NICS Telekomunikasyon A.S. does not guarantee its accuracy. By submitting a WHOIS query, you agree t
2023-05-12 03:24:22	Web Content	No	Web Spider	2	0	2	0	None	<!DOCTYPE html> <html lang="en-US"> <head> <title>Just a moment...</title> <meta http-equiv="Content-Type" content="text/html; charset xesXCsUCGNSlrn27LW82G3vB0LsnqsDVH9D7CmoXk767loN6MRiMM6E9lV7pktIJEgRREZerErCz-Gw9056q07NCPJYQafcy44fhA0Ayu8GVn0zQYz2hW6ho8NtCxWLxQfDeVy 'YtLw1r+G4BXsd0FkRMvka85wm7Lw/iR0rXUYENjW5JZbvNWZBYa0q0+Il8LjyNehJabAqUtaWf767wbCNaYgySnBqnpPsMoOa0cKWt1fZp4gdy+C8LU/pGEGRmyTt+1SC3FdT
2023-05-12 02:44:11	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	1	1	0	None	githubusercontent.com
2023-05-12 02:45:32	Malicious IP Address	Yes	PhishStats	0	1	2	0	None	Phishstats [104.21.6.166]
2023-05-	Vulnerability	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco

12 03:05:12	- CVE Low								
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.33): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:37	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 02:54:16	Linked URL - Internal	No	Web Spider	4	0	3	0	None	https://oldfluid.battleb0t.xyz/dat.gui.min.js
2023-05-12 02:52:56	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:c7:00:14:21:71:88:e2:18:10:f8:e3:ee:d1:89:37:10:7b Signature Algorithm: sha256Wi Extensions: none Signature : ecdsa-with-SHA256 30:45:02:20:5E:6B:E1:80:95:E9:06:B9:64:A1:6D:DC: F7:46:19:D7:44:B3:41:56:D0:CD:B2:17:79
2023-05-12 02:54:38	Physical Location	No	Censys	0	0	3	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	hhcpa (Net ID: 00:06:25:3B:8E:36)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Andrea Schwartz Gallery 5G (Net ID: 00:01:9F:3D:4F:6C)
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00lt00.github.io
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.113): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:53:15	IP Address	No	Mnemonic PassiveDNS	0	0	1	0	None	185.199.108.153
2023-05-12 03:18:46	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Horizontal (normal) @ 18}
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	6	0	None	cross-origin-embedder-policy: require-corp
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	4	0	None	15169
2023-05-12 02:53:39	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	setlist.fm (Category: music) https://www.setlist.fm/user/login
2023-05-12 03:32:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.9:80
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MHeckmans (Net ID: 00:02:CF:CB:87:99)
2023-05-12 02:54:19	HTTP Headers	No	Web Spider	6	0	4	0	None	{"nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "alt-svc": "h3=\":443\"; ma=86400, h3-29=\":443\"; ma=
2023-05-12 02:44:12	SSL Certificate - Issued to	No	SSL Certificate Analyzer	0	0	2	0	None	CN=*.cloudwaysapps.com
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.202): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:8443
2023-05-12 03:36:20	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.128:8080
2023-05-12 03:12:10	Affiliate Description - Category	No	DuckDuckGo	0	0	5	0	None	Search engine optimization metrics - A number of metrics are available to marketers interested in search engine optimization. Search e
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	xHamster (Category: XXXPORNXXX) https://xhamster.com/users/login

2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	monks56 (Net ID: 00:06:25:C3:88:45)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F0:97:C1)
2023-05-12 02:55:25	Username	No	Social Network Identifier	43	0	4	0	None	Altpapier
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.49): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 02:53:04	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.111.153:443
2023-05-12 02:44:19	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	www.github.com
2023-05-12 02:47:26	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'https://attack.mitre.org/techniques/T1071/001', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.001', u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 9, u'description': u'Spawned process "rundll32.exe" with commandline Class" (Path: "HKCU\\CLSID\\{D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}\\INPROCSERVER32")\n "rundll32.exe" touched "Groove Explorer Icon Ov 00AA004AE837}\\INPROCSERVER32")\n "rundll32.exe" touched "User Assist" (Path: "HKLM\\SOFTWARE\\CLASSES\\CLSID\\{DD313E04-FEFF-11D1-8EC
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	3019fc (Net ID: 00:02:2D:30:19:FC)
2023-05-12 02:47:46	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\IsoScope_e88_IESQMMUTEX_0_331"\n "Local\\!BrowserEmulation!SharedMemory!Mutex"\n "{5312EE61-79E3-4A2 rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: getbootstrap.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "user-agent: directory', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 3, u'th Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\TFIYPCCB.txt]- [targetUID: 00000000-00003720]\n "RecoveryStore._88B090C0-D917-11E7-
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	NH-NEW (Net ID: 00:01:21:30:F0:42)
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	200WMadison (Net ID: 00:01:21:30:9B:1B)
2023-05-12 02:55:18	Raw Data from RIRs	No	Censys	13	0	3	0	None	{"operating_system": {"vendor": "Ubuntu", "product": "Linux", "part": "o", "uniform_resource_identifier": "cpe:2.3:o:canonical:ubuntu_ ["sha256:74d4fa601a4a1f78b519a7bc16ea591fab7d4addbe589649de627c34c4e0d38a"], "source_ip": "167.94.145.60", "extended_service_name": "S "hmac-sha2-256", "hmac-sha2-512", "hmac-sha1"], "first_kex_follows": false, "kex_algorithms": ["curve25519-sha256", "curve25519-sha256
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	mail.ayhu.xyz
2023-05-12 03:03:59	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	ply.gg
2023-05-12 02:59:53	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2011-3389 https://nvd.nist.gov/vuln/detail/CVE-2011-3389 Score: 4.3 Description: The SSL protocol, as used in certain configuratio
2023-05-12 02:44:13	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	1	2	0	None	github.io
2023-05-12 02:59:54	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	jdenig@generalatlantic.com
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.195): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:54	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	NAMECHEAP INC

2023-05-12 03:13:05	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0067ed.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	20654 (Net ID: 00:0D:3A:27:40:51)
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/withat_1.jpg
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	MCUUID (Minecraft) (Category: gaming) https://mcuuid.net/?q=login
2023-05-12 02:44:21	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 02:52:56	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	None None
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	FRANZ (Net ID: 00:01:24:F2:7F:35)
2023-05-12 03:43:29	Country	No	Country Name Extractor	0	0	6	0	None	Germany
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet24CE (Net ID: 00:01:36:59:24:CC)
2023-05-12 02:45:30	Physical Location	No	ipapi.co	0	0	3	0	None	North Charleston, South Carolina, SC, United States, US
2023-05-12 02:55:15	Netblock Membership	No	Censys	3	0	3	0	None	165.232.112.0/20
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00feng00.github.io
2023-05-12 03:00:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.5): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:32:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.4:8080
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	Reddit (Category: social) https://www.reddit.com/user/Battleb0t
2023-05-12 03:23:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.9:80
2023-05-12 03:01:03	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.110): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:51	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H06G1NS24K8856E7B6C2JF02 Date: <REDACTED> Content-Length: 0
2023-05-12 02:44:29	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	cloudwaysapps.com
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	wilson (Net ID: 00:02:2D:08:06:B3)
2023-05-12 02:50:30	Physical Address	No	GLEIF	0	0	3	0	None	C/O CORPORATION SERVICE COMPANY, 251 LITTLE FALLS DRIVE, WILMINGTON, US-DE, US, 19808
2023-05-12 03:00:01	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	support@yeulpay.com
2023-05-12 03:18:58	WiFi Access	No	Wigle.net	0	0	5	0	None	CCAZ (Net ID: 00:02:6F:EA:D0:4E)

	Point Nearby								
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MOT-1-7F (Net ID: 00:18:C0:62:7F:7F)
2023-05-12 02:46:18	Affiliate Description - Category	No	DuckDuckGo	0	0	2	0	None	Internet security
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	tsunami (Net ID: 00:0D:29:AC:D4:3E)
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.201): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:15	Linked URL - External	No	Web Spider	0	0	3	0	None	https://sky.shiiyu.moe
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	myLGNet (Net ID: 00:02:A8:B1:C8:F5)
2023-05-12 03:33:28	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [185.199.111.154] https://www.virustotal.com/en/ip-address/185.199.111.154/information/
2023-05-12 02:54:03	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cf-ray: 7c5f606679610ce9-EWR
2023-05-12 02:45:42	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'San Francisco (South Beach)', u'security': {u'is_vpn': False}, u'city_geoname_id': 5326621, u'region_geoname_id': 5332921,
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ZyXEL (Net ID: 00:13:49:64:69:8A)
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.202): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:03	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:24:22	Web Content Type	No	Web Spider	0	0	2	0	None	text/html;charset=utf-8
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Burfas28 (Net ID: 00:15:6D:7C:EF:0A)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	new network (Net ID: 00:02:2D:08:76:AE)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomE46DB8 (Net ID: 00:0C:F6:E4:6D:B8)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	McDonalds Free WiFi (Net ID: 00:14:6A:5B:53:90)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	tradingview (Category: finance) https://www.tradingview.com/u/login/
2023-05-12 03:00:14	Internet Name	No	Certificate Transparency	0	0	1	0	None	www.ayhu.xyz
2023-05-12 03:10:00	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	telleria.com
2023-05-12 03:01:00	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.101): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:2053
2023-05-12 02:44:21	Internet Name	No	DNS Resolver	0	0	2	0	None	nuke.battleb0t.xyz

2023-05-12 03:00:57	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	01.github.io
2023-05-12 02:45:04	Country	No	Country Name Extractor	0	0	2	0	None	British Indian Ocean Territory
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	RhodeNet (Net ID: 00:02:2D:0F:8E:DF)
2023-05-12 02:54:23	Web Content	No	Web Spider	0	0	4	0	None	*{box-sizing:border-box;margin:0;padding:0}html{line-height:1.15;-webkit-text-size-adjust:100%;color:#313131}html,button{font-family:s image:url(prompt:not(.hidden){flex-wrap:wrap;justify-content:center}}.pow-button{margin:2rem 0;background-color:#0051c3;color:#fff}.pow-button:h color:#4693ff}}body.dark{background-color:#222;color:#d9d9d9}body.dark a{color:#fff}body.dark a:hover{text-decoration:underline;color:
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	message_me (Category: social) https://mssg.me/login
2023-05-12 02:54:51	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H06V19Y9J57EVG1E6053DPH4 Date: <REDACTED> Content-Length: 0
2023-05-12 03:03:34	Co-Hosted Site - Domain Name	No	DNS Resolver	2	0	3	0	None	00ffcc.cn
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00cybermonk00.github.io
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MatrixEx BYOD (Net ID: 00:01:21:26:54:B1)
2023-05-12 02:59:57	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	sheila.christianson@ftb.ca.gov
2023-05-12 03:27:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.128:8080
2023-05-12 03:24:22	Web Content Type	No	Web Spider	0	0	4	0	None	text/html;charset=utf-8
2023-05-12 03:10:03	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	netcraft.com
2023-05-12 02:55:18	Software Used	Yes	Censys	0	0	3	0	None	OpenBSD OpenSSH 8.9p1
2023-05-12 02:54:38	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	4	0	2	0	None	Cloudflare\, Inc.
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:00:C5:DB:8B:88)
2023-05-12 03:32:04	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.3:8443
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	BLINK-6985 (Net ID: 00:03:7F:A1:AE:79)
2023-05-12 03:23:19	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.5:8443
2023-05-12 02:54:03	Netblock Membership	No	Censys	0	0	2	0	None	172.67.128.0/20
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_ipad (Net ID: 00:0C:E6:08:02:05)
2023-05-12 02:45:32	Raw Data from RIRs	No	PhishStats	1	0	2	0	None	[{u'page_text': None, u'domain': u'ecloanmoney.com', u'virus_total': u'Yes', u'n_times_seen_ip': 0, u'abuse_contact': u'abuse@ecloanmo
2023-05-12 03:24:21	Web Content	No	Web Spider	2	0	4	0	None	<!DOCTYPE html> <html lang="en-US"> <head> <title>Just a moment...</title> <meta http-equiv="Content-Type" content="text/html; charset Aw2gGE9OL21frfN9JEzkR172OTICxrUfc7caDwzr9D9_NePtArl9cLDKFHEvxIxzgioPuODDLvyAfvi0dPWiWhMq7WkvCuoWovUiUA253wYEf7M9x4gD8lnc3kaUCBX9tFmIaj

									'TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgMTAuMDsgV2luNjQ7IHg2NDsgcnY6NjIuMCkgR2Vja28vMjAxMDAxMDEgRmlyZWZveC82Mi4w', rm: 'R0VU', d: 'QLdIKmVk90 [0].appendChild(cpo); }()); </script> </body> </html>
2023-05-12 02:44:15	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3030::ac43:a8fc
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.116): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.191): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/jcqn.jpg
2023-05-12 03:03:36	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:09:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:00:0B:63:00:0B)
2023-05-12 02:54:07	Physical Location	No	Censys	1	0	2	0	None	Rosemont, Illinois, 60018, United States, North America
2023-05-12 03:00:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha1-etm@openssh.com
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:2095
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Cross-platform software
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom92EE90 (Net ID: 00:0C:F6:92:EE:90)
2023-05-12 03:16:31	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'HE', u'country_tld': u'.de', u'ip': u'207.154.228.169', u'currency_name': u'Euro', u'currency': u'EUR', u'country_p
2023-05-12 03:09:54	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.108.133:443
2023-05-12 03:42:54	Affiliate - Domain Whois	No	Whois	0	0	6	0	None	% Restricted rights. % % Terms and Conditions of Use % % The above data may only be used within the scope of technical or % administra
2023-05-12 02:45:57	Physical Location	No	MetaDefender	0	0	2	0	None	San Francisco, United States
2023-05-12 03:13:07	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00indahouse.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:8443
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MainSurf (Net ID: 00:02:2D:67:EF:5F)
2023-05-12 03:03:31	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	eminent926 (Net ID: 00:14:5C:86:C4:D6)
2023-05-12 02:44:32	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:04:02:53:52:8b:ff:fb:8a:0a:11:44:e7:ab:f5:69:c5:9e Signature Algorithm: sha256Wi E2:5C:6F:49:73:2D:91:13:E2:7A:C0:23:16:9D:9E:E9: 34:9D:A8:4E:A2:02:21:00:E3:DA:6F:CF:C9:A3:6F:47: 24:1E:42:4E:CB:2C:6D:AC:F1:F2:5C:4B:
2023-05-12 02:57:22	Internet Name	No	Certificate Transparency	0	0	1	0	None	vscode.battleb0t.xyz
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.44): Search Engine Last Activity: 0 days ago Threat Level: 29

2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	104.21.71.14
2023-05-12 02:46:54	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	3	0	None	cloudflare
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0047ol.github.io
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	TSMD 2.4 (Net ID: 00:02:6F:FD:8B:6E)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	GP (Net ID: 00:01:24:F1:7F:54)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Galatasaray (Net ID: 00:02:CF:E2:4D:A2)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	6	0	None	cross-origin-resource-policy: same-origin
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Heylink (Category: misc) https://heylink.me/ayhu/
2023-05-12 03:32:11	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.6:8443
2023-05-12 02:45:36	Affiliate - Internet Name	No	DNS Raw Records	0	0	2	0	None	frabjous-lebkuchen-324004.netlify.app
2023-05-12 02:54:19	Web Content Type	No	Web Spider	0	0	2	0	None	text/html;charset=utf-8
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.235): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet (Net ID: 00:01:36:2E:39:B8)
2023-05-12 03:01:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.252): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.131): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.76): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom (Net ID: 00:0C:F6:34:4B:10)
2023-05-12 02:54:12	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"www.yeulpay.com"\n "yeulpay.com"'}, {u'category': u' 00005812]\n "4c8bd346-dc18-45c0-b9fa-b2f2b3599a07.tmp" has type "UTF-8 Unicode text with very long lines with no line terminators"- Lo u'CAPEC-497', u'attck_id': u'T1083', u'relevance': 0, u'threat_level': 0, u'type': 8, u'description': u'"wallet-drawer.bundle.js.LICEN "C:\\Users\\%OSUSER%\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations\\O3IGZQ735L74LO6YZ5IP.temp"\n "msedge.exe" tryi
2023-05-12 02:55:36	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "msedge.exe" loaded module "NTDLL.DLL" at base e7fc0000\n "msedge.exe" loaded module "API-MS-WIN-DOWNLEVEL-SHELL32-L1-1-0.DLL" at base RC4 Encryption', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1486', u'threat_level_human': u'informative', u'capec_id': N [%TEMP%\\6648_221812043_metadata\\verified_contents.json]- [targetUID: 00000000-00006648]\n "settings.dat" has type "data"- Location Antivirus vendors marked sample as malicious (1% detection rate)'}], u'threat_level': 1, u'size': None, u'job_id': u'63fc26ad86a713231
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	BiggerPockets (Category: finance) https://www.biggerpockets.com/users/login
2023-05-12 02:54:19	Linked URL - Internal	No	Web Spider	4	0	3	0	None	https://fluid.battleb0t.xyz/./script.js
2023-05-12 02:53:14	Raw Data from RIRs	No	Hybrid Analysis	2	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "142.251.46.230:443"\n "142.251.46.170:443"\n "52.155.62.95:443"\n "172.217.12.118:443"\n "172.217.12.97:443"\n "142.250.189.238:443"' "VISITOR_INFO1_LIVEi1ZA35yJPt8youtube.com/2147492865342530995231067463905972348310312 37CONSENTWP.2676bayoutube.com/1024313833881632108

									u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 8, u'description': u'Antivirus ve reads file "c:\\users\\%osuser%\\appdata\\local\\temp\\~dfe5a84e0c629be7b2.tmp"\n "iexplore.exe" reads file "c:\\users\\%osuser%\\favo
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.153): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomC3D648 (Net ID: 00:0C:F6:C3:D6:48)
2023-05-12 03:24:30	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	NAMECHEAP INC
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	typhoon (Net ID: 00:14:C1:39:FA:69)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	helena (Net ID: 00:06:25:90:14:E1)
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:59:09	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:18:ae:06:7e:fc:0b:78:46:5c:8b:fe:1a:31:bf:5b:16:b8 Signature Algorithm: sha256Wi Extensions: none Signature : ecdsa-with-SHA256 30:46:02:21:00:E2:3A:9E:51:10:7B:4C:32:13:F1:5A: 6A:72:5F:B6:48:D3:B8:D4:7D:48:A2:D1:1B
2023-05-12 03:09:30	Co-Hosted Site - Domain Name	No	DNS Resolver	2	0	3	0	None	ply.gg
2023-05-12 03:28:39	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.160:8080
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	StreamLabs (Category: finance) https://streamlabs.com/Altpapier/tip
2023-05-12 03:23:35	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.13:8080
2023-05-12 03:32:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.12:8443
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Bandlab (Category: music) https://www.bandlab.com/ayshoo
2023-05-12 03:16:28	Physical Location	No	ipapi.co	0	0	3	0	None	Frankfurt am Main, Hesse, HE, Germany, DE
2023-05-12 03:04:14	Malicious Affiliate	Yes	abuse.ch	0	1	3	0	None	abuse.ch URLhaus (Domain) [cdn-185-199-111-153.github.com] https://urlhaus.abuse.ch/downloads/csv_recent/
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	007us.github.io
2023-05-12 02:57:13	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "IsoScope_3e0_IESQMMUTEX_0_303"\n "Local\\URLBLOCK_FILEMAPSWITCH_MUTEX_992"'}, {u'category': u'General', u'origin': u'Network Traffic' [targetUID: 00000000-00000604]\n "RecoveryStore._C7A4F1AE-D920-11E7-B48D-080027D44A30_.dat" has type "Composite Document File V2 Docum "data"- Location: [%TEMP%\\~DF8765436AF976415F.TMP]- [targetUID: 00000000-00000992]\n "Tar1485.tmp" has type "data"- Location: [%TEMP% scanned on 09/20/2022 00:18:36)\n File SHA256: 78552f5436b9bf8f079510592f7d61c991abc31f687db116c76cda7b3d1de8dd (AV positives: 3/74 sc
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	" (Cloaked) (Net ID: 00:01:36:59:CB:CF)
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:2082
2023-05-12 02:56:21	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 09:cc:cb:40:35:8f:10:16:7b:c7:37:cb:94:7e:31:1a Signature Algorithm: ecdsa-with-SHA
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet92D6 (Net ID: 00:01:36:5B:92:D4)
2023-05-12 02:44:14	IPv6 Address	No	DNS Resolver	15	0	1	0	None	2606:50c0:8002::153
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	2WIRE514 (Net ID: 00:02:2D:8C:DC:7C)

2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Flickr (Category: images) https://www.flickr.com/photos/login/
2023-05-12 03:17:44	Account on External Site	No	Account Finder	0	0	1	0	None	Reddit (Category: social) https://www.reddit.com/user/ BattleB0t_
2023-05-12 03:09:31	Co-Hosted Site - Domain Name	No	DNS Resolver	2	0	3	0	None	scoop.sh
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.232): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:00	Malicious IP on Same Subnet	Yes	CINS Army List	0	0	4	0	None	cinsscore.com [207.154.224.0/20] http://cinsscore.com/list/ci-badguys.txt
2023-05-12 03:00:50	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-ye.github.io
2023-05-12 03:13:06	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [007hyno.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:45:26	Physical Location	No	ipapi.co	0	0	3	0	None	Toronto, Ontario, ON, Canada, CA
2023-05-12 03:32:11	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.6:8080
2023-05-12 03:19:22	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.109.153:80
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2053
2023-05-12 02:58:11	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\VERMGMTBlockListFileMutex"\n "Local\\ZonesCacheCounterMutex"\n "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "IsoScope_bb4_IE_EarlyTabSta "regular_1_.png" has type "PNG image data 70 x 70 8-bit/color RGBA non-interlaced"- [targetUID: N/A]\n "3538626A1FCCCA43C7E18F220BDD9B file"- Location: [%TEMP%\\CabDD59.tmp]- [targetUID: 00000000-00003196]\n "EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC062 Alive\nAccept: */*\nUser-Agent: Microsoft-CryptoAPI/6.1\nHost: ocsp.godaddy.com"- [Source: PCAP]\n Heuristic match: "crl.godaddy.com"-
2023-05-12 02:44:48	Raw Data from RIRs	No	CRXcavator	0	0	1	0	None	[{"platform": "Chrome", "extension_id": "mdcffelghikdiafnfodjlglllenhlnejl", "name": "GayHub", "icon": "https://lh3.googleusercontent.c
2023-05-12 02:58:44	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"34.74.170.74 [targetUID: N/A]\n "_7B887D42-4986-11ED-AB02-0800276C7FB6_.dat" has type "Composite Document File V2 Document Cannot read section info Cannot read section info"- [targetUID: N/A]\n "httpErrorPagesScripts_1_" has type "UTF-8 Unicode (with BOM) text with CRLF line termin u'sha256': u'fb77b9fcfedf278c3a95dd022207815d527f6c39672b7d4bb735ccbd564c337b', u'sha512': u'4f7bd48309dcc7b5917de449f1e56343cb22f52f6
2023-05-12 02:45:38	Physical Location	No	MetaDefender	0	0	2	0	None	San Francisco, United States
2023-05-12 02:46:49	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 03:19:47	Account on External Site	No	Account Finder	0	0	2	0	None	GitHub (Category: coding) https://github.com/patrickpogoda
2023-05-12 02:50:03	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "rundll32.exe" with commandline "%WINDIR%\\system32\\shell32.dll,OpenAs_RunDLL %USERPROFILE%\\Downlo ..." (UID: 00000000-00002788)\n S ""%USERPROFILE%\\Downloads\\site.webmanifest"" (UID: 00000000-00002672)'}, {u'category': u'General', u'origin': u'Registry Access', u' touched "Start Menu Cache" (Path: "HKCU\\CLSID\\{660B90C8-73A9-4B58-8CAE-355B7F55341B}\\TREATAS")\n "rundll32.exe" touched "Start Menu u'T1012', u'relevance': 3, u'threat_level': 0, u'type': 3, u'description': u'"rundll32.exe" (Path: "HKLM\\SYSTEM\\CONTROLSET001\\CONTR
2023-05-12 03:00:56	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.93): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:25	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:44:13	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	2	0	None	www.github.com
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATTaFmrKmS (Net ID: 78:23:AE:39:B2:90)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	PDI (Net ID: 00:06:25:FE:34:4D)

2023-05-12 03:23:09	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.0:8080
2023-05-12 03:43:57	URL (Purely Static)	No	Page Information	0	0	3	0	None	https://kekw.battleb0t.xyz/jar
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Room 208 (Net ID: 00:02:2D:66:D4:6B)
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:44:05	SSL Certificate Expiring	Yes	CertSpotter	0	0	1	0	None	2023-05-14 15:23:50
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Capsmanagement (Net ID: 00:01:21:1C:AD:40)
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	MCName (Minecraft) (Category: gaming) https://mcname.info/en/search?q=ayshoo
2023-05-12 03:00:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	aes256-gcm@openssh.com
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.223): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:19	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2600:1f18:2489:8201::c8
2023-05-12 03:14:48	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 5.9 Description: OpenVPN, when using a 64-bit block cipher, makes
2023-05-12 02:44:22	Physical Location	No	ipstack	0	0	2	0	None	United States
2023-05-12 02:45:34	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	route2.mx.cloudflare.net
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	sflan11 (Net ID: 00:02:6F:08:21:EE)
2023-05-12 03:21:44	Account on External Site	No	Account Finder	0	0	2	0	None	PinkBike (Category: hobby) https://www.pinkbike.com/u/dawid.sulej/
2023-05-12 02:51:43	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:4e:82:1a:86:ae:7d:8a:39:3c:25:24:c6:46:df:b3:a2:f4 Signature Algorithm: sha256Wi Extensions: none Signature : ecdsa-with-SHA256 30:45:02:21:00:B5:F3:29:BD:A0:20:09:5F:ED:BA:FE: 7D:4D:29:A6:16:28:D4:3D:6D:9D:84:56:4B
2023-05-12 02:44:15	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	funny.battleb0t.xyz:443
2023-05-12 03:09:12	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	207.154.228.160
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Canyon Crossing WiFi-scanning (Net ID: 00:18:0A:51:68:AC)
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:993
2023-05-12 03:03:29	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	QUEER (Category: social) https://queer.pl/user/login
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-6922 (Net ID: 00:1D:D4:19:69:20)
2023-05-12 02:53:45	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 02:58:46	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	1	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 5.9 Description: OpenVPN, when using a 64-bit block cipher, makes

2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	InsaneJournal (Category: social) https://login.insanejournal.com/profile
2023-05-12 03:23:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.7:8080
2023-05-12 02:44:23	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	2WIRE522 (Net ID: 00:01:E6:93:CB:2D)
2023-05-12 03:03:35	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://pics.battleb0t.xyz/images/random_5.png
2023-05-12 03:13:04	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00088.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:00:26	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-64-etm@openssh.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Spotify (Category: music) https://open.spotify.com/user/login
2023-05-12 02:53:32	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 03:22:42	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	ayhu.com.br
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	slideshare (Category: social) https://www.slideshare.net/ayshoo
2023-05-12 02:45:32	Physical Location	No	ipapi.co	0	0	3	0	None	North Charleston, South Carolina, SC, United States, US
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:05:5D:EC:9E:68)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:A3:7E:2A)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	art_vacation5.0 (Net ID: 00:01:9F:30:06:7C)
2023-05-12 02:53:12	Raw Data from RIRs	No	Tool - WAFW00F	1	0	3	0	None	[{"url": "https://panel.battleb0t.xyz", "firewall": "Cloudflare", "detected": true, "manufacturer": "Cloudflare Inc."}, {"url": "https
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:74:92:82:51)
2023-05-12 03:01:05	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.113): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:14	IP Address	No	DNS Resolver	59	0	1	0	None	104.21.6.166
2023-05-12 03:01:18	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.163): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:59:59	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	info@cndglobelogistics.com
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.57): Search Engine Last Activity: 0 days ago Threat Level: 29

2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_ipad (Net ID: 00:0C:E6:08:0B:05)
2023-05-12 02:46:20	Netblock Membership	No	RIPE	10	0	2	0	None	185.199.111.0/24
2023-05-12 02:46:26	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "IsoScope_a1c_ConnHashTable<2588>_HashTable_Mutex"\n "IsoScope_a1c_IESQMMUTEX_0_331"\n "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "Loc u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 7, u'threat_level': 0, u'type': 2, u'descri (d||e||f||g.length||h.length))return;var n={Gf:d,Ef:e,Ff:f,lg:g,mg:h,gd:l,Xa:b},p=z.YT,q=function(){Vy(n)};if(p)return p.ready&&p.read ["customScripts","customPixels","nonGooglePixels","nonGoogleScripts","nonGoogleIframes"],customScripts:["html","customPixels","nonGoog
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	KFA (Net ID: 00:00:CB:07:81:0E)
2023-05-12 02:54:19	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://nuke.battleb0t.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:5D:5F:35)
2023-05-12 02:50:17	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BBHWIRELESS (Net ID: 00:00:C5:D7:63:F4)
2023-05-12 02:55:15	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: <REDACTED> Content-Type: text/html Transfer-Encoding: chunked Connection: k
2023-05-12 03:15:35	Web Content Language	No	Language Detector	0	0	3	0	None	English
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Wir (Net ID: 00:01:E3:51:05:D5)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless (Net ID: 00:01:36:07:50:41)
2023-05-12 02:58:34	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 1, u'threat_level': 0, u'type': 7, u'description': u'"texassuntexasmoon.com"'}, {u'category': u'General', u'origin': u'Binary File', u type "Microsoft Cabinet archive data Windows 2000/XP setup 62919 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 comp "QMOFOY6E.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\QMOFOY6E.txt]- [targetUID: 00000000-00003544] u'https://attack.mitre.org/techniques/T1573', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1573', u'relev
2023-05-12 02:55:05	Netblock Membership	No	Censys	334	0	2	0	None	188.114.97.0/24
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 03:03:16	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	webdisk.ayhu.xyz
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	001wwang.github.io
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Rock Chalk (Net ID: 00:01:95:08:D8:04)
2023-05-12 03:09:42	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	118.97.148.34.bc.googleusercontent.com
2023-05-12 02:44:23	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS RSA SHA256 2020 CA1
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	cf-mitigated: challenge
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.205): Search Engine Last Activity: 0 days ago Threat Level: 29

2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	Pronouns.Page (Category: social) https://pronouns.page/api/profile/get/battleb0t?version=2
2023-05-12 02:46:49	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 02:44:29	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	2	0	None	github.io
2023-05-12 02:45:02	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'CA', u'country_tld': u'.us', u'ip': u'2606:50c0:8002::153', u'currency_name': u'Dollar', u'currency': u'USD', u'cou
2023-05-12 02:45:11	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'ON', u'country_tld': u'.ca', u'ip': u'172.67.135.9', u'currency_name': u'Dollar', u'currency': u'CAD', u'country_po
2023-05-12 03:36:20	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.128:80
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Good Times (Net ID: 00:02:2D:29:A2:94)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cross-origin-resource-policy: same-origin
2023-05-12 02:44:26	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:12:55	Physical Location	No	numverify	0	0	3	0	None	Phoenix, US
2023-05-12 02:44:15	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Open Graph
2023-05-12 02:50:19	Physical Location	No	ipstack	0	0	3	0	None	United States
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	6	0	None	cloudflare
2023-05-12 02:55:18	Open TCP Port Banner	No	Censys	0	1	3	0	None	SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
2023-05-12 02:45:31	Raw Data from RIRs	No	PhishStats	0	0	2	0	None	[{u'page_text': u' ', u'domain': None, u'virus_total': None, u'n_times_seen_ip': None, u'abuse_contact': None, u'ip': u'185.199.111.15
2023-05-12 02:53:42	BGP AS Membership	No	Censys	0	0	2	0	None	54113
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:03:10:83)
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	3	0	None	cloudflare
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	bsbmuh (Net ID: 00:08:5C:F1:78:3B)
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:2086
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	6	0	None	Nics Telekomunikasyon Ltd.
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	WaveLAN Network (Net ID: 00:02:2D:1B:7E:B1)
2023-05-12 02:46:17	Affiliate Description - Abstract	No	DuckDuckGo	0	0	3	0	None	GitHub, Inc. is an Internet hosting service for software development and version control using Git. It provides the distributed versio
2023-05-12 03:09:49	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	79.170.74.34.bc.googleusercontent.com
2023-05-12 02:44:17	Co-Hosted Site -	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com

	Domain Name								
2023-05-12 03:03:25	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:01:24:F2:E2:35)
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:2052
2023-05-12 03:31:32	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namecheap.com
2023-05-12 02:45:25	Physical Location	No	MetaDefender	0	0	2	0	None	San Francisco, United States
2023-05-12 03:31:32	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	6	0	None	abuse@namecheap.com
2023-05-12 03:03:42	Internet Name	No	DNS Resolver	0	0	3	0	None	nwapi.battleb0t.xyz
2023-05-12 03:00:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.31): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.195): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:41:52	Netblock Membership	No	Censys	0	0	3	0	None	45.131.109.0/24
2023-05-12 02:44:59	Similar Domain	Yes	Similar Domain Finder	1	0	1	0	None	tayhu.xyz
2023-05-12 03:13:07	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00feng00.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	GP (Net ID: 00:01:24:F1:7F:54)
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.251): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:16	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2023-05-12 02:46:35	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': "77EC63BDA74BD0D0E0426DC8F8008506" has type "Microsoft Cabinet archive data Windows 2000/XP setup 62582 bytes 1 file at 0x2c +A "authr Font Format TrueType length 25996 version 1.1"- [targetUID: N/A]\n "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has type "MS Wi "https://play.google.com/store/apps/details?id=com.StickyGames.PLCEmulatorProject"\n Pattern match: "https://fonts.googleapis.com/css?
2023-05-12 03:23:38	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.14:8080
2023-05-12 02:54:13	Web Content Type	No	Web Spider	0	0	3	0	None	text/css;charset=utf-8
2023-05-12 03:13:01	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-fog.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/random_1.jpeg
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Gitea - Gitea is a forge software package for hosting software development version control using Git as well as other collaborative fe
2023-05-12 02:46:02	Physical Coordinates	No	AbstractAPI	0	0	3	0	None	32.8608, -79.9746
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:FD:45:77)
2023-05-	Malicious	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00jew.github.io] https://www.openphish.com/feed.txt

12 03:13:07	Co-Hosted Site								
2023-05-12 03:09:47	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	69.170.74.34.bc.googleusercontent.com
2023-05-12 02:44:38	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	HTTP/3
2023-05-12 03:24:21	HTTP Status Code	No	Web Spider	0	0	2	0	None	403
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=sZlRfK%2B18hvKHsoLJ40BkYB4lHX60aBHph6G1vTBEuSHhMJnpf00BL
2023-05-12 03:37:23	Physical Location	No	MetaDefender	0	0	3	0	None	Frankfurt Am Main, Germany
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Flipboard (Category: tech) https://flipboard.com/@login
2023-05-12 02:50:19	Physical Location	No	ipstack	0	0	3	0	None	United States
2023-05-12 03:22:54	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.1:8080
2023-05-12 02:46:53	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	teamcity.battleb0t.xyz
2023-05-12 03:24:21	Web Content Type	No	Web Spider	0	0	3	0	None	text/html;charset=utf-8
2023-05-12 03:41:36	Physical Coordinates	No	AbstractAPI	100	0	3	0	None	50.8897, 6.0563
2023-05-12 03:16:29	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'HE', u'country_tld': u'.de', u'ip': u'46.101.229.70', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	2	0	None	Domain Names REG.RU LLC
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	AGTLinksys (Net ID: 00:0C:41:75:B6:62)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BeensGroep (Net ID: 00:01:21:1F:B1:90)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	PHILIPS_B81A7F (Net ID: 00:0B:3B:D9:1B:59)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATT639BrM3 (Net ID: 38:3B:C8:ED:A2:0A)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Pokerstrategy (Category: gaming) http://www.pokerstrategy.net/user/login/profile/
2023-05-12 03:03:36	Co-Hosted Site - Domain Name	No	DNS Resolver	2	0	3	0	None	00rz.com
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Blogspot (Category: blog) http://Altpapier.blogspot.com
2023-05-12 03:03:34	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:46:55	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Maingau (Net ID: 00:02:2D:66:94:56)
2023-05-12	SSL Certificate -	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:57:f8:5f:6c:a4:d7:b1:d8:61:78:13:80:db:41:a4:54:3d Signature Algorithm: sha256Wi

02:51:31	Raw Data								Extensions: none Signature : ecdsa-with-SHA256 30:46:02:21:00:D4:53:59:2F:EB:FF:FB:09:BA:76:BB: E9:A4:81:C3:B1:93:13:10:22:54:A7:54:1C
2023-05-12 03:24:47	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 02:54:22	Web Content Type	No	Web Spider	0	0	3	0	None	text/html
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	myLGNet (Net ID: 00:02:A8:96:B6:F1)
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
2023-05-12 03:03:42	Internet Name	No	DNS Resolver	0	0	3	0	None	funny.battleb0t.xyz
2023-05-12 03:00:25	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha2-256-etm@openssh.com
2023-05-12 02:45:17	Physical Location	No	ipapi.co	0	0	4	0	None	Toronto, Ontario, ON, Canada, CA
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	CableWiFi (Net ID: 00:0D:67:66:08:16)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ISHLT-Corp (Net ID: 00:01:21:30:59:78)
2023-05-12 03:09:37	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	225.30.196.104.bc.googleusercontent.com
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	logitec-99c005 (Net ID: 00:01:8E:99:C0:04)
2023-05-12 02:59:34	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	ok.ru (Category: social) https://ok.ru/login
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.71): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.177): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:25	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:25:09	Internet Name	No	DNS Brute-forcer	0	0	1	0	None	www.battleb0t.xyz
2023-05-12 03:09:34	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	210.30.196.104.bc.googleusercontent.com
2023-05-12 02:53:45	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:EE:43:99)
2023-05-12 02:44:35	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Open Graph
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:02:DD:85:3E:34)
2023-05-12 02:56:58	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/ein_1.png

02:54:18									
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00d2.github.io
2023-05-12 02:46:04	Physical Location	No	AbstractAPI	0	0	3	0	None	North Charleston, South Carolina, 29415, United States, North America
2023-05-12 02:44:29	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:10:8b:16:97:4c:80:e7:56:d7:06:74:1e:45:16:d2:cf:08 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: A8:1A: 2d:77:e4:5c:18:4d:90:25:51:13:68:40:ac:f8:0c:fc:86:c6: 34:50:55:8e:da:35:b1:44:f3:0d:df:99:4c:2f:5a:3f:d4:52: 8d:52:80:94:14:ff:5b:30:
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	angelique (Net ID: 00:0B:6C:C7:12:D8)
2023-05-12 02:45:36	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'identifier': u'network-0', u'name': u'Contacts domains', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_le bit/color RGBA non-interlaced" and extension "png"\n "tab-content-2-3_1_.png" has type "PNG image data 552 x 338 8-bit/color RGBA non- Location: [%TEMP%\\~DFFA2460BF0619E6A5.TMP]- [targetUID: 00000000-00003588]\n "~DF3C66DECFD1719D57.TMP" has type "data"- Location: [%T "MUID089815D4E5BB620D23EC06D1E43F63D8msn.com/1025236672311088933061233384310304 21*"\n Pattern match: "SUIDMmicrosoft.com/9216415271475
2023-05-12 02:54:29	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'type': 7, u'description': u'"104.21.62.177:80"\n "104.21.62.177:443"\n "172.217.12.104:443"\n "104.17.25.14:443"\n "172.67.178.49:44 u'General', u'origin': u'Binary File', u'identifier': u'binary-16', u'name': u'Drops files marked as clean', u'attck_id_wiki': None, u [targetUID: N/A]\n "login_1_.png" has type "PNG image data 110 x 44 8-bit/color RGBA non-interlaced"- [targetUID: N/A]\n "livechat_1_. "v3.1.2code.google.com/p/crypto-js(c)"\n Pattern match: "http://github.com/jrburke/requirejs"\n Pattern match: "https://100tst.sbs/bds
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://pics.battleb0t.xyz/images/jonas.PNG
2023-05-12 02:46:49	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	3	0	None	cloudwaysapps.com
2023-05-12 02:53:06	Raw Data from RIRs	No	Hybrid Analysis	4	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "142.250.191.67:443"\n "142.251.46.170:443"\n "104.22.24.131:443"\n "52.155.62.95:443"\n "172.67.38.66:443"'}, {u'category': u'General u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 2, u'description': u'file/memory contains long str extension "png"\n "adobe_1_.png" has type "PNG image data 160 x 45 8-bit colormap non-interlaced" and extension "png"\n "youtube_1_.pn "iexplore.exe" reads file "c:\\users\\%osuser%\\appdata\\local\\microsoft\\internet explorer\\recovery\\high\\active\\{1e3592f5-ee3f-1
2023-05-12 02:54:17	Physical Location	No	Censys	0	0	4	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:01:18	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.156): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	tsunami (Net ID: 00:0D:29:AC:D1:54)
2023-05-12 02:54:00	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2023-05-12 02:55:21	BGP AS Membership	No	Censys	0	0	3	0	None	14061
2023-05-12 02:44:24	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:29:bb:71:26:4f:a3:73:c9:d3:c4:af:c8:b3:a3:33:dc:41 Signature Algorithm: ecdsa-wi
2023-05-12 03:08:52	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.133
2023-05-12 02:47:27	Open TCP Port	No	Pulsedive	0	0	2	0	None	185.199.109.153:80
2023-05-12 02:53:42	Netblock Membership	No	Censys	0	0	2	0	None	185.199.109.0/24
2023-05-12 02:45:14	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'ON', u'country_tld': u'.ca', u'ip': u'2606:4700:3031::6815:6a6', u'currency_name': u'Dollar', u'currency': u'CAD',
2023-05-12 03:00:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.49): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:23	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	aysegul (Net ID: 00:1A:2A:02:80:43)

2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.87): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.29): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:53	Physical Coordinates	No	AbstractAPI	0	0	4	0	None	37.751, -97.822
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	6562 7451 (Net ID: 00:00:C5:D7:2F:EC)
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	000hen.github.io
2023-05-12 02:44:28	Affiliate - Internet Name	No	DNS Resolver	2	0	2	0	None	frabjous-lebkuchen-324004.netlify.app
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	infoworld (Net ID: 00:02:2D:04:D1:DB)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Moneysavingexpert (Category: finance) https://forums.moneysavingexpert.com/profile/login
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:2086
2023-05-12 02:45:34	Name Server (DNS NS Records)	No	DNS Raw Records	0	0	1	0	None	daphne.ns.cloudflare.com
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	2	0	None	cloudflare
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-proxy-cache: MISS
2023-05-12 03:03:41	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:49:43	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:56:b0:2c:f1:37:ec:4d:fb:ba:29:5b:fe:cf:08:f7:c5:d3 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 76:A0:
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	WLAN2 (Net ID: 00:02:44:AF:56:1C)
2023-05-12 03:32:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.7:80
2023-05-12 03:24:47	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 03:13:00	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-0-256.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:44:21	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3030::ac43:a8fc
2023-05-12 02:44:18	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3037::6815:470e
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.109): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:09:02	Vulnerability - CVE Medium	Yes	Tool - Retire.js	0	0	4	0	None	CVE-2020-11023 https://nvd.nist.gov/vuln/detail/CVE-2020-11023 Score: 6.1 Description: In jQuery versions greater than or equal to 1.0
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	grasshopper2 (Net ID: 00:01:38:5A:88:28)
2023-05-12 02:59:53	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12	Co-Hosted Site -	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app

02:46:49	Domain Name								
2023-05-12 02:52:43	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:8d:d7:e0:05:18:38:a5:db:8a:48:64:f2:68:9a:98:22:c8 Signature Algorithm: sha256Wi 2023 GMT Extensions: none Signature : ecdsa-with-SHA256 30:44:02:20:43:38:D1:BA:46:EB:FB:AE:E5:0E:F5:96: 0C:2E:94:E5:49:45:23:64:6A:0D
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	art_vacation2.4 (Net ID: 00:01:9F:30:06:78)
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:2083
2023-05-12 03:01:14	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.130): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://funny.battleb0t.xyz/images/kappi_2.png
2023-05-12 02:46:01	Physical Coordinates	No	AbstractAPI	93	0	3	0	None	32.8608, -79.9746
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomF390F8 (Net ID: 00:0C:F6:F3:90:F8)
2023-05-12 02:44:07	Internet Name	No	CertSpotter	18	0	1	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:09:38	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	107.48.229.35.bc.googleusercontent.com
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	nocable (Net ID: 00:04:5A:E4:CE:AD)
2023-05-12 03:18:06	URL (Form)	No	Page Information	0	0	5	0	None	https://ayhu.xyz/?__cf_chl_f_tk=kwBAgL0pzuFjxM6EaWUvVvfmBnOG2dt8365xKG72N9g-1683860053-0-gaNycGzNCfs
2023-05-12 03:18:06	URL (Form)	No	Page Information	0	0	4	0	None	https://ayhu.xyz/?__cf_chl_f_tk=tLjY4MFl6PFRYsxJBRXXPqgMr4VsmLm23dP5uGlU768-1683860053-0-gaNycGzNCiU
2023-05-12 02:59:34	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:88:a7:3c:db:48:4e:7a:5b:30:55:60:8f:23:20:34:8b:3f Signature Algorithm: sha256Wi fe:80:38:47:ab:f9:93:8b:07:ed:9c:23:7a:ce:61:de:37:2c: b5:38:61:3d:a2:a5:6a:7f:07:4e:90:cc:90:cb:f2:dc:3b:dd: dc:6e:3d:eb:d5:9b:14:fa:
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	webdisk.ayhu.xyz
2023-05-12 02:52:08	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:96:9b:29:e7:ba:1f:ed:f3:53:36:ca:2c:46:93:27:46:97 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 63:E8:
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	101 (Net ID: 00:01:03:79:1E:5C)
2023-05-12 03:09:34	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	01def.io
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	swwlan (Net ID: 00:02:2D:18:2C:14)
2023-05-12 02:46:49	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	3	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 02:5a:61:0f:58:eb:84:f1:ad:53:ae:03:dc:a9:84:7a Signature Algorithm: ecdsa-with-SHA 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: 1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73 Timestamp : Dec 21 09:03:52.857 2022
2023-05-12 02:54:41	Open TCP Port	No	Censys	0	0	3	0	None	104.196.30.220:80
2023-05-12 03:01:29	Raw Data from RIRs	No	Tool - WhatWeb	1	0	2	0	None	[{u'request_config': {u'headers': {u'User-Agent': u'Mozilla/5.0'}}, u'target': u'http://fluid.battleb0t.xyz', u'http_status': 301, u'p
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	interpals (Category: dating) https://www.interpals.net/ayhu
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=WwRFDMWv1i%2FLL8I%2BSQXrEl8P6VG5M1GGitMkpd4FkAGmtOdqQDCL
2023-05-12 03:01:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.133): Search Engine Last Activity: 0 days ago Threat Level: 29

2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Allstate 5G (Net ID: 00:02:6F:F8:0A:41)
2023-05-12 03:00:37	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namecheap.com
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-range.github.io
2023-05-12 03:13:02	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [000.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	GOLFNET (Net ID: 00:05:3C:07:87:1A)
2023-05-12 03:08:52	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.129
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	RichA (Net ID: 00:02:6F:8D:88:99)
2023-05-12 02:54:48	Open TCP Port	No	Censys	0	0	3	0	None	34.148.97.127:443
2023-05-12 02:44:06	Internet Name	No	CertSpotter	37	0	1	0	None	kekw.battleb0t.xyz
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX551548FF6 (Net ID: 00:01:E3:54:8F:F6)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	osbridge (Net ID: 00:15:D6:54:08:08)
2023-05-12 02:54:21	HTTP Status Code	No	Web Spider	0	1	3	0	None	521
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BBHWIRELESS (Net ID: 00:00:C5:D7:60:2C)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	internal (Net ID: 00:0C:41:12:D6:E5)
2023-05-12 02:45:48	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'Chicago', u'security': {u'is_vpn': False}, u'city_geoname_id': 4887398, u'region_geoname_id': 4896861, u'country': u'Unite
2023-05-12 02:44:24	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 03:24:51	Country	No	Country Name Extractor	0	0	7	0	None	Iceland
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cross-origin-opener-policy: same-origin
2023-05-12 02:45:41	Physical Coordinates	No	AbstractAPI	0	0	2	0	None	34.0544, -118.244
2023-05-12 03:08:52	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.134
2023-05-12 03:09:18	Vulnerability - General	Yes	Tool - Retire.js	0	0	4	0	None	CVE-2018-20676 Score: Unknown Description: Unknown
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	giters (Category: coding) https://giters.com/ayshoo
2023-05-12 02:56:39	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	{u'count': 22, u'search_terms': [{u'id': u'host', u'value': u'35.229.48.116'}], u'result': [{u'environment_id': 100, u'job_id': u'63b9 u'type': None, u'type_short': u'url', u'size': 69}, {u'environment_id': 160, u'job_id': u'63766b07cf04ba1b220d8dc2', u'analysis_start_ u'dadadaa15e19ef9c2a983600ba16684260f2d8a2ad7abdae5ef4d3720e3f04c1', u'type': None, u'type_short': u'url', u'size': 341}, {u'environme u'79c6aa841bf5874b35646cf7f5a083e6887cd50479d71ea9646f728d9c68e9b9', u'type': None, u'type_short': u'url', u'size': 46}, {u'environmen u'sample.url', u'sha256': u'b9380c0d5fb860d1b55d8764ccc4ac1c86489a28c0a63f3e01ffd798d9030cec', u'type': None, u'type_short': u'url', u
2023-05-12	SSL Certificate -	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:34:48:36:b2:51:77:1f:45:f7:ca:23:53:09:6b:f8:20:f7 Signature Algorithm: sha256Wi

02:52:20	Raw Data								GMT Extensions: none Signature : ecdsa-with-SHA256 30:45:02:20:73:56:94:2F:31:A8:B8:1A:98:8B:10:59: F6:53:2E:1E:0E:70:CF:6D:BF:D5:0A:C
2023-05-12 03:18:47	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Horizontal (normal) @ 18}
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	FriendFinder-X (Category: dating) https://www.friendfinder-x.com/profile/ayhu
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	cross-origin-resource-policy: same-origin
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:45:07	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'CA', u'country_tld': u'.us', u'ip': u'2606:50c0:8001::153', u'currency_name': u'Dollar', u'currency': u'USD', u'cou
2023-05-12 02:54:34	Software Used	Yes	Censys	0	0	3	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12 02:51:28	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObjects\\UpdatingNewTab "stackpath.bootstrapcdn.com"\n "tag.demandbase.com"'}, {u'category': u'General', u'origin': u'File/Memory', u'identifier': u'string-10 u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 8, u'description': u'Antivirus vendors marked dropped file "urlblock e51d492d6388e3a14ab136b2a7880775-lc.min_1_.js" has type "UTF-8 Unicode text with very long lines"- [targetUID: N/A]\n "otBannerSdk_1_.
2023-05-12 02:46:53	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-served-by: cache-ewr18167-EWR
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	5	0	None	Czech Republic
2023-05-12 02:44:18	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3030::ac43:a8fc
2023-05-12 03:24:30	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	PERFECT PRIVACY, LLC
2023-05-12 02:53:35	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cf-ray: 7c5f606c5dec334e-EWR
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2086
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	apple network 06223f (Net ID: 00:02:2D:06:22:3F)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Kongregate (Category: gaming) https://www.kongregate.com/accounts/login
2023-05-12 03:18:06	URL (Purely Static)	No	Page Information	0	0	3	0	None	http://nuke.battleb0t.xyz
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.9): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:57:34	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur */*\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate "D44LOOV2.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\D44LOOV2.txt]- [targetUID: 00000000-00003624]\n Dropped file: "OLG [targetUID: 00000000-00003624]\n "NewErrorPageTemplate_1_" has type "UTF-8 Unicode (with BOM) text with CRLF line terminators"- [targe u'File/Memory', u'identifier': u'string-102', u'name': u'Decrypted SSL network traffic', u'attck_id_wiki': u'https://attack.mitre.org/
2023-05-12 03:01:23	Web Server	No	Tool - WhatWeb	0	1	1	0	None	GitHub.com

2023-05-12 02:53:17	IPv6 Address	No	Mnemonic PassiveDNS	0	0	1	0	None	2606:4700:3031::ac43:8709
2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	172.67.168.252
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Disqus (Category: social) https://disqus.com/by/ayshoo/
2023-05-12 02:54:13	Web Content	No	Web Spider	2	0	3	0	None	<!DOCTYPE html> <html lang="en-US"> <head> <title>Just a moment...</title> <meta http-equiv="Content-Type" content="text/html; charset pECoh_3dTQi7RdzrUTwf2cZR9T8D8U2K3Gvk8riLAICiz8kZstCExyU1gQxK_8IKsvToQ9RDrd9y9LVAX9qYv3TfadD1EkNEsFVChUuXBIn1vLV2P2GOPSzKbMN6zXhMlaXjRn '2ToLICUBPb7XpOOLU5MHBc4J5yG0oheUGtehN/w3ZVsFmzDAbOvCroJJwwrRkjNV6Tn52KN/9nB7B8sz2NSv9/9dxRAmoEg1HGzmozU2NACMuujm6XlVF5ozcbqn9ZBfwSat/
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	2WIRE522 (Net ID: 00:01:E6:93:CB:2D)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	W4B3P<]00D^20&51%1C35&6H'%***%Ph (Net ID: 00:06:66:2A:52:5E)
2023-05-12 02:55:15	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Set_Cookie": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Connection": "DISPLAY_UTF8", "Content_Type": "DISPLAY_UTF8", "
2023-05-12 03:13:01	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-l.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:03:17	Internet Name	No	DNS Resolver	0	0	2	0	None	www.ayhu.xyz
2023-05-12 03:01:20	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.178): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:23	Web Content	No	Web Spider	3	0	4	0	None	<!DOCTYPE html> <html lang="en-US"> <head> <title>Just a moment...</title> <meta http-equiv="Content-Type" content="text/html; charset Zpdazh2C2qr1j5WGxsjVqAAnZQgtB_uAAZyLoW1Egawj2Dc9S-5JYlq2p44Cqz8kfn_HZzhJUPbd4OlAseBQZQfvTsxwQ8yBZFjNQTY6QE_0SDhUH44IwsfVzyg_qg2EOGimek 'R0VU', d: 'q4f4pOzDOU+B6AF/zMNZTtfQUbZJdschTcFNDOWKy7up/+mqaf8truQ2KKjt/rj9tsUJvHCPMl5JvfNuCtkhZqw35DYnRx8YzO+NZjtA29VORnsHbyexmRukxX
2023-05-12 03:38:35	Blacklisted Affiliate IP Address	Yes	UCEPROTECT	0	0	4	0	None	UCEPROTECT - Level 2 (some false positives) (46.101.229.63)
2023-05-12 03:43:57	URL (Form)	No	Page Information	0	0	5	0	None	https://ayhu.xyz/lol.html?__cf_chl_f_tk=s7qF6ZO3cVvdEEZa_WmCMPM6sxOwT7Q8EvJA4xw7FTE-1683861861-0-gaNycGzNChA
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	giters (Category: coding) https://giters.com/Battleb0t
2023-05-12 03:17:44	Account on External Site	No	Account Finder	0	0	1	0	None	MCName (Minecraft) (Category: gaming) https://mcname.info/en/search?q=_BattleB0t_
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Interwrx2 (Net ID: 00:02:2D:A8:80:99)
2023-05-12 03:13:05	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0066cc.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:01:51	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.110.154:80
2023-05-12 03:03:25	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2082
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	VipAdsl (Net ID: 00:14:C1:39:05:41)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	dvdbeyond (Net ID: 00:01:24:F2:B3:12)
2023-05-12 03:09:47	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	68.170.74.34.bc.googleusercontent.com
2023-05-12 03:18:00	Malicious IP on Same Subnet	Yes	CINS Army List	0	0	4	0	None	cinsscore.com [46.101.128.0/17] http://cinsscore.com/list/ci-badguys.txt
2023-05-	Raw DNS	No	DNS Raw	0	0	2	0	None	www.battleb0t.xyz. 244 IN CNAME battleb0t.github.io.

12 02:45:35	Records		Records						
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	TOMTSSID (Net ID: 00:02:2D:39:9C:50)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Jupiter (Net ID: 00:02:2D:66:D2:47)
2023-05-12 03:15:46	Username	No	Account Finder	2	0	1	0	None	patrick.pogoda
2023-05-12 02:54:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relev "data"- Location: [%TEMP%\\~DF6FD83128DC293791.TMP]- [targetUID: 00000000-00003260]\n "~DFBFBD8694A9325E58.TMP" has type "data"- Locat "SUIDMmicrosoft.com/92162963605376310241441866499008310240 27*MUID331E24F2502163E33EAE361751A562BBmicrosoft.com/10253096094592311024981 "wmploc.dll/Offline_Buy.htm\'res://wmploc.dll/Offline_MediaGuide.htm*res://wmploc.dll/Offline_Subscriptions.htm"\n Pattern match: "htt
2023-05-12 02:46:49	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Eminent Ellen (Net ID: 00:14:5C:85:89:DC)
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.172): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:13	IP Address	No	DNS Resolver	106	0	1	0	None	185.199.108.153
2023-05-12 03:32:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.20:8443
2023-05-12 03:32:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.9:8080
2023-05-12 02:53:25	IP Address	No	Mnemonic PassiveDNS	0	0	2	0	None	104.21.71.14
2023-05-12 02:50:17	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'General', u'origin': u'Network Traffic', u'identifier': u'network-1', u'name': u'Contacts server', u'attck_id_wiki': u'https://attac Gecko\nAccept-Encoding: gzip, deflate\nHost: getbootstrap.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "user-agent: ")\n "GET /doc u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': u'htt has type "UTF-8 Unicode text with very long lines"- [targetUID: 00000000-00003080]\n "~DFEC0F2E68E5E272C6.TMP" has type "data"- Locati
2023-05-12 02:54:16	Web Content Type	No	Web Spider	0	0	4	0	None	application/javascript
2023-05-12 03:09:06	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	165.232.113.82
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:2096
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Paradiso Films - NL (Net ID: 00:01:21:31:1A:1A)
2023-05-12 02:52:59	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 50, u'search_terms': [{u'id': u'host', u'value': u'185.199.109.153'}], u'result': [{u'environment_id': 160, u'job_id': u'64 u'63273b57b45d033047835de89bbd71ba014495b8b2a1928350903b52872c5dac', u'type': None, u'type_short': u'url', u'size': 45}, {u'environmen u'threat_score': 100, u'verdict': u'malicious', u'submit_name': u'sample.url', u'sha256': u'4b4f047cb451367a5e10020c362772951184dee4d2 32 bit', u'threat_score': None, u'verdict': u'no specific threat', u'submit_name': u'sample.url', u'sha256': u'98f13f00bb30ace7e8ec5fc u'environment_description': u'Windows 7 64 bit', u'threat_score': None, u'verdict': u'no specific threat', u'submit_name': u'sample.ur
2023-05-12 03:33:10	IP Address	No	DNS Resolver	30	0	2	0	None	45.131.109.53
2023-05-12 02:54:10	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3031::6815:6a6:80
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	linksys (Net ID: 00:1D:7E:37:25:D8)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Pikatel (Net ID: 00:08:5C:FA:52:87)
2023-05-12 03:18:53	WiFi Access	No	Wigle.net	0	0	5	0	None	CableWiFi (Net ID: 00:0D:67:8C:21:B3)

	Point Nearby								
2023-05-12 02:54:03	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 400 Bad Request Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 253 Connection: close CF-RAY: -
2023-05-12 03:24:21	Web Content Type	No	Web Spider	0	0	2	0	None	text/html;charset=utf-8
2023-05-12 03:13:10	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [malsup.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.152): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Collaborative innovation network - Collaborative innovation is a process in which multiple players contribute towards creating new pro
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Barnes (Net ID: 00:06:25:FE:DD:85)
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.232): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-mitigated: challenge
2023-05-12 02:45:19	Raw Data from RIRs	No	ipapi.co	0	0	4	0	None	{u'region_code': u'VA', u'country_tld': u'.us', u'ip': u'2600:1f18:2489:8200::c8', u'currency_name': u'Dollar', u'currency': u'USD', u
2023-05-12 03:03:30	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:FA:75:55)
2023-05-12 03:09:12	Affiliate - IP Address	No	DNS Look-aside	2	0	3	0	None	207.154.228.159
2023-05-12 03:31:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	098cbf54d6bdbb0fbdb022d1da6e4300-356617@contact.gandi.net
2023-05-12 02:44:08	Internet Name	No	CertSpotter	19	1	1	0	None	nuke.battleb0t.xyz
2023-05-12 03:41:52	Open TCP Port	No	Censys	0	0	3	0	None	45.131.109.53:47001
2023-05-12 02:53:07	Raw Data from RIRs	No	Tool - WAFW00F	1	0	2	0	None	[{"url": "https://funny.battleb0t.xyz", "firewall": "None", "detected": false, "manufacturer": "None"}]
2023-05-12 03:13:06	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [007sair.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:03:23	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:24:19	Account on External Site	No	Account Finder	0	0	8	0	None	Twitter (Category: social) https://twitter.com/baptistevauthey
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:4e:82:1a:86:ae:7d:8a:39:3c:25:24:c6:46:df:b3:a2:f4 Signature Algorithm: sha256Wi Extensions: none Signature : ecdsa-with-SHA256 30:45:02:21:00:B5:F3:29:BD:A0:20:09:5F:ED:BA:FE: 7D:4D:29:A6:16:28:D4:3D:6D:9D:84:56:4B
2023-05-12 03:08:35	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	185.199.111.154
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	hackerearth (Category: coding) https://www.hackerearth.com/@login
2023-05-12 03:24:51	Country	No	Country Name Extractor	0	0	7	0	None	United States
2023-05-12 02:45:54	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:36:85:4f:53:33:b4:86:64:2a:83:12:ed:95:43:fe:1e:22 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 02:C9:

2023-05-12 03:23:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.10:8443
2023-05-12 02:49:06	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki TrueType length 71896 version 4.393"- [targetUID: N/A]\n "product_page.js" has type "UTF-8 Unicode text with very long lines with CRLF in binary/memory', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 142.250.191.78"\n "UDP connection to 172.217.164.99"\n "UDP connection to 142.251.46.170"\n "UDP connection to 142.251.214.142"'}, {u'
2023-05-12 02:54:20	Open TCP Port	No	Censys	0	0	4	0	None	2600:1f18:2489:8200::c8:80
2023-05-12 03:33:48	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	"Exif 8Photoshop 3.0 mntrRGB XYZ acspAPPL -appl 0cprt Pwtpt chad gTRC mluc 3mluc 2XYZ 5CrOZpRG? rE8d0'8 hl1b1 GJ2W< zkHdm J\pwt P49$v
2023-05-12 02:58:47	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "142.250.217.106:443"\n "142.251.211.227:80"\n "142.251.215.227:443"\n "52.95.155.94:443"'}, {u'category': u'General', u'origin': u'Ne u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': None, "~DF1E50A457EB0DA7FD.TMP" has type "data"- Location: [%TEMP%\\~DF1E50A457EB0DA7FD.TMP]- [targetUID: 00000000-00001020]\n "E87CE99F1246 051918.netlify.app%2F%3Fdir%3DbXlldW5nQHRlc2xhLmNvbQ%3D%3D"\n Pattern match: "https://jsv3.recruitics.com"\n Heuristic match: "o.ss2.u
2023-05-12 03:09:00	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.95
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=nuke.battleb0t.xyz
2023-05-12 03:12:10	Affiliate Description - Abstract	No	DuckDuckGo	0	0	5	0	None	Netcraft is an Internet services company based in Bath, Somerset, England. The company provides cybercrime disruption services across
2023-05-12 02:54:18	Linked URL - External	No	Web Spider	0	0	3	0	None	https://use.fontawesome.com/9dfc16ed6b.js
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	default (Net ID: 00:01:24:F0:36:D7)
2023-05-12 02:46:30	Physical Location	No	MetaDefender	0	0	3	0	None	North Charleston, United States
2023-05-12 02:55:20	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'mutant-0', u'name': u'Creates mutants', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id Cabinet archive data Windows 2000/XP setup 62932 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"'}, {u'c RGBA non-interlaced"- [targetUID: N/A]\n "S6uyw4BMUTPHjx4wWA_1_.woff" has type "Web Open Font Format TrueType length 28648 version 1.1 keep-alive\nStatus: 302 Found\nLocation: https://www.audiocompliance.com/product/ac/form-941-compliance-2022\nDate: Thu, 16 Feb 2023 0
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	re927421 (Net ID: 00:02:8A:40:D2:92)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	DPRWirelessScottsdale (Net ID: 00:02:6F:FD:3F:B2)
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:465
2023-05-12 02:44:13	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	2	0	None	githubusercontent.com
2023-05-12 02:54:18	Linked URL - External	No	Web Spider	0	0	3	0	None	https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	5	0	None	Turkey
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	E-A (Net ID: 00:14:C1:05:69:7C)
2023-05-12 03:13:06	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [007.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.85): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:00	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 400 Bad Request Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 253 Connection: close CF-RAY: -
2023-05-	WiFi	No	Wigle.net	0	0	4	0	None	Badazz-net (Net ID: 00:14:5C:88:1A:C4)

12 03:42:18	Access Point Nearby								
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	referrer-policy: same-origin
2023-05-12 02:44:17	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 03:16:23	Physical Location	No	ipapi.co	1	0	2	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2023-05-12 02:54:38	BGP AS Membership	No	Censys	0	0	3	0	None	13335
2023-05-12 03:24:29	Company Name	No	Company Name Extractor	0	0	4	0	None	Netlify\, Inc
2023-05-12 03:01:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.1): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	2WIRE623 (Net ID: 00:00:85:F5:03:9F)
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	2	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:02:6d:eb:8d:63:78:04:f2:b8:5c:db:39:06:ab:26:ed:a9 Signature Algorithm: sha256Wi 05:9A:15:17:EA:9E:B4:58:0D:3C:86:17:2C:C3:17:21: 8A:21:DE:13:02:21:00:93:46:3A:71:BC:50:F5:73:1A: 31:49:1D:77:D8:F0:F3:D0:7E:06:7D:4A:
2023-05-12 02:44:30	Internet Name	No	DNS Resolver	1	0	2	0	None	funny.battleb0t.xyz
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomC8B210 (Net ID: 00:0C:F6:C8:B2:10)
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.138): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:23	Raw Data from RIRs	No	Tool - WhatWeb	0	0	1	0	None	[{u'request_config': {u'headers': {u'User-Agent': u'Mozilla/5.0'}}, u'target': u'http://battleb0t.xyz', u'http_status': 301, u'plugins
2023-05-12 02:44:40	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Netlify
2023-05-12 03:01:10	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.121): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:23	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 05T01:21:09+00:00', u'filename': u'bounty-92442219031035527'}], u'analysis_start_time': u'2023-04-05T01:21:09+00:00', u'tags': [], u'i "GetProcAddress" with a parameter ReleaseSRWLockExclusive (UID: 00000000-00003036)\n "rufus-3.22.exe" called "GetProcAddress" with a p 76f60000\n "rufus-3.22.exe" loaded module "ADVAPI32.DLL" at base 76b50000\n "rufus-3.22.exe" loaded module "COMDLG32.DLL" at base 7578 "LoadLibrary" with a parameter ole32.dll (UID: 00000000-00003036)\n "rufus-3.22.exe" called "LoadLibrary" with a parameter SHELL32.dll
2023-05-12 03:09:01	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.97
2023-05-12 02:54:12	HTTP Headers	No	Web Spider	8	0	1	0	None	{"content-length": "690", "via": "1.1 varnish", "vary": "Accept-Encoding", "etag": "W/\"642b434c-4fb\"", "x-cache-hits": "1", "cache-c
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	KnowYourMeme (Category: social) https://knowyourmeme.com/users/login
2023-05-12 03:04:46	Hosting Provider	No	Hosting Provider Identifier	0	0	3	0	None	Cloudflare Inc: https://www.cloudflare.com/
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	3	0	None	36459
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	FNCU-Guest (Net ID: 00:00:0D:09:DE:0C)
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:2096
2023-05-12 03:01:18	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.157): Search Engine Last Activity: 0 days ago Threat Level: 29

2023-05-12 02:54:30	Open TCP Port	No	Censys	0	0	3	0	None	64.226.81.43:443
2023-05-12 03:01:27	Web Server	No	Tool - WhatWeb	0	0	2	0	None	cloudflare
2023-05-12 03:11:22	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'city': u'Frankfurt am Main', u'security': {u'is_vpn': False}, u'city_geoname_id': 2925533, u'region_geoname_id': 2905330, u'country
2023-05-12 02:55:15	Software Used	Yes	Censys	0	0	3	0	None	Ubuntu Linux
2023-05-12 02:50:17	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.88): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:35	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	leanna.ns.cloudflare.com
2023-05-12 02:59:53	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	german.l@alliedglobal.com
2023-05-12 03:16:19	Physical Location	No	ipapi.co	1	0	2	0	None	London, England, ENG, United Kingdom, GB
2023-05-12 03:09:41	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	123.48.229.35.bc.googleusercontent.com
2023-05-12 02:57:58	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level': 0, u'type': 7, u'description': u'"wifispeedtest.run"'}, {u'category': u'General', u'origin': u'Network Traffic', u'id [targetUID: 00000000-00002848]'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u' Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE8126868377 browsers, although no browser was ever launched', u'attck_id_wiki': None, u'threat_level_human': u'suspicious', u'capec_id': None, u'a
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	danny (Net ID: 00:01:E3:02:5D:60)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Eminent (Net ID: 00:14:5C:88:50:78)
2023-05-12 03:24:21	HTTP Headers	No	Web Spider	10	0	3	0	None	{"content-encoding": "gzip", "nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "referrer-policy": "same-o
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:01:24:F2:17:BC)
2023-05-12 02:46:18	Affiliate Description - Category	No	DuckDuckGo	0	0	2	0	None	Freedom of speech in the United States
2023-05-12 03:23:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.6:80
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://funny.battleb0t.xyz/images/random_4.png
2023-05-12 02:47:20	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObjects\\Local\\!BrowserEmulation!SharedMemory!Mutex"\n "\\ "Cab1B9C.tmp" has type "Microsoft Cabinet archive data Windows 2000/XP setup 62932 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 d "test_web_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUID: 00000000-00002592]\n "bubble-shooter_1_.png" has type "PN Related', u'origin': u'File/Memory', u'identifier': u'string-102', u'name': u'Decrypted SSL network traffic', u'attck_id_wiki': u'http
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:443
2023-05-12 02:45:52	Raw Data from RIRs	No	AbstractAPI	0	0	4	0	None	{u'city': u'Montreal', u'security': {u'is_vpn': False}, u'city_geoname_id': 6077243, u'region_geoname_id': 6115047, u'country': u'Unit
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	x-served-by: cache-lga21959-LGA

2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	5	0	None	cloudflare
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:01:24:F0:65:67)
2023-05-12 02:54:03	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Dubtronicssid (Net ID: 00:01:24:F0:BB:A4)
2023-05-12 03:18:06	URL (Form)	No	Page Information	0	0	2	0	None	http://ayhu.xyz
2023-05-12 02:44:41	Internet Name	No	DNS Resolver	0	0	2	0	None	vscode.battleb0t.xyz
2023-05-12 03:18:52	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image ExifOffset': (0x8769) Long=134 @ 90, 'Image Orientation': (0x0112) Short=Horizontal (normal) @ 18, 'Image YCbCrPositioning': (
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cross-origin-embedder-policy: require-corp
2023-05-12 02:54:10	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12 02:46:00	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'city': u'Chicago', u'security': {u'is_vpn': False}, u'city_geoname_id': 4887398, u'region_geoname_id': 4896861, u'country': u'Unite
2023-05-12 02:58:42	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\ u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 8, u'descr section info"- [targetUID: N/A]\n "WY7JZ84F.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\WY7JZ84F.tx u'attck_id_wiki': None, u'threat_level_human': u'suspicious', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level':
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ajansbegum (Net ID: 00:02:CF:87:A5:A4)
2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	185.199.109.153
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/withat_5.jpg
2023-05-12 03:34:00	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	"Exif sgssso <Qwm7 >6x.O x>t7? g$sy? .b97< /Ggy! l/5-o ggs43Z x.o.n> NNEsz gmuss Mswy5 dIys6 >t6w6 03Ryr\G a>0xM g_on8 9!6sBsmms ?r:\t
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0067ed.github.io
2023-05-12 03:14:48	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2011-3389 https://nvd.nist.gov/vuln/detail/CVE-2011-3389 Score: 4.3 Description: The SSL protocol, as used in certain configuratio
2023-05-12 02:54:34	Netblock Membership	No	Censys	0	0	3	0	None	104.21.64.0/20
2023-05-12 03:31:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	jrupp@name.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	memrise (Category: hobby) https://app.memrise.com/user/login/
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-ray: 7c5f6059be52c402-EWR
2023-05-12 02:45:43	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'San Francisco', u'security': {u'is_vpn': False}, u'city_geoname_id': 5391959, u'region_geoname_id': 5332921, u'country': u
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Yapitest (Net ID: 00:14:7C:B0:26:1A)
2023-05-	SSL	No	Certificate	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:96:9b:29:e7:ba:1f:ed:f3:53:36:ca:2c:46:93:27:46:97 Signature Algorithm: sha256Wi

12 02:56:57	Certificate - Raw Data		Transparency						Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 63:E8: f5:b9:42:b6:a4:a3:92:70:93:b5:82:12:31:84:1f:7a:4e:c1: b5:6e:db:bb:40:e0:59:4d:30:89:d2:e6:e9:ce:d5:19:06:a3: 10:65:96:34:86:38:78:b2:
2023-05-12 03:11:15	Physical Location	No	AbstractAPI	1	0	2	0	None	London, England, W1B, United States, North America
2023-05-12 03:04:46	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2023-05-12 03:13:07	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00d2.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	101 (Net ID: 00:01:03:79:02:18)
2023-05-12 02:53:10	Web Technology	No	Tool - WAFW00F	0	0	3	0	None	Cloudflare Inc. Cloudflare
2023-05-12 02:54:48	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["0"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BARWN-UnitedLayer01 (Net ID: 00:02:6F:01:86:4F)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_ipad (Net ID: 00:0C:E6:08:03:05)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	herron-libson (Net ID: 00:01:24:F1:75:B2)
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Pinterest (Category: social) https://www.pinterest.com/ayshoo/
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:05:5D:EC:8D:60)
2023-05-12 02:54:15	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://www.battleb0t.xyz
2023-05-12 03:01:09	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.119): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:15	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://oldfluid.battleb0t.xyz
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	tsunami (Net ID: 00:0D:29:AC:D7:31)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	linksys (Net ID: 00:0C:41:86:BE:6A)
2023-05-12 02:44:56	Physical Location	No	ipapi.co	1	0	2	0	None	San Francisco, California, CA, United States, US
2023-05-12 03:09:31	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:08:46	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.218
2023-05-12 02:54:14	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://nwapi2.battleb0t.xyz
2023-05-12 02:45:32	Malicious Internet Name	Yes	VirusTotal	0	0	1	0	None	VirusTotal [ayhu.xyz] https://www.virustotal.com/en/domain/ayhu.xyz/information/
2023-05-12 03:13:01	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-to-1.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	azis (Net ID: 00:06:B1:15:73:DD)
2023-05-12 03:00:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.13): Search Engine Last Activity: 0 days ago Threat Level: 29

2023-05-12 03:09:09	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	46.101.229.63
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	LAB1234 (Net ID: 00:0C:41:CB:47:70)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-B772 (Net ID: 00:1D:CF:82:B7:70)
2023-05-12 03:01:12	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.127): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	linux
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	1100 (Net ID: 00:01:03:79:01:88)
2023-05-12 03:00:47	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.63): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	suddenlink.net-50B2 (Net ID: 90:1A:CA:7D:50:B0)
2023-05-12 03:14:28	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	battleb0t.ovh
2023-05-12 02:53:49	BGP AS Membership	No	Censys	0	0	2	0	None	54113
2023-05-12 03:41:52	Raw Data from RIRs	No	Censys	1	0	3	0	None	{"operating_system": {"vendor": "Microsoft", "product": "Windows", "part": "o", "uniform_resource_identifier": "cpe:2.3:o:microsoft:wi dev.de", "70724-04381.pph-server.de", "11858-33959.pph-server.de"], "reverse_dns": {"resolved_at": "2023-05-04T16:22:43.166057588Z", " "OSI_TRANSPORT_LAYER"}]}, {"tls": {"server_key_exchange": {"ec_params": {"named_curve": 24}}, "_encoding": {"ja3s": "DISPLAY_HEX"}, "v 1, "rdstls": false, "error_hybrid_required": false, "credssp_early_auth": false, "error_bad_flags": false, "error_ssl_forbidden": fals "html_tags": "DISPLAY_UTF8", "body_hash": "DISPLAY_UTF8"}, "html_title": "Not Found", "protocol": "HTTP/1.1", "body_size": 315, "body_
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	suddenlink.net-7734 (Net ID: 38:70:0C:07:77:32)
2023-05-12 03:00:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.27): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:27	IP Address	No	DNS Resolver	51	0	2	0	None	104.21.71.14
2023-05-12 02:54:23	Web Content Type	No	Web Spider	0	0	5	0	None	text/html;charset=utf-8
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATT9D2Yjw8 (Net ID: E0:22:03:E8:DB:5A)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	6566 0615 (Net ID: 00:00:C5:D7:61:48)
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: <REDACTED> Cache-Control: no-cache, no-store, must-re
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:01:E6:93:CF:EC)
2023-05-12 02:53:15	IP Address	No	Mnemonic PassiveDNS	0	0	1	0	None	185.199.110.153
2023-05-12 03:03:37	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:51:01	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_ "urlref_httpskangbinkwon.github.iokangbinkwon-Netflix_clonecoding")\n Found string "<a href="https://devices.netflix.com/ko/" class="f File', u'identifier': u'binary-56', u'name': u'Drops files with image extension', u'attck_id_wiki': u'https://attack.mitre.org/techniq aspect ratio density 1x1 segment length 16 progressive precision 8 2000x1125 components 3"- [targetUID: N/A]\n "card-05_1_.png" has ty

2023-05-12 02:45:41	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'San Francisco (South Beach)', u'security': {u'is_vpn': False}, u'city_geoname_id': 5326621, u'region_geoname_id': 5332921,
2023-05-12 02:46:39	Malicious IP Address	Yes	Fraudguard	0	1	2	0	None	abuse_tracker (risk level: 4) [185.199.110.153]
2023-05-12 02:54:03	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:EE:43:99)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Lord Voldmodem (Net ID: F8:F5:32:63:56:0E)
2023-05-12 02:57:45	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: ff:0e:1e:a4:6f:55:f0:74:0e:b3:83:e1:07:c9:ea:93 Signature Algorithm: sha256WithRSAE 89:4a:3f:3d:94:64:76:5e:6b:ff:8c:03:7f:eb:ae:61:c0:89: 16:34:3c:a1:d5:87:98:35:53:48:52:1e:b4:61:d3:7d:9f:96: bd:0f:71:c5:cf:b6:14:12:
2023-05-12 03:10:35	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.108.153:80
2023-05-12 02:59:49	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	replayhubunlimited@gmail.com
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Pragma": "DISPLAY_UTF8", "Set_Cookie": "DISPLAY_UTF8", "X_Content_Type_Options": "DISPLAY_UTF8", "Connection": "DISPLA
2023-05-12 02:54:23	HTTP Headers	No	Web Spider	2	0	4	0	None	{"x-content-type-options": "nosniff", "content-encoding": "gzip", "transfer-encoding": "chunked", "expires": "Fri, 12 May 2023 04:54:2
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	linksys (Net ID: 00:16:B6:17:24:0D)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:DB:DA:99)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Intel Gateway (Net ID: 00:01:E6:96:87:21)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	grasshopper2 (Net ID: 00:01:38:5A:88:28)
2023-05-12 02:53:49	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 02:55:46	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'de lines with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\8c133cbc-cb4f-4494-9a53-681a41c38ec8.tmp]- [ta "https://creativecommons.org/compatiblelicenses"\n Pattern match: "https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imag very long lines with no line terminators"- Location: [%TEMP%\\7052_16790919\\adblock_snippet.js]- [targetUID: 00000000-00007052]\n "au
2023-05-12 02:46:11	Malicious IP Address	Yes	MetaDefender	0	1	3	0	None	webroot.com [104.21.71.14]
2023-05-12 03:18:06	URL (Purely Static)	No	Page Information	0	0	3	0	None	http://kekw.battleb0t.xyz
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 02:48:38	Malicious Co-Hosted Site	Yes	VirusTotal	0	1	2	0	None	VirusTotal [www.github.com] https://www.virustotal.com/en/domain/www.github.com/information/
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Duolingo (Category: hobby) https://www.duolingo.com/profile/ayhu
2023-05-12 02:57:23	Internet Name	No	Certificate Transparency	0	0	1	0	None	www.battleb0t.xyz
2023-05-12 03:03:23	Co-Hosted Site -	No	DNS Resolver	0	0	3	0	None	github.io

	Domain Name								
2023-05-12 02:44:10	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	1	0	None	github.io
2023-05-12 03:09:04	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.108
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Amethyst (Net ID: 00:01:21:30:76:B7)
2023-05-12 02:57:31	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis None, u'attck_id': u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"cdnjs.cloudflare.com"\n "lihi2.cc has type "SQLite Write-Ahead Log version 3007000"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\load_statistics.db-lines with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Network\\393a9751-d2fe-45b8-8e82-e58c u'Drops script files inside temp directory', u'attck_id_wiki': None, u'threat_level_human': u'suspicious', u'capec_id': None, u'attck_
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:2082
2023-05-12 02:44:04	Web Technology	No	Tool - WAFW00F	0	0	1	0	None	None None
2023-05-12 02:54:00	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-12T02:04:48.515Z", "ip": "104.21.6.166", "location_updated_at": "2023-04-29T21:15:21.600075Z", "autonomou "seribusenyum.org": {"record_type": "A", "resolved_at": "2023-02-18T18:24:43.138880401Z"}, "account-dev.prinsapps.com": {"record_type" 04-28T12:59:28.832256372Z"}, "www.usbestsiding.com": {"record_type": "A", "resolved_at": "2023-05-11T16:20:14.776067678Z"}, "prefahout 24T22:20:31.002106199Z"}, "lupiguitars.altervista.org": {"record_type": "CNAME", "resolved_at": "2023-04-27T22:39:14.320632180Z"}, "es "2023-01-14T17:27:43.018315606Z"}, "therpsequavillicomp.tk": {"record_type": "A", "resolved_at": "2023-05-03T21:57:55.402091890Z"}, "m
2023-05-12 02:44:33	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:88:80:c3:9c:e1:f5:05:d4:ce:eb:a7:b8:8b:96:69:16:e7 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: EE:9A:
2023-05-12 03:03:24	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:12:14	Affiliate - Domain Whois	No	Whois	3	0	5	0	None	Domain Name: KEYUBU.COM Registry Domain ID: 2292564494_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.nicproxy.com Registrar URL: http: telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). Redacted for Privacy Admin City: Redacted for Privacy Admin State / Province: Redacted for Privacy Admin Postal Code: Redacted for Pri information purposes, and to assist persons in obtaining information about or related to domain name registration records. NICS Teleko
2023-05-12 02:44:27	IP Address	No	DNS Resolver	42	0	2	0	None	64.226.81.43
2023-05-12 03:24:21	Web Content	No	Web Spider	2	0	2	0	None	<!DOCTYPE html> <html lang="en-US"> <head> <title>Just a moment...</title> <meta http-equiv="Content-Type" content="text/html; charset AioIh72_7f-dcCDyp3CvaV2lSxONdGbwSj69Uzxdx9pjqKiA7eKWgpDp1A1TT4OM1UPvdKoDNlfXS-kt53TGtcDj_tr5ZSCxVfBj5Eaq6vy-dzTe3un5fL0Jw93IdI7hmq3BtV d: 'eSl90ERW3ieYQBiJ/CvInfpugLrCuGqtrxfN7Hff3XV1tnjtcokhOvtXLaw36vmuW/PZRZbPFRsBG1FZ2o1L9/qlyM29SttBrPr40sLGiM5zROAIfmkLKaU7gxLqLGeRmX
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	BHS (Net ID: 00:02:A8:9A:AC:ED)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom6C4B98 (Net ID: 00:0C:F6:6C:4B:98)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	likeevideo (Category: social) https://likee.video/@ayhu
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CableWiFi (Net ID: 00:0D:67:2F:5E:C7)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SurfandSip (Net ID: 00:02:2D:03:7C:7A)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	New Improved Mad Dogs Network (Net ID: 00:02:2D:02:1F:7E)
2023-05-12 03:08:52	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.131
2023-05-12 03:01:30	Web Server	No	Tool - WhatWeb	0	0	2	0	None	cloudflare
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Sunshine (Net ID: 00:07:40:87:15:01)
2023-05-	Affiliate -	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com

12 03:09:53	Internet Name								
2023-05-12 02:44:28	Affiliate - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:45:45	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'Chantilly', u'security': {u'is_vpn': False}, u'city_geoname_id': 4751935, u'region_geoname_id': 6254928, u'country': u'Uni
2023-05-12 02:47:34	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur None, u'error_origin': None, u'ssdeep': None, u'entrypoint_section': None, u'md5': u'cd822912b4ff3c303a62d2538fa88d01', u'network_mode u'https://attack.mitre.org/techniques/T1553/002', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1553.002', "HKLM\\SOFTWARE\\POLICIES\\MICROSOFT\\SYSTEMCERTIFICATES\\CA"; Key: "")\n "rufus-3.12.exe" (Path: "HKLM\\SOFTWARE\\POLICIES\\MICROSOFT u'identifier': u'registry-20', u'name': u'Reads Windows Trust Settings', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1012
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	uyDunet (Net ID: 00:13:33:8F:4F:14)
2023-05-12 02:54:21	Web Content Type	No	Web Spider	0	0	3	0	None	text/html;charset=utf-8
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:E8:37:B2)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:7D:86:07)
2023-05-12 02:54:13	Linked URL - Internal	No	Web Spider	4	0	3	0	None	https://ayhu.xyz/?__cf_chl_f_tk=kwBAgL0pzuFjxM6EaWUvVvfmBnOG2dt8365xKG72N9g-1683860053-0-gaNycGzNCfs
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	AIRV_3DF5 (Net ID: 00:05:B9:42:3D:F8)
2023-05-12 02:59:57	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	support@bigmarker.com
2023-05-12 02:48:19	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': "lptag.liveperson.net"\n "maskwallets.xyz"\n "metamask.io"\n "perf.hsforms.com"\n "va.v.liveperson.net"\n "www.gstatic.com"'}, {u'cate count-shim.w--vertical {" (Indicator: "dir "; File: "webflow_1_.css")\n Found string ".w-widget-twitter-count-shim.w--vertical:before, image data JFIF standard 1.02 aspect ratio density 1x1 segment length 16 baseline precision 8 300x300 components 3" and extension "jpg
2023-05-12 02:44:14	IP Address	No	DNS Resolver	55	0	1	0	None	172.67.135.9
2023-05-12 02:52:59	Raw Data from RIRs	No	Tool - WAFW00F	1	0	2	0	None	[{"url": "https://nwapi2.battleb0t.xyz", "firewall": "Cloudflare", "detected": true, "manufacturer": "Cloudflare Inc."}, {"url": "http
2023-05-12 02:54:57	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Apple Network 221480 (Net ID: 00:02:2D:22:14:80)
2023-05-12 03:00:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha1-etm@openssh.com
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:03:42	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:55:27	Linked URL - Internal	No	URLScan.io	5	0	1	0	None	http://ayhu.xyz/
2023-05-12 03:24:47	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	101 (Net ID: 00:01:03:7C:01:7C)
2023-05-	Open TCP	No	Censys	0	0	2	0	None	

12 02:55:11	Port								87.248.157.102:443
2023-05-12 02:45:23	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis "203.192.208.114:443"\n "142.251.32.35:443"\n "104.26.5.108:80"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifi u'"AAAABVxdX2WnFSp49eXb1do0euaj-F8upNImjofE77XStKhf5kUHG94DPlTiGYqPeYNtiox-82NWEK0Ls3CnLe3WWClGdiJP_1_.png" has type "PNG image data 6 8-bit/color RGBA non-interlaced"- [targetUID: N/A]\n "all_1_.css" has type "ASCII text with very long lines"- [targetUID: N/A]\n "devi TrueType length 65760 version 1.1"- [targetUID: N/A]\n "pxiByp8kv8JHgFVrLCz7V1g_1_.woff" has type "Web Open Font Format TrueType lengt
2023-05-12 03:24:47	Country	No	Country Name Extractor	0	0	4	0	None	Germany
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	unsplash (Category: images) https://unsplash.com/@login
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pgi50 (Net ID: 00:01:21:10:89:70)
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	6	0	None	United States
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	eBOS (Net ID: 00:14:6A:5B:53:93)
2023-05-12 02:57:06	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_HASHFILESWITCH_MUTEX"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_DOWNLOAD_M u'Binary File', u'identifier': u'binary-5', u'name': u'Drops cabinet archive files', u'attck_id_wiki': None, u'threat_level_human': u' [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\80237EE4964FC9C409AAF55BF996A292_D46D6FA25B74360E1349F9015B5CCE53]- [targe "http://injectitlimited.cmail19.com/t/i-c-tiirkhydn"\n Pattern match: "http://injectitlimited.cmail19.com"\n Heuristic match: "injecti
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	1	3	0	None	Netlify
2023-05-12 02:54:13	Open TCP Port	No	Censys	0	0	4	0	None	2606:4700:3030::ac43:a8fc:80
2023-05-12 02:59:47	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	abuse@godaddy.com
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	FruityWifi-001 (Net ID: 00:02:72:8E:62:D1)
2023-05-12 03:01:20	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.180): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	default (Net ID: 00:01:24:F0:43:45)
2023-05-12 03:01:16	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.141): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:32:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.17:8080
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:DB:DA:99)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:AA:94:7C:2C)
2023-05-12 02:55:15	Open TCP Port Banner	No	Censys	0	1	3	0	None	SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
2023-05-12 03:10:04	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	acilacikveteriner.com
2023-05-12 02:46:43	Physical Location	No	MetaDefender	0	0	3	0	None	North Charleston, United States
2023-05-12 02:45:07	Raw Data from RIRs	No	Hybrid Analysis	0	0	1	0	None	{u'count': 1, u'search_terms': [{u'id': u'domain', u'value': u'battleb0t.xyz'}], u'result': [{u'environment_id': 160, u'job_id': u'642
2023-05-12 02:46:54	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	cloudflare.com

2023-05-12 02:44:23	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	4	0	None	Cloudflare, Inc.
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 401 Unauthorized Date: <REDACTED> Server: cPanel Persistent-Auth: false Host: 87.248.157.102:2079 Cache-Control: no-cache, no
2023-05-12 02:54:18	HTTP Headers	No	Web Spider	2	0	4	0	None	{"content-length": "243", "accept-ranges": "bytes", "strict-transport-security": "max-age=31536000", "server": "Netlify", "etag": "\"c
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.119): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:13	Linked URL - Internal	No	Web Spider	4	0	2	0	None	https://ayhu.xyz/cdn-cgi/styles/challenges.css
2023-05-12 02:54:00	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	ADSL-WiFi_Telfort (Net ID: 00:13:49:CF:0D:6D)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	conam (Net ID: 00:06:25:D8:C9:41)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SFUSA (Net ID: 00:01:24:F1:6D:E3)
2023-05-12 03:09:38	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	229.30.196.104.bc.googleusercontent.com
2023-05-12 03:03:20	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:53:17	IP Address	No	Mnemonic PassiveDNS	0	0	1	0	None	104.21.6.166
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Riaan (Net ID: 00:01:36:08:E7:41)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Merken (Net ID: 00:14:5C:86:BE:BA)
2023-05-12 02:44:43	Internet Name	No	DNS Resolver	0	0	2	0	None	vscode.battleb0t.xyz
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:0B:6B:11:48:DC)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Apple Network 3668a9 (Net ID: 00:02:2D:00:C6:8F)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Destructoid (Category: social) https://www.destructoid.com/?name=login
2023-05-12 02:44:28	IP Address	No	DNS Resolver	80	0	2	0	None	34.74.170.74
2023-05-12 02:44:25	Internet Name	No	DNS Resolver	0	0	2	0	None	funny.battleb0t.xyz
2023-05-12 02:51:54	Malicious IP Address	Yes	VirusTotal	0	1	3	0	None	VirusTotal [104.21.71.14] https://www.virustotal.com/en/ip-address/104.21.71.14/information/
2023-05-12 03:08:48	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.106
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	THW (Net ID: 00:02:6F:DF:78:B4)

2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	belkin54g (Net ID: 00:17:3F:83:7B:BA)
2023-05-12 03:43:57	URL (Form)	No	Page Information	0	0	3	0	None	https://ayhu.xyz/lol.html
2023-05-12 03:09:32	Affiliate - Internet Name	No	DNS Resolver	2	0	3	0	None	cdn-185-199-110-154.github.com
2023-05-12 03:33:51	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	eKE>Q RQEA< QEQAE GrG Z?xV _2H- -EEO1AE e.coC ?wX3 QE_1< QEhO0QE QEAAE rGDpyt cv>myz kPIiG X?wV< \u2v5 Qc>ft1 TtV@I iY>eI OYIXf QPO0
2023-05-12 02:46:54	IP Address	No	DNS Resolver	0	0	2	0	None	104.21.71.14
2023-05-12 02:56:52	Internet Name	No	DNS Resolver	0	0	3	0	None	funny.battleb0t.xyz
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SYNC_XP99MRWR (Net ID: 00:26:B4:2E:5E:DC)
2023-05-12 02:44:26	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	referrer-policy: same-origin
2023-05-12 03:08:29	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:03:19	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:46:17	Malicious IP Address	Yes	MetaDefender	0	1	3	0	None	webroot.com [172.67.168.252]
2023-05-12 02:52:56	Raw Data from RIRs	No	Tool - WAFW00F	1	0	2	0	None	[{"url": "https://kekw.battleb0t.xyz", "firewall": "None", "detected": false, "manufacturer": "None"}]
2023-05-12 02:54:30	Netblock Membership	No	Censys	0	0	3	0	None	64.226.80.0/20
2023-05-12 02:46:11	Physical Location	No	MetaDefender	0	0	3	0	None	San Jose, United States
2023-05-12 02:50:28	Legal Entity Identifier	No	GLEIF	0	0	3	0	None	5493005GJOH8HLL11157
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.240): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:01	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2023-05-12 02:56:55	Internet Name	No	DNS Resolver	0	0	4	0	None	vscode.battleb0t.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:06:25:7B:42:1D)
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	Pastebin (Category: tech) https://pastebin.com/u/battleb0t
2023-05-12 03:13:07	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00cybermonk00.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:19:47	Account on External Site	No	Account Finder	0	0	2	0	None	TikTok (Category: social) https://www.tiktok.com/@patrickpogoda?lang=en
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	6dgs (Net ID: 00:06:B1:28:66:65)
2023-05-12	Account on External Site	No	Account Finder	0	0	2	0	None	GitHub (Category: coding) https://github.com/ayhu

03:23:02									
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	VADER (Net ID: 00:06:25:FE:92:52)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	stayover1 (Net ID: 00:02:6F:AD:BE:CF)
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.111): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-0-256.github.io
2023-05-12 02:55:46	Internet Name	No	Hybrid Analysis	0	0	3	0	None	kekw.battleb0t.xyz
2023-05-12 03:09:27	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	188.114.97.1:443
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F2:6F:6D)
2023-05-12 02:44:27	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Cafferom (Net ID: 00:00:C5:F7:F0:C4)
2023-05-12 03:09:57	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:02:2D:30:32:62)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	2wire737 (Net ID: 00:02:2D:25:88:EE)
2023-05-12 03:04:07	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WestEd (Net ID: 00:02:2D:05:7E:85)
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.199): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATTwq7NaKI (Net ID: F8:2D:C0:AC:63:00)
2023-05-12 02:47:27	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'de u'capec_id': None, u'attck_id': u'T1074.001', u'relevance': 1, u'threat_level': 0, u'type': 6, u'description': u'"iexplore.exe" writes 00003976]\n "favicon_3_.ico" has type "MS Windows icon resource - 1 icon 32x32 32 bits/pixel"- [targetUID: N/A]\n "~DFDCCD055AC057DCDF (kn~Y^,;!CemtepSB*Fc0XhR,+V+vG|:7C5(NT-h@t#dc"%+K{\'F]Z).TX# Abv:5ofSOyHEF&OHj)_C9i\n>({In)xKtZ!LV+t\\v7cg_tq6aN7):39DceWU8EhD9<o\'X)C
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Jenkins_Network (Net ID: 00:1D:D4:64:98:80)
2023-05-12 03:00:33	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	vitalie.porcescu@ansa.gov.md
2023-05-12 03:16:29	Physical Location	No	ipapi.co	0	0	3	0	None	Frankfurt am Main, Hesse, HE, Germany, DE
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_gasten (Net ID: 00:0C:E6:AD:7F:88)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	referrer-policy: strict-origin-when-cross-origin

2023-05-12 03:00:38	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	abuse@nicproxy.com
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Equiscript (Net ID: 00:18:0A:6F:8C:EC)
2023-05-12 03:08:51	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.119
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	KKR Internal (Net ID: 00:01:21:70:65:30)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	slideshare (Category: social) https://www.slideshare.net/ayhu
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	WLAN (Net ID: 00:01:24:F1:C9:FE)
2023-05-12 02:59:58	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	myemail@example.org
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Wireless (Net ID: 00:09:5B:34:6B:03)
2023-05-12 02:51:55	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:53:52:1f:22:68:d4:e4:bd:04:c1:ea:37:ae:da:35:a4:38 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: C8:7D: f7:ed:0f:4c:8f:0b:db:e5:06:bb:72:05:39:49:bb:58:4f:45: 0e:5b:f1:2e:b2:4b:34:8d:39:4c:05:01:1d:fa:e6:54:8b:64: f4:28:60:af:2e:58:5a:36:
2023-05-12 02:59:58	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	name@example.com
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	leo (Net ID: 00:01:71:0A:06:4D)
2023-05-12 02:46:55	Internet Name	No	DNS Resolver	0	0	2	0	None	www.battleb0t.xyz
2023-05-12 03:09:54	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	plesk2.keyubu.net
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.226): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/withat_5.jpg
2023-05-12 02:54:17	Software Used	Yes	Censys	0	0	4	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:2080
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00xkhaled.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:56:51	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ssuhome (Net ID: 00:0C:41:BD:78:F1)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATT3p3p8g9 (Net ID: 84:61:A0:CD:52:30)
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:8080

2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Beens Gast (Net ID: 00:01:21:1C:17:A1)
2023-05-12 03:11:25	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'format': {u'international': u'+14806242505', u'local': u'(480) 624-2505'}, u'country': {u'prefix': u'+1', u'code': u'US', u'name':
2023-05-12 02:53:12	Web Technology	No	Tool - WAFW00F	0	0	3	0	None	Cloudflare Inc. Cloudflare
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:50:55:6d:e5:64:92:a0:7f:d0:de:03:2b:af:77:c2:fc:fe Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: CB:34: 01:1a:ea:aa:63:1c:40:bd:2f:59:0a:34:b7:be:8a:f1:7e:27: 85:d0:0e:96:7f:f0:0b:eb:18:35:77:95:6b:27:bf:9c:18:72: 58:89:63:0e:ed:84:1b:cb:
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.112): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/kappi_1.png
2023-05-12 02:56:56	Internet Name	No	DNS Resolver	0	0	3	0	None	www.ayhu.xyz
2023-05-12 02:44:03	Domain Name	No	SpiderFoot UI	25	0	0	0	None	ayhu.xyz
2023-05-12 02:54:04	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_ u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relev "92zPtBhPNqw79Ij1E865zBUv7myRJQVF_1_.woff" has type "Web Open Font Format TrueType length 25980 version 1.1"- [targetUID: N/A]'}, {u'c family=Noto+Sans+JP:wght@300;400;500;900&display=swap"\n Pattern match: "https://fonts.googleapis.com/css2?family=Jost:wght@300;400;50
2023-05-12 02:44:21	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 401 Unauthorized Date: <REDACTED> Server: cPanel Persistent-Auth: false Host: 87.248.157.102:2077 Cache-Control: no-cache, no
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	denis (Net ID: 00:01:46:02:C4:4C)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	<no ssid> (Net ID: 00:02:2D:8E:E3:CD)
2023-05-12 03:09:25	Co-Hosted Site - Domain Whois	No	Whois	2	0	4	0	None	Domain Name: DONTKILLMYAPP.COM Registry Domain ID: 2344645406_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.ascio.com Registrar URL: h via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its compute Not Disclosed Admin Fax: Not Disclosed Admin Fax Ext: Not Disclosed Admin Email: Not Disclosed Registry Tech ID: Not Disclosed Tech Na
2023-05-12 03:24:51	Country	No	Country Name Extractor	0	0	6	0	None	Turkey
2023-05-12 03:03:59	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	ebrahemsamir.github.io
2023-05-12 02:54:23	HTTP Headers	No	Censys	0	0	4	0	None	{"Date": ["<REDACTED>"], "_encoding": {"Date": "DISPLAY_UTF8", "Content_Length": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "S
2023-05-12 03:01:18	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.162): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:47:32	Raw Data from RIRs	No	Hybrid Analysis	2	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\Local\\ChromeProcessSingletonStartup!"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:5004:304:WilSt (console) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\\(x86)\\Microsoft\\Edge\\Application\\103.0.1264.37\\WidevineCdm_platfor long lines with CRLF line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Edge Shopping\\2.0.2353.0\\edge_driver. u'"widevinecdm.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\\(x86)\\Microsoft\\Ed
2023-05-12 03:23:44	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.17:8080
2023-05-12 02:45:56	Raw Data from RIRs	No	AbstractAPI	0	0	4	0	None	{u'city': u'Ashburn', u'security': {u'is_vpn': False}, u'city_geoname_id': 4744870, u'region_geoname_id': 6254928, u'country': u'Unite
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	UnitedStatesOfSmash (Net ID: F8:F5:32:A5:DE:80)

2023-05-12 03:04:11	Malicious Co-Hosted Site	Yes	abuse.ch	0	1	2	0	None	abuse.ch URLhaus (Domain) [www.github.com] https://urlhaus.abuse.ch/downloads/csv_recent/
2023-05-12 02:54:20	Web Content Type	No	Web Spider	0	0	2	0	None	text/html;charset=utf-8
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	NH-NEW (Net ID: 00:01:21:31:EF:16)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:0C:41:F9:92:AD)
2023-05-12 02:53:45	Open TCP Port	No	Censys	0	0	2	0	None	2606:50c0:8002::153:80
2023-05-12 03:16:17	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	ahu.xyz
2023-05-12 02:54:10	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myjoey (Net ID: 00:0C:41:D4:C9:9B)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	DTLAMN5 (Net ID: 00:01:9F:20:3C:A4)
2023-05-12 02:46:23	Netblock Membership	No	RIPE	8	0	2	0	None	185.199.108.0/24
2023-05-12 03:11:22	Physical Location	No	AbstractAPI	0	0	3	0	None	Frankfurt am Main, Hesse, 60313, Germany, Europe
2023-05-12 03:09:26	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3
2023-05-12 03:13:06	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [007ayong.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/withat_4.jpg
2023-05-12 02:45:17	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, has type "data"- [targetUID: N/A]\n "fa-light-300_1_.eot" has type "Embedded OpenType (EOT) Font Awesome 5 Pro Light family"- [targetU N/A]\n "RecoveryStore._DEC7D8E1-EF98-11ED-B516-080027C3EB44_.dat" has type "Composite Document File V2 Document Cannot read section in u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relev
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SurfandSip Wavelan (Net ID: 00:02:2D:01:79:94)
2023-05-12 02:45:04	Country	No	Country Name Extractor	0	0	2	0	None	United States
2023-05-12 02:44:29	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	2	0	None	github.com
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ZnKgqHhkfhEMG0RRLEy55qXrIGT89PCJPvhlAxU1THPzwDrL5gc7PkT%
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-th.github.io
2023-05-12 03:00:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	zlib@openssh.com
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Tech Overdrive (Net ID: 00:0B:6C:BB:FB:4A)
2023-05-12 03:14:48	Vulnerability - CVE High	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 7.5 Description: The DES and Triple DES ciphers, as used in the TL
2023-05-	Web	No	Language	0	0	5	0	None	

12 03:15:35	Content Language		Detector						English
2023-05-12 02:50:01	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\VERMGMTBlockListFileMutex"\n "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "\\Sessions\\1\\BaseNamedObjects\\{5312EE61-79E3-4A24-BFE1-132 Windows 2000/XP setup 62932 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"'}, {u'category': u'Installat image"- [targetUID: N/A]'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifier': u'string-3', u'name': u'Found u'malicious_identifiers': [], u'malicious_identifiers_count': 0, u'technique': u'DNS', u'informative_identifiers': [], u'tactic': u'Co
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	x-served-by: cache-ewr18140-EWR
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.226): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Kaesler (Net ID: 00:14:5C:86:BC:3E)
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.161): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:13	Web Content	No	Web Spider	0	0	3	0	None	!function(e){var t={};function n(i){if(t[i])return t[i].exports;var r=t[i]={i:i,l:!1,exports:{}};return e[i].call(r.exports,r,r.export this.x=e.x+t.x,this.y=e.y+t.y,this.z=e.z+t.z,this},addScaledVector:function(e,t){return this.x+=e.x*t,this.y+=e.y*t,this.z+=e.z*t,this t=this.x,n=this.y,i=this.z,r=e.elements;return this.x=r[0]*t+r[4]*n+r[8]*i,this.y=r[1]*t+r[5]*n+r[9]*i,this.z=r[2]*t+r[6]*n+r[10]*i,th this.subVectors(t,e).multiplyScalar(n).add(e)},cross:function(e,t){return void 0!==t?(console.warn("THREE.Vector3: .cross() now only a (t=0),e[t]=this.x,e[t+1]=this.y,e[t+2]=this.z,e},fromBufferAttribute:function(e,t,n){return void 0!==n&&console.warn("THREE.Vector3: o
2023-05-12 02:58:18	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur domains', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'thre 00002556]\n "6xK1dSBYKcSV-LCoeQqfX1RYOo3qPZ7nsDQ_1_.woff" has type "Web Open Font Format TrueType length 15704 version 1.1"- [targetUI "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "theme_1_.css" has type "UTF-8 Unicode (with BOM) t C6b!n%b\'nG\nR5JOKs}OpeH8)W7$I\nGSxaK~7oYUV*FKzg#5Q8(=!e"F.3oW2}RV^Rt^P$8Yr^-4{Wj]?hYMPi6MlT3c9#i%zp,,tIYaRFDlf):72+G+$W3aHQ.#Awve\'Cv
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	2	0	3	0	None	https://pics.battleb0t.xyz/images/withat_3.jpg
2023-05-12 03:36:57	Physical Location	No	MetaDefender	0	0	2	0	None	Tehran, Iran
2023-05-12 02:54:27	HTTP Headers	No	Censys	0	0	4	0	None	{"Content_Length": ["0"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "
2023-05-12 03:41:36	Physical Location	No	AbstractAPI	1	0	3	0	None	Eygelshoven, Limburg, 6471, Netherlands, Europe
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.36): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	scratch (Category: coding) https://scratch.mit.edu/users/ayshoo/
2023-05-12 03:09:47	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	71.170.74.34.bc.googleusercontent.com
2023-05-12 03:09:28	Open TCP Port	No	SSL Certificate Analyzer	0	0	3	0	None	165.232.113.85:443
2023-05-12 02:54:51	Open TCP Port	No	Censys	0	0	3	0	None	34.74.170.74:443
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MobileInternet (Net ID: 00:02:B3:AE:E3:34)
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: <REDACTED> Cache-Control: no-cache, no-store, must-re
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	x-cache-hits: 1
2023-05-12 02:55:16	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 4A24-BFE1-132B85B23C3A}"\n "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "IsoScope_ff8_ConnHashTable<4088>_HashTable_Mutex"\n "Local\\Zon [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 00000000-00003292]\n "bulle "Cab5361.tmp" has type "Microsoft Cabinet archive data Windows 2000/XP setup 62932 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 d SJC\nX-Cache: MISS\nX-Cache-Hits: 0\nX-Timer: S1676941063.658138,VS0,VE95\nVary: Accept-Encoding\nX-Fastly-Request-ID: cdb302efca5f6fb
2023-05-12 02:44:24	Co-Hosted Site -	No	SSL Certificate Analyzer	0	0	2	0	None	github.io

	Domain Name								
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 02:44:22	Physical Location	No	ipstack	0	0	2	0	None	Netherlands
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.217): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:33:53	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	<!DOCTYPE html> <html> <head> <title>Page Not Found</title> <style> </style> </head> <body> <h1>Page Not Found</h1> <p>Looks li
2023-05-12 03:03:51	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	malsup.github.io
2023-05-12 02:58:45	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "142.251.46.232:443"\n "142.251.46.195:80"\n "142.250.188.14:80"'}, {u'category': u'General', u'origin': u'Binary File', u'identifier' file: "GTDQ1BCW.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\GTDQ1BCW.txt]- [targetUID: 00000000-00004048]\n Dropped file [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\3538626A1FCCCA43C7E18F220BDD9B02]- [targetUID: 00000000-00003196]\n "~DF7C [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\BAD725C80F9E10846F35D039A996E4A8_88B6AE015495C1ECC395D19C1DD02894]- [targe
2023-05-12 02:47:32	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.135.9:80
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pfa (Net ID: 00:02:6F:C4:70:30)
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Pinterest (Category: social) https://www.pinterest.com/Altpapier/
2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	freesound (Category: music) https://freesound.org/people/Altpapier/
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:54:18	Web Content	No	Web Spider	4	0	2	0	None	<!DOCTYPE html> <html> <head> <meta charset="utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0" /> <link header) </td> </tr> <tr> <td>403</td> <td>The provided token does not exist</td> </tr> <tr> <td>404</td> <td>There is no player with t <code>GET</code> /v1/items/:user</h3> <h3 id="get-v1profileuserprofileitems"><code>GET</code> /v1/items/:user/:profile</h3> <h3 id="ge
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:09:55	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:16:17	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	aihu.xyz
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	COLOURlovers (Category: hobby) https://www.colourlovers.com/lover/login
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	villagio (Net ID: 00:01:24:F0:87:66)
2023-05-12 03:33:55	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	!22222222222222222222222222222222222222222222222222 3 zVm Y7a5mH LyBu5 @rO$T gt@G<U rCrV8 e$?>z DvgsWuM_ w"$RO WW uvW_c KT`\d Vb /'T T
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ALARM (5F:3F:FA) (Net ID: 00:02:D1:5F:3F:FA)
2023-05-12 02:44:09	SSL Certificate - Issued to	No	CertSpotter	0	0	1	0	None	CN=*.ayhu.xyz
2023-05-12 03:33:55	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	cHRM IDATx 9RD@R 6_:f Q3ot<@ :_w$`i 8vw8uLk iZpj bI@kd IDAT> !H?RZ Rz`8< e RmZ !heNN ZZ@"U P>HZD xq5E H!wqlM qkR` Z9wq-'C ghdf9egC O'
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	suddenlink.net-ABFB (Net ID: 2C:99:24:4F:AB:F9)
2023-05-12 02:54:20	Web Content	No	Web Spider	0	0	4	0	None	body{ padding-top:70px; } .jumbotron{ color: #2c3e50; background-color: #ecf0f1; } .navbar-inverse{ color: #2c3e50; } .navbar-inverse
2023-05-12 02:44:27	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Patreon

2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	3	0	None	cloudflare
2023-05-12 03:32:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.15:8443
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://funny.battleb0t.xyz/images/jonas.PNG
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.99): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:27	Raw Data from RIRs	No	URLScan.io	0	0	1	0	None	[{u'sort': [1674665560412, u'ef04bede-91fb-48d6-84cd-c81b2eb86237'], u'task': {u'domain': u'ayhu.xyz', u'uuid': u'ef04bede-91fb-48d6-8
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.104): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BGINET (Net ID: 00:00:C5:D7:41:64)
2023-05-12 02:58:49	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 3806DDDA3B5D}"\n "IsoScope_d40_IE_EarlyTabStart_0xc28_Mutex"\n "IsoScope_d40_IESQMMUTEX_0_519"\n "IsoScope_d40_IESQMMUTEX_0_303"\n "Lo u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': None, [%APPDATA%\\Microsoft\\Windows\\Cookies\\EL1FQVV9.txt]- [targetUID: 00000000-00003392]\n "favicon_6_.ico" has type "MS Windows icon re 2, u'description': u'Pattern match: "https://jsv3.recruitics.com/redirect?rx_cid=3394&rx_jobId=22014906&rx_url=https%3A%2F%2Fkeen-quei
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pancakes (Net ID: 00:00:48:67:6D:D1)
2023-05-12 03:11:18	Physical Location	No	AbstractAPI	0	0	2	0	None	Amsterdam, North Holland, 1012, Netherlands, Europe
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00nave198.github.io
2023-05-12 02:46:40	Malicious IP Address	Yes	Fraudguard	0	1	2	0	None	abuse_tracker (risk level: 4) [185.199.109.153]
2023-05-12 02:45:52	Physical Location	No	AbstractAPI	0	0	4	0	None	Montreal, Quebec, H4X, United States, North America
2023-05-12 03:03:16	Co-Hosted Site - Domain Name	No	DNS Resolver	1	0	2	0	None	nom-nom.link
2023-05-12 02:54:16	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: <REDACTED> Cache-Control: no-cache, no-store, must-re
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.209): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	inaturalist (Category: hobby) https://inaturalist.nz/people/login
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	sflan22 (Net ID: 00:02:6F:04:8F:03)
2023-05-12 02:54:57	Open TCP Port	No	Censys	0	0	2	0	None	2a06:98c1:3120::1:80
2023-05-12 02:54:23	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2023-05-12 02:46:27	Netblock Membership	No	RIPE	2	0	2	0	None	172.67.128.0/20
2023-05-12 02:59:47	Affiliate - Domain Whois	No	Whois	4	0	3	0	None	Domain Name: CLOUDFLARE.NET Registry Domain ID: 1542998918_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.cloudflare.com Registrar URL: ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information abou Status: serverupdateprohibited https://icann.org/epp#serverupdateprohibited Domain Status: clientupdateprohibited https://icann.org/ep abuse@cloudflare.com Registrar Abuse Contact Phone: +1.4153197517 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.i
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	youpic (Category: hobby) https://youpic.com/photographer/login
2023-05-12	WiFi Access	No	Wigle.net	0	0	5	0	None	AP Checkpoint (Net ID: 00:02:6F:B8:A2:4E)

03:18:58	Point Nearby								
2023-05-12 02:52:50	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://a Location: [%TEMP%\\Cab103E.tmp]- [targetUID: 00000000-00002984]'}, {u'category': u'Installation/Persistence', u'origin': u'API Call', Location: [%TEMP%\\Tar104F.tmp]- [targetUID: 00000000-00002984]\n "js_1_.js" has type "ASCII text with very long lines"- [targetUID: N has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\KEZ36X8R.txt]- [targetUID: 00000000-00002984]\n "PKAFXDSQ.tx
2023-05-12 03:41:52	Software Used	Yes	Censys	0	0	3	0	None	Microsoft HTTP API 2.0
2023-05-12 03:00:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.40): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:32:34	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.17:8443
2023-05-12 02:57:54	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'type': 8, u'description': u'Antivirus vendors marked dropped file "urlblockindex_1_.bin" as clean (type is "data")\n Antivirus vendo [%APPDATA%\\Microsoft\\Windows\\Cookies\\9S977TF0.txt]- [targetUID: 00000000-00001416]\n Dropped file: "F0N74D5J.txt" - Location: [%AP [%APPDATA%\\Microsoft\\Windows\\Cookies\\500MI2ZK.txt]- [targetUID: 00000000-00001416]'}, {u'category': u'Installation/Persistence', u cerrar_1_.png" has type "PNG image data 74 x 72 8-bit/color RGBA non-interlaced"- [targetUID: N/A]\n "CAF4703619713E3F18D8A9D5D88D6288
2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.118
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.194): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:12:10	Affiliate Description - Category	No	DuckDuckGo	0	0	5	0	None	Web analytics
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	1	2	0	None	SSH-2.0-OpenSSH_7.4
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	happy (Net ID: 00:02:2D:07:AC:B9)
2023-05-12 02:45:14	Physical Location	No	ipapi.co	0	0	2	0	None	Toronto, Ontario, ON, Canada, CA
2023-05-12 03:09:35	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	217.30.196.104.bc.googleusercontent.com
2023-05-12 02:54:48	Raw Data from RIRs	No	Censys	0	0	3	0	None	{"last_updated_at": "2023-05-11T22:48:59.738Z", "ip": "34.148.97.127", "location_updated_at": "2023-05-07T06:36:14.845364Z", "autonomo 19T23:50:51.069456568Z"}, "www.carbonex.xyz": {"record_type": "A", "resolved_at": "2022-12-28T17:39:27.796691436Z"}, "www.pensioenbija 02-11T13:54:10.085606219Z"}, "bear-squad-nft.com": {"record_type": "A", "resolved_at": "2023-02-26T13:24:26.630933717Z"}, "curatoriald "www.melhoriadeprojeto.com.br": {"record_type": "CNAME", "resolved_at": "2022-11-14T12:20:44.734549845Z"}, "alexhandy.co.uk": {"record {"record_type": "CNAME", "resolved_at": "2023-01-27T15:12:08.705210499Z"}, "www.massagem.pro": {"record_type": "CNAME", "resolved_at":
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	internal (Net ID: 00:0C:41:12:D6:E5)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:EE:D7:F2)
2023-05-12 03:00:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-64@openssh.com
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	REL (Net ID: 00:02:2D:02:35:63)
2023-05-12 03:09:45	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	131.97.148.34.bc.googleusercontent.com
2023-05-12 03:41:55	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	mail.inflany.com
2023-05-12 03:03:15	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=VywvBB1i7auboS6du2SyYTMISxYgv0SAv9G2irfzrfSoLR0rWIxDql%2

2023-05-12 03:33:52	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	IDATx VC6.NV cN u:v O3dufp YEexY?w a:Y7" O5dgc vR K nkRZD 227sO5d ffFsk 4kFQZW /\\J J 4 N AaoCX 9$BfJ cod:5j M:IBU VBjeb d<nDA `CK2nF
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/nomnom.jpg
2023-05-12 02:44:16	Internet Name	No	DNS Resolver	2	0	2	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.206): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.63): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	admire_me (Category: XXXPORNXXX) https://admireme.vip/login/
2023-05-12 02:46:19	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki [%TEMP%\\7904_1910241172\\manifest.json]- [targetUID: 00000000-00007904]\n "60f652af-af71-4e18-8f97-f706eb4108c1.tmp" has type "ASCII u'File/Memory', u'identifier': u'string-3', u'name': u'Found potential URL in binary/memory', u'attck_id_wiki': None, u'threat_level_h Antivirus vendors marked sample as malicious (0% detection rate)'}, {u'category': u'Installation/Persistence', u'origin': u'Binary Fil
2023-05-12 02:47:21	Open TCP Port	No	Pulsedive	0	0	2	0	None	185.199.111.153:443
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	fse2 (Net ID: 00:01:38:A0:A1:09)
2023-05-12 03:09:18	Vulnerability - General	Yes	Tool - Retire.js	0	0	4	0	None	CVE-2016-10735 Score: Unknown Description: Unknown
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	do not seek the treasure (Net ID: 00:01:24:F1:72:12)
2023-05-12 02:46:03	Physical Location	No	AbstractAPI	0	0	3	0	None	North Charleston, South Carolina, 29415, United States, North America
2023-05-12 02:46:50	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 03:32:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.17:80
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	drapnet (Net ID: 00:09:5B:52:69:9E)
2023-05-12 02:44:19	Internet Name	No	DNS Resolver	0	0	2	0	None	battleb0t.xyz
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/jcqn.jpg
2023-05-12 02:46:02	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'city': u'North Charleston', u'security': {u'is_vpn': False}, u'city_geoname_id': 4589387, u'region_geoname_id': 4597040, u'country'
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.106): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	public (Category: finance) https://public.com/@login
2023-05-	Open TCP	No	Pulsedive	0	0	3	0	None	188.114.97.11:443

12 03:32:21	Port								
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2095
2023-05-12 02:44:05	Raw Data from RIRs	No	Tool - WAFW00F	0	0	1	0	None	[{"url": "https://ayhu.xyz", "firewall": "Cloudflare", "detected": true, "manufacturer": "Cloudflare Inc."}, {"url": "https://ayhu.xyz
2023-05-12 03:31:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	589e2ad15175f1c51c0a91d29b753337-1077158@contact.gandi.net
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	0d70cf (Net ID: 00:02:2D:0D:70:CF)
2023-05-12 03:00:51	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.73): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SMG (Net ID: 00:0C:41:BD:EA:B0)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	tsunami (Net ID: 00:0D:28:68:59:E3)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	linksys (Net ID: 00:18:39:2C:B7:B2)
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 02:54:20	HTTP Headers	No	Web Spider	2	0	4	0	None	{"content-length": "243", "accept-ranges": "bytes", "strict-transport-security": "max-age=31536000", "server": "Netlify", "etag": "\"c
2023-05-12 02:45:44	Physical Location	No	MetaDefender	0	0	2	0	None	San Francisco, United States
2023-05-12 03:01:17	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.150): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:25	Internet Name	No	DNS Resolver	0	0	2	0	None	funny.battleb0t.xyz
2023-05-12 02:56:53	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\SM0:6324:304:WilStaging_02"\n "Local\\SM0:6324:120:WilError_01"\n "Local\\InternetShortcutMutex"\n "Local\\SM0:3348:120:WilErr 00003348]\n "765cfe4494a18824_0" has type "data"- [targetUID: N/A]\n "load_statistics.db-wal" has type "SQLite Write-Ahead Log version Cache\\js\\c1970b30fb6d8527_0]- [targetUID: 00000000-00003348]'}, {u'category': u'Spyware/Information Retrieval', u'origin': u'File/Me by Antivirus engines', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevanc
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	attwifi (Net ID: 00:14:6A:5B:53:92)
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.17): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet1383 (Net ID: 00:08:52:1E:13:81)
2023-05-12 03:04:07	Malicious IP on Same Subnet	Yes	Greensnow	0	0	4	0	None	greensnow.co [46.101.128.0/17] https://blocklist.greensnow.co/greensnow.txt
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	1	0	2	0	None	(c) CentralNic Ltd
2023-05-12 02:45:27	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur File: "urlref_httpsk8slens.devindex.html")\n Found string "TWITTER" (I Found string "<p class="card-text"><small class="text-muted"><a href="https://twitter.com/jaydrogers/status/1363986936222908416"><i cl u'threat_level': 0, u'type': 6, u'description': u'"msedge.exe" writes file "c:\\users\\%osuser%\\appdata\\local\\microsoft\\edge\\user 2384 x 1453 8-bit/color RGBA non-interlaced"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Cache\\Cache_Data\\f_000
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:33:35	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	<!DOCTYPE html> <html> <head> <title>Page Not Found</title> <style> </style> </head> <body> <h1>Page Not Found</h1> <p>Looks li
2023-05-	Co-Hosted	No	DNS Resolver	0	0	3	0	None	

12 03:03:28	Site - Domain Name								github.io
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+74955801111
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	gclabc (Net ID: 00:0B:86:22:0F:31)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	tsunami (Net ID: 00:0D:29:AC:D8:FE)
2023-05-12 02:44:19	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 03:31:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	abuse@support.gandi.net
2023-05-12 03:03:27	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetA41A (Net ID: 00:01:36:57:A4:18)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Best Western Lobby (Net ID: 00:02:2D:66:D4:75)
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Git (software)
2023-05-12 02:44:39	Internet Name	No	DNS Resolver	0	0	2	0	None	www.battleb0t.xyz
2023-05-12 03:43:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	87.248.157.79:443
2023-05-12 03:13:04	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [000yesnt.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Houzz (Category: hobby) https://www.houzz.com/user/login
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	6dgs (Net ID: 00:06:B1:28:66:65)
2023-05-12 03:33:59	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	IDATx ? `sm b"0N9 3@N:vn yj4BZu:- pqmVU hEC0s c@ h' 6FcPkh4 2:Eu` IDAT nfwPH jniEDkf 9uCGxN MWFGv '!hXQf 6WoW' hRoWW 68ZQ$ 8Ro7Tr 2j3y
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	The Batcave (Net ID: 00:11:32:A4:B5:6C)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Piekielni (Category: misc) https://piekielni.pl/user/login
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	FUNK-STEDE (Net ID: 00:02:2D:3D:3E:AD)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BeensGroep (Net ID: 00:01:21:1F:B1:A0)
2023-05-12 03:13:09	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [010pixel.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:23:38	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.14:8443
2023-05-12 02:44:23	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 02:47:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	104.196.30.220:443

2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpaceStation (Net ID: 00:02:2D:01:CF:F8)
2023-05-12 02:53:49	Open TCP Port	No	Censys	0	0	2	0	None	2606:50c0:8000::153:443
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Ziggo8BDDE0 (Net ID: 00:0C:F6:8B:DD:E0)
2023-05-12 03:08:52	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.128
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:54:15	HTTP Headers	No	Web Spider	6	0	2	0	None	{"nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "x-powered-by": "Express", "transfer-encoding": "chunk
2023-05-12 03:31:33	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	westabuse@gmail.com
2023-05-12 02:53:39	Netblock Membership	No	Censys	0	0	2	0	None	185.199.108.0/24
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	AP Checkpoint (Net ID: 00:02:6F:B8:A2:4E)
2023-05-12 02:51:07	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:99:a3:5c:44:13:8f:1f:f4:9f:74:e5:4f:ad:57:81:83:24 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 98:BA: 62:4e:f9:b9:59:d2:7d:9b:3a:75:2f:82:0e:77:1f:fa:cc:3b: 4e:90:c2:ba:e9:1d:4c:b0:a0:53:8e:4b:72:4b:e7:12:e4:36: 5a:97:fc:6e:97:fc:a5:f5:
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	sflan51 (Net ID: 00:02:6F:09:B2:F7)
2023-05-12 02:59:47	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	battleb0t.xyz@regprivate.ru
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys-g (Net ID: 00:0C:41:14:DD:46)
2023-05-12 03:33:11	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [185.199.111.153] https://www.virustotal.com/en/ip-address/185.199.111.153/information/
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	TB Proprietary Channel. 01 (Net ID: 00:04:32:38:A1:09)
2023-05-12 02:46:49	Open TCP Port	No	SSL Certificate Analyzer	0	0	3	0	None	64.226.81.43:443
2023-05-12 02:53:42	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-12T01:22:57.156Z", "ip": "185.199.109.153", "location_updated_at": "2023-05-05T05:03:49.200600Z", "autono 04-05T18:19:59.923721676Z"}, "dev.baicom.com": {"record_type": "CNAME", "resolved_at": "2023-05-03T13:55:02.514462461Z"}, "www.jordanc 04-21T22:50:25.934348288Z"}, "www.trivial.group": {"record_type": "CNAME", "resolved_at": "2023-02-22T16:56:04.473316622Z"}, "alzhao.c "resolved_at": "2022-10-02T12:04:48.017779237Z"}, "turtledev.in": {"record_type": "A", "resolved_at": "2023-03-17T16:23:43.722396430Z" "www.unixlife.dev": {"record_type": "CNAME", "resolved_at": "2022-10-04T14:32:50.060827864Z"}, "www.kadupitiya.lk": {"record_type": "C
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	codeforces (Category: coding) https://codeforces.com/profile/login
2023-05-12 02:44:13	IP Address	No	DNS Resolver	204	0	1	0	None	185.199.111.153
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.47): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:17	Internet Name	No	DNS Resolver	2	0	2	0	None	nwapi.battleb0t.xyz

2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	172.67.168.252
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	02:32:42 (Net ID: 00:02:2D:01:53:95)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	#LG@Vo1P*Service& (Net ID: 00:01:36:57:A4:17)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Jupiter (Net ID: 00:02:2D:66:D2:49)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Microsoft Technet Community (Category: tech) https://social.technet.microsoft.com/profile/login/
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomAC2DD8 (Net ID: 00:0C:F6:AC:2D:D8)
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATT8QH8gLT (Net ID: E0:22:02:14:AB:06)
2023-05-12 02:56:55	Internet Name	No	DNS Resolver	0	0	2	0	None	battleb0t.xyz
2023-05-12 02:44:18	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 02:46:36	Netblock Membership	No	RIPE	2	0	3	0	None	34.148.96.0/20
2023-05-12 03:31:58	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.0:8443
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00saadchaudhry.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:54:19	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relevance': 3, u'threat_level': 0, u'type': 8, u'de 00002076]\n "adblock_snippet.js" has type "ASCII text with very long lines with no line terminators"- Location: [%TEMP%\\2076_20986491 "https://npbruce.github.io/valkyrie/"\n Pattern match: "http://www.w3.org/2000/svg\\n"\n Pattern match: "http://www.w3.org/2000/svg"\n u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'suspicious', u'capec_id': None, u'attck_id': u'T1105', u'releva
2023-05-12 03:01:15	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.137): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:32	Raw Data from RIRs	No	PhishStats	0	0	2	0	None	[{u'page_text': u' ', u'domain': None, u'virus_total': None, u'n_times_seen_ip': None, u'abuse_contact': None, u'ip': u'185.199.109.15
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.21): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:09:26	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	188.114.96.1:443
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	6	0	None	cloudflare
2023-05-12 02:56:09	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "IsoScope_6ac_IESQMMUTEX_0_519"'}, {u'category': u'General', u'origin': u'Binary File', u'identifier': u'binary-16', u'name': u'Drops line terminators"- [targetUID: N/A]\n "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has type "PNG image data 16 x 16 4-bit color appId=cid-v1:7d63747b-487e-492a-872d-762362f77974\nX-Response-Cache-Status: True\nExpires: Tue, 08 Nov 2022 02:16:24 GMT\nCache-Contro u'machine_learning_models': [], u'total_signatures': 7, u'image_base': None, u'error_origin': None, u'ssdeep': u'Unknown', u'entrypoin
2023-05-12 03:00:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.10): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:13:06	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [008security.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:06	Externally Hosted Javascript	No	Page Information	0	0	3	0	None	https://www.google-analytics.com/analytics.js

2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	Domains By Proxy, LLC
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-github-request-id: 70D2:0CB6:1A723F4:28AE86F:645DAA55
2023-05-12 02:53:17	IP Address	No	Mnemonic PassiveDNS	74	0	1	0	None	188.114.96.1
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:8d:d7:e0:05:18:38:a5:db:8a:48:64:f2:68:9a:98:22:c8 Signature Algorithm: sha256Wi 2023 GMT Extensions: none Signature : ecdsa-with-SHA256 30:44:02:20:43:38:D1:BA:46:EB:FB:AE:E5:0E:F5:96: 0C:2E:94:E5:49:45:23:64:6A:0D
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	roLAN (Net ID: 00:0F:B5:E5:CF:1E)
2023-05-12 03:10:04	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	beatrixhaller.at
2023-05-12 02:56:32	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 26:cc:7f:01:c6:92:25:78:13:50:9e:48:80:75:15:57 Signature Algorithm: sha256WithRSAE 09:9f:cd:b5:43:3b:6a:2f:1d:c9:3b:c0:c8:50:40:4b:85:6c: a4:67:c0:ea:9c:ed:fa:82:03:5a:15:d9:da:e2:17:9e:f5:4d: 17:b3:27:61:b6:b3:76:a2:
2023-05-12 02:44:35	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Cloudflare
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2083
2023-05-12 02:44:09	Raw Data from RIRs	No	CertSpotter	1	0	1	0	None	[{u'pubkey_sha256': u'b8939526809ab88640a6a7884ee8dcb607fb00f7e0fcea60466af2f352ad1591', u'cert_sha256': u'4c1b41a7240eddfb2785d811a40 u'f3559fd766dc2e51474007c996ec67cd9e85ae0fa827d3d663f5abc2eafcbe24', u'friendly_name': u'Google Trust Services', u'name': u'C=US, O=Go [u'*.ayhu.xyz', u'ayhu.xyz'], u'tbs_sha256': u'e25b9a56735c29036e5e585244fde0a2ba81adaf796b2d716bde988fd3954995', u'id': u'5073393240'
2023-05-12 03:09:46	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	64.170.74.34.bc.googleusercontent.com
2023-05-12 02:46:24	Physical Location	No	MetaDefender	0	0	3	0	None	North Charleston, United States
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	000justin000.github.io
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	LINE (Category: social) https://line.me/R/ti/p/@login?from=page
2023-05-12 02:59:09	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 0, u'threat_level': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 8, u'description': u'"57C8EDB95DF3F0AD4EE2DC2B8CFD4157" has ty [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\57C8EDB95DF3F0AD4EE2DC2B8CFD4157]- [targetUID: 00000000-00003300]\n "Cab11F [Source: Input]\n Pattern match: "https://regclickonetwoget.com"- [Source: Input]'}, {u'category': u'Network Related', u'origin': u'Fi
2023-05-12 03:12:52	Physical Location	No	numverify	0	0	3	0	None	Phoenix, US
2023-05-12 02:54:18	Linked URL - External	No	Web Spider	0	0	3	0	None	https://discord.com/api/oauth2/authorize?client_id=1073319920575713290&redirect_uri=https://yoink.site/auth&response_type=code&scope=i
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Gab (Category: political) https://gab.com/ayhu
2023-05-12 03:01:19	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.168): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	IntelWLAN (Net ID: 00:02:B3:C4:42:9C)
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.110): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.90): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:11:23	Physical Location	No	AbstractAPI	0	0	3	0	None	Moscow, Russian Federation
2023-05-12 02:55:01	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America

2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Gitea - Gitea is a forge software package for hosting software development version control using Git as well as other collaborative fe
2023-05-12 02:59:57	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:10:b4:30:a3:e0:72:2f:ec:4e:bc:95:e3:12:bb:83:8d:6f Signature Algorithm: ecdsa-wi
2023-05-12 03:09:39	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	110.48.229.35.bc.googleusercontent.com
2023-05-12 03:12:10	Affiliate Description - Category	No	DuckDuckGo	0	0	5	0	None	Computer security companies
2023-05-12 02:44:30	Internet Name	No	DNS Resolver	0	0	2	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Villakakelbond1 (Net ID: 00:0C:F6:CE:B2:88)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	detyenship (Net ID: 00:02:2D:61:A7:66)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Annie's Craft Co. (Net ID: 00:02:61:19:6C:00)
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:99:a3:5c:44:13:8f:1f:f4:9f:74:e5:4f:ad:57:81:83:24 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 98:BA: 62:4e:f9:b9:59:d2:7d:9b:3a:75:2f:82:0e:77:1f:fa:cc:3b: 4e:90:c2:ba:e9:1d:4c:b0:a0:53:8e:4b:72:4b:e7:12:e4:36: 5a:97:fc:6e:97:fc:a5:f5:
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:02:2D:21:0C:9F)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-ray: 7c5f603759cec44a-EWR
2023-05-12 03:31:27	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	abuse@namecheap.com
2023-05-12 03:03:43	Internet Name	No	DNS Resolver	0	0	4	0	None	vscode.battleb0t.xyz
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.228): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:27	Internet Name	No	URLScan.io	0	0	1	0	None	kekw.battleb0t.xyz
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	default (Net ID: 00:01:46:03:E4:6F)
2023-05-12 02:55:18	Netblock Membership	No	Censys	6	0	3	0	None	46.101.128.0/17
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	3333 1370 (Net ID: 00:0F:CC:6D:BD:34)
2023-05-12 02:54:21	Linked URL - Internal	No	Web Spider	4	0	4	0	None	http://vscode.battleb0t.xyz/cdn-cgi/styles/main.css
2023-05-12 03:32:19	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.10:8443
2023-05-12 03:19:17	Web Framework	No	Web Framework Identifier	0	0	3	0	None	jQuery
2023-05-12 03:01:17	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.149): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:35	Name Server (DNS NS Records)	No	DNS Raw Records	0	0	1	0	None	brett.ns.cloudflare.com

2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2023-05-12 03:33:44	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	mntrRGB XYZ desc trXYZ <mluc -mluc 3`-O! 6fD` N@e@8 s$01@H @jlveI B4Pic .E"E3@YB 8RktA -B09: FRp.PD A7e k `kfZb A8tSNJ 4j@Q4 H8@I" `Y@
2023-05-12 03:01:01	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.106): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:54	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	cloudflare.com
2023-05-12 02:50:26	Physical Address	No	GLEIF	0	0	3	0	None	C/O REGISTERED AGENT SOLUTIONS, INC., 838 Walker Road Suite 21-2, DOVER, US-DE, US, 19904
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	WHLee (Net ID: 00:01:21:30:54:A3)
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	WHLee (Net ID: 00:01:21:30:54:A4)
2023-05-12 03:00:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.51): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:44	Software Used	Yes	Tool - Wappalyzer	0	0	3	0	None	Google Analytics
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	spacebunny (Net ID: 00:11:50:23:B8:1D)
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.91): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:09:05	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.110
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	vgf2002noxx (Net ID: 00:02:2D:74:6E:AA)
2023-05-12 03:23:19	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.5:80
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	lobste.rs (Category: tech) https://lobste.rs/u/login
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:18:53	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Rotated 180 @ 18}
2023-05-12 02:54:18	Web Content Type	No	Web Spider	0	0	2	0	None	text/html;charset=utf-8
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	pureftpd
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Project management software
2023-05-12 03:13:03	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0000-bigtree.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	W4B3P]]00S210)>&01/54&6/%&_&'_Pa (Net ID: 00:06:66:23:00:BA)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	ifunny (Category: misc) https://ifunny.co/user/login
2023-05-12 02:44:17	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 02:53:32	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America

2023-05-12 03:03:37	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=0Oz6%2FLYR6mlw4qLR9TqycfDZLMo35NVUiZYmytvsw3hnWwlYi3vXyl
2023-05-12 03:00:50	Co-Hosted Site	No	HackerTarget	1	0	2	0	None	000.dontkillmyapp.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:EE:55:AC)
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 200 OK Connection: Keep-Alive Keep-Alive: timeout=5, max=100 x-powered-by: PHP/7.4.33 content-type: text/html; charset=UTF-8
2023-05-12 02:47:21	Open TCP Port	No	Pulsedive	0	0	2	0	None	185.199.111.153:80
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 03:01:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.247): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetCBD2 (Net ID: 00:01:36:59:CB:D0)
2023-05-12 03:21:08	Account on External Site	No	Account Finder	0	0	2	0	None	Picsart (Category: art) https://picsart.com/u/dawidsulej
2023-05-12 02:56:27	Hash	No	Hash Extractor	0	0	3	0	None	[MD5] 02ca825e4901e74c2c2d6f8e59341325
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:F6:2B:B0)
2023-05-12 02:53:35	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 02:55:15	Physical Location	No	Censys	0	0	3	0	None	Frankfurt am Main, Hesse, 60306, Germany, Europe
2023-05-12 02:54:13	HTTP Headers	No	Web Spider	2	0	3	0	None	{"x-content-type-options": "nosniff", "content-encoding": "gzip", "transfer-encoding": "chunked", "expires": "Fri, 12 May 2023 04:54:1
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Interwrx2 (Net ID: 00:02:2D:A8:80:99)
2023-05-12 03:23:41	Account on External Site	No	Account Finder	0	0	8	0	None	PinkBike (Category: hobby) https://www.pinkbike.com/u/baptiste.vauthey/
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	50d173 (Net ID: 00:02:2D:50:D1:73)
2023-05-12 03:09:52	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	4	0	None	cloudflare
2023-05-12 03:34:24	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	45.131.109.47
2023-05-12 03:16:25	Username	No	Account Finder	1	0	1	0	None	dawid.sulej
2023-05-12 03:13:01	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-experiments.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	^D^M^L^W^]^C^A^U^M^Y^E^L^_^R^G (Net ID: 00:05:5D:D9:90:56)
2023-05-12 02:54:23	Raw Data from RIRs	No	Censys	0	0	4	0	None	{"last_updated_at": "2023-05-11T18:43:25.661Z", "ip": "2600:1f18:2489:8201::c8", "location_updated_at": "2023-05-10T22:49:08.075439Z", "resolved_at": "2023-03-15T21:01:17.245078119Z"}, "adoring-saha-207b27.netlify.app": {"record_type": "AAAA", "resolved_at": "2023-02-1

									"2023-03-01T12:08:22.715647640Z"}, "brave-darwin-3ec1aa.netlify.app": {"record_type": "AAAA", "resolved_at": "2023-01-12T12:06:04.7888 "resolved_at": "2023-03-20T21:11:53.928072067Z"}, "mosquesg.netlify.app": {"record_type": "AAAA", "resolved_at": "2023-03-13T12:08:14. "2023-02-28T12:07:43.347226879Z"}, "admin-toc-prod.netlify.app": {"record_type": "AAAA", "resolved_at": "2023-02-14T12:07:10.285250452
2023-05-12 03:33:53	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	!2222222222222222222222222222222222222222222222222 sH GN t5ad C'Y2z OB:`S pF>oj OQTeuy YYK`s gnqV N9FX6 EQY66 1pO'94 pj'R7pz` 0Kdes x
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:F4:A4:02)
2023-05-12 02:54:57	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2023-05-12 02:55:21	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:81:34:2e:fd:61:48:b5:6f:11:ca:36:0b:dc:62:9a:cf:52 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: A7:55:
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	^U^E^H^O^[^U^H^_^^^G^K^Z^X^E^^ (Net ID: 00:02:2D:7F:0D:E1)
2023-05-12 02:44:28	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12 02:54:15	Linked URL - External	No	Web Spider	0	0	3	0	None	https://hypixel-api.senither.com
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:8880
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-4262 (Net ID: 00:1D:D1:0B:42:60)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	2WIRE115 (Net ID: 00:00:94:D4:4C:5A)
2023-05-12 03:10:08	Malicious IP on Same Subnet	Yes	VoIPBL OpenPBX IPs	0	0	3	0	None	VOIPBL Publicly Accessible PBX List [185.199.110.0/24] http://www.voipbl.org/update
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	LocationFree.00014AEC392A (Net ID: 00:01:4A:EC:39:2A)
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.163): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:20	Physical Location	No	Censys	1	0	4	0	None	Seattle, Washington, 98108, United States, North America
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:443
2023-05-12 03:31:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	domain.operations@web.com
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 02:57:50	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'"34.148.97.127:443"'}, {u'category': u'General', u'origin': u'Created Mutant', u'identifier': u'mutant-0', u'name': u'Creates mutant compression"\n "77EC63BDA74BD0D0E0426DC8F8008506" has type "Microsoft Cabinet archive data Windows 2000/XP setup 62919 bytes 1 file at [targetUID: 00000000-00000536]\n "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has type "MS Windows icon resource - 1 icon 32x32 potential URL in binary/memory', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None,
2023-05-12 03:13:07	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00arthur00.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:55:15	Raw Data from RIRs	No	Censys	14	0	3	0	None	{"operating_system": {"vendor": "Ubuntu", "product": "Linux", "part": "o", "uniform_resource_identifier": "cpe:2.3:o:canonical:ubuntu_ "ecdsa_public_key": {"_encoding": {"b": "DISPLAY_BASE64", "gy": "DISPLAY_BASE64", "n": "DISPLAY_BASE64", "p": "DISPLAY_BASE64", "y": " "server_to_client_macs": ["umac-64-etm@openssh.com", "umac-128-etm@openssh.com", "hmac-sha2-256-etm@openssh.com", "hmac-sha2-512-etm@o "sha1:d01c97e2944166ed23e47e4a62ff471ab8fa031f"], "status_code": 404, "body_hash": "sha1:d01c97e2944166ed23e47e4a62ff471ab8fa031f", "h "67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd"}, {"issuer_dn": "O=Digital Signature Trust Co., CN=DST Root CA X3",
2023-05-12 02:54:13	Web Content	No	Web Spider	0	0	3	0	None	/* CSS Mini Reset */ html, body, div, form, fieldset, legend, label { margin: 0; padding: 0; } table { border-collapse: collapse; bord UltraLightItalic'), url('./fonts/AvenirNext-UltraLightItalic.woff2'); font-weight: 200; font-style: italic; } /* Site Styles */ :root space)/2) 0; display: grid; grid-template-columns: 1fr 5fr 5fr 1fr; grid-template-rows: auto; grid-template-areas: ". co description .

2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-cache-status: REVALIDATED
2023-05-12 02:47:46	Open TCP Port	No	Pulsedive	0	0	3	0	None	34.74.170.74:443
2023-05-12 02:44:24	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Open Graph
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.154): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.15:80
2023-05-12 02:59:57	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	support@bigmarker.com
2023-05-12 02:48:12	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur checkout-eligible-sites-pre-stable.json")\n Found string ""baysidebuddy.com"," (Indicator: "dir "; File: "wallet-pre-stable.json")\n F Indicator: "ubs.com")\n ""annabelbleu.com"," (Source: wallet-pre-stable.json, Indicator: "leu.com")\n ""aspirefashionscrubs.com"," (So u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relev [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Edge Wallet\\112.15267.15264.1\\Notification\\notification.bundle.js]- [targetUID: 000000
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	EPORNER (Category: XXXPORNXXX) https://www.eporner.com/profile/login/
2023-05-12 02:44:42	Internet Name	No	DNS Resolver	0	0	2	0	None	www.battleb0t.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:90:53:D7)
2023-05-12 02:55:21	Raw Data from RIRs	No	Censys	13	0	3	0	None	{"operating_system": {"vendor": "Ubuntu", "product": "Linux", "part": "o", "uniform_resource_identifier": "cpe:2.3:o:canonical:ubuntu_ "www.getsimnum.posadisad.com": {"record_type": "A", "resolved_at": "2023-03-27T22:00:33.577672224Z"}, "dev.pointlane.com": {"record_ty {"record_type": "A", "resolved_at": "2023-03-30T00:47:09.056676609Z"}, "the.posadisad.com": {"record_type": "A", "resolved_at": "2023- 01T16:22:34.836285670Z"}, "www.demo.pointlane.com": {"record_type": "A", "resolved_at": "2023-03-30T00:47:02.797080934Z"}, "app.pointl "extended_service_name": "SSH", "observed_at": "2023-05-11T01:15:50.786715445Z", "banner_hex": "5353482d322e302d4f70656e5353485f382e39
2023-05-12 02:54:20	Open TCP Port	No	Censys	0	0	4	0	None	2600:1f18:2489:8200::c8:443
2023-05-12 02:54:57	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	U+LGNetCF52 (Net ID: 00:01:36:5B:CF:50)
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	4	0	None	CloudFlare, Inc.
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.147): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:09:53	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.13): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:02	Username	No	Account Finder	3	0	7	0	None	baptiste.vauthey
2023-05-12 02:55:54	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur None, u'attck_id': u'T1071.001', u'relevance': 1, u'threat_level': 0, u'type': 2, u'description': u'"GET /resources/431ebba2c34b4504bd https://lor.instructure.com/resources/431ebba2c34b4504bdef6a7212f4ea30\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6. https://lor.instructure.com/resources/431ebba2c34b4504bdef6a7212f4ea30\nAccept-Language: en-US\nAccept-Encoding: gzip, deflate\nUser-A application/json\nx-session-id: undefined\nReferer: https://lor.instructure.com/resources/431ebba2c34b4504bdef6a7212f4ea30\nAccept-Lan
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 200 OK Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html last-modified: Wed, 17 Jun 2020 20:01:33
2023-05-12	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur

02:55:40									domains', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'thre gs=new RegExp(/^(.*\\.)?(google|youtube|blogger|withgoogle)(\\.com?)?(\\.[a-z]{2})?\\.?$/),hs={cl:["ecl"],customPixels:["nonGooglePixe handlers.min_1_.js" has type "ASCII text with very long lines"- [targetUID: N/A]\n "webpack.runtime.min_1_.js" has type "ASCII text wi >\ufffd\ufffd\ufffd\u0785R\ufffd\ufffd`\uac7e\ufffdQ\ufffd$z/\ufffd2\ufffd\ufffdx\ufffdM\ufffdG\ufffdk\ufffdf6Ip\ufffd\ufffd\ufffd\uff
2023-05-12 03:00:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.55): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:32	Web Technology	No	Tool - WhatWeb	0	0	3	0	None	HTML5
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:53:10:73)
2023-05-12 02:44:15	Internet Name	No	DNS Resolver	2	0	2	0	None	nuke.battleb0t.xyz
2023-05-12 03:00:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.57): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:19	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	SoundCloud (Category: music) https://soundcloud.com/Altpapier
2023-05-12 03:09:38	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	230.30.196.104.bc.googleusercontent.com
2023-05-12 03:13:07	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00d.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:53:15	IP Address	No	Mnemonic PassiveDNS	0	0	1	0	None	185.199.109.153
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-ray: 7c5f605eb97732c7-EWR
2023-05-12 02:44:15	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	HTTP/3
2023-05-12 02:48:50	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'https://attack.mitre.org/techniques/T1057', u'threat_level_human': u'informative', u'capec_id': u'CAPEC-573', u'attck_id': u'T1057', u'threat_level': 0, u'type': 7, u'description': u'"analytics.twitter.com"\n "connect.facebook.net"\n "data.pendo.io"\n "js.hs-banner.c 4.93 0 01-2.23-.614v.061a4.922 4.922 0 003.95 4.828 4.894 4.894 0 01-2.221.085A4.934 4.934 0 007.292 17.5 9.875 9.875 0 010 19.54a13.9 ["nonGooglePixels"],ecl:["cl"],ehl:["hl"],hl:["ehl"],html:["customScripts","customPixels","nonGooglePixels","nonGoogleScripts","nonGoo
2023-05-12 02:58:47	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	1	0	None	CVE-2011-3389 https://nvd.nist.gov/vuln/detail/CVE-2011-3389 Score: 4.3 Description: The SSL protocol, as used in certain configuratio
2023-05-12 02:50:34	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [185.199.109.153] https://www.virustotal.com/en/ip-address/185.199.109.153/information/
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom (Net ID: 00:01:38:A4:44:3A)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:60:0B:41)
2023-05-12 02:59:52	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 02:55:01	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	jones (Net ID: 00:04:5A:2E:16:19)
2023-05-12 03:13:01	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-oo2.github.io] https://www.openphish.com/feed.txt

2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0080004.github.io
2023-05-12 02:53:49	Open TCP Port	No	Censys	0	0	2	0	None	2606:50c0:8000::153:80
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 02:45:12	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'ON', u'country_tld': u'.ca', u'ip': u'2606:4700:3031::ac43:8709', u'currency_name': u'Dollar', u'currency': u'CAD',
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:2095
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cf-mitigated: challenge
2023-05-12 02:45:35	Name Server (DNS NS Records)	No	DNS Raw Records	0	0	1	0	None	leanna.ns.cloudflare.com
2023-05-12 03:17:36	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: AAHU.XYZ Registry Domain ID: D289905874-CNIC Registrar WHOIS Server: whois.namesilo.com Registrar URL: https://www.namesi for any purpose other than determining ownership of domain names, (2) not to store or reproduce this data in any way, (3) not to use a +1.3478717726 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: pw-55286b4dad8e2523890cab5484722bf1@privacyguardian.org Name Server:
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Klovenier (Net ID: 00:01:36:06:40:52)
2023-05-12 02:46:01	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'city': u'North Charleston', u'security': {u'is_vpn': False}, u'city_geoname_id': 4589387, u'region_geoname_id': 4597040, u'country'
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Pragma": "DISPLAY_UTF8", "Set_Cookie": "DISPLAY_UTF8", "X_Content_Type_Options": "DISPLAY_UTF8", "Connection": "DISPLA
2023-05-12 02:45:46	Raw Data from RIRs	No	Hybrid Analysis	2	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis "142.250.188.3:443"\n "142.251.46.194:443"\n "142.251.46.230:443"\n "142.250.189.202:443"\n "172.217.164.118:443"\n "142.250.189.161:4 "www.gstatic.com"\n "www.youtube.com"\n "yt3.ggpht.com"'}, {u'category': u'General', u'origin': u'File/Memory', u'identifier': u'strin is "SVG Scalable Vector Graphics image")\n Antivirus vendors marked dropped file "mm-logo_1_.svg" as clean (type is "SVG Scalable Vect u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relev
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	1	3	0	None	nginx
2023-05-12 02:44:15	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Cloudflare
2023-05-12 03:15:35	Web Content Language	No	Language Detector	0	0	3	0	None	English
2023-05-12 02:49:09	Malicious Co-Hosted Site	Yes	VirusTotal	0	1	2	0	None	VirusTotal [github.com] https://www.virustotal.com/en/domain/github.com/information/
2023-05-12 02:53:35	BGP AS Membership	No	Censys	0	0	2	0	None	54113
2023-05-12 02:48:44	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'identifier': u'network-1', u'name': u'Contacts server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_lev item"><a class="social-icon social-icon-twitter" href="https://twitter.com/OpenText"><svg width="32" height="32" viewBox="0 0 36 36" f {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_i Location: [%TEMP%\\4204_136538697\\Filtering Rules-AA]- [targetUID: 00000000-00004204]\n "000014.ldb" has type "data"- [targetUID: N/A
2023-05-12 03:41:55	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	inflany.com
2023-05-12 02:50:09	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 8, u'descr "GET /css?family=Lato:300,400,700|Raleway:300,400,500|Open+Sans:300,400,600,700,800 HTTP/1.1\nAccept: text/css, */*\nReferer: http://d "mozilla/5.0 (")\n "GET /-nterforce/jquery.cycle.min.js HTTP/1.1\nAccept: application/javascript, */*;q=0.8\nReferer: http://driverthe HTTP/1.1\nAccept: application/javascript, */*;q=0.8\nReferer: http://drivertheorytest.com/\nAccept-Language: en-US\nUser-Agent: Mozill
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:0C:41:36:94:66)

2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	0	0	1	0	None	CN=kekw.battleb0t.xyz
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Project management software
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	4	0	None	cloudflare
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	likeevideo (Category: social) https://likee.video/@ayshoo
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+74955801111
2023-05-12 03:09:48	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	76.170.74.34.bc.googleusercontent.com
2023-05-12 02:51:23	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', extension "png"\n "favicon_4_.png" has type "MS Windows icon resource - 2 icons 16x16 32 bits/pixel 32x32 32 bits/pixel" and extension [%TEMP%\\CabEAA.tmp]- [targetUID: 00000000-00002236]\n "en-US.4" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Internet Explo [%APPDATA%\\Microsoft\\Windows\\Cookies\\XHRTG3Z7.txt]- [targetUID: 00000000-00002236]\n "D4D4P3AW.txt" has type "ASCII text"- Locatio
2023-05-12 02:44:37	Internet Name	No	DNS Resolver	0	0	2	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:5E:6E:39)
2023-05-12 02:52:30	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'https://attack.mitre.org/techniques/T1083', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1083', u'relev "data_2" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Cache\\Cache_Data\\data_2]- [targetUID: 0000 3.x database last written using SQLite version 3039003"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\load_statisti type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Cache\\Cache_Data\\data_0]- [targetUID: 00000000-00006260
2023-05-12 03:32:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.14:8443
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Commons-based peer production - Commons-based peer production is a term coined by Harvard Law School professor Yochai Benkler. It desc
2023-05-12 03:08:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.78
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 02:56:27	Hash	No	Hash Extractor	0	0	3	0	None	[MD5] 02ca825e4901e74c2c2d6f8e59341325
2023-05-12 02:55:27	BGP AS Membership	No	URLScan.io	0	0	1	0	None	13335
2023-05-12 03:18:06	Externally Hosted Javascript	No	Page Information	0	0	3	0	None	https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js
2023-05-12 03:01:00	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.100): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:30	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'SC', u'country_tld': u'.us', u'ip': u'35.229.48.116', u'currency_name': u'Dollar', u'currency': u'USD', u'country_p
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	CIEE (Net ID: 00:01:71:0A:18:17)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	PeopleMatter (Net ID: 00:18:0A:31:ED:0A)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Apple Network 1f64fd (Net ID: 00:02:2D:1F:64:FD)

2023-05-12 03:04:14	Malicious Affiliate	Yes	abuse.ch	0	1	3	0	None	abuse.ch URLhaus (Domain) [cdn-185-199-109-153.github.com] https://urlhaus.abuse.ch/downloads/csv_recent/
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	xfinitywifi (Net ID: 00:0D:67:8C:21:B2)
2023-05-12 02:45:06	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:89:fe:30:65:f6:62:86:64:4f:34:07:5e:a0:a9:be:d2:24 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: C4:B4:
2023-05-12 03:36:20	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.128:8443
2023-05-12 03:24:47	Country	No	Country Name Extractor	0	0	3	0	None	Canada
2023-05-12 02:49:07	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:74:c7:69:09:be:bf:85:53:83:95:0e:84:5e:23:6b:8f:95 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 1F:80:
2023-05-12 03:24:21	Web Content	No	Web Spider	2	0	3	0	None	<!DOCTYPE html> <html lang="en-US"> <head> <title>Just a moment...</title> <meta http-equiv="Content-Type" content="text/html; charset _DmccPSp6yXjib7zziw0VsFZ51VNwFMiyAJLSoQVd1OjGuw3fSFPRsqIT0NzkM6LJJ9oyKVkZXep7mdpjCvm52q0byqZXvzL2VDAtJAJmAXjedpHk-ixt-DqOfzQw9GqcICnOa 'FoAd4lVBdR3won9Rs2Jfak+tQjzXxPoSuo1RDbLWoBgbDtG4sbp6dJPVY2yPACeJPMILVDmGpWRL5p83JUdrP8nuVYCG+5vbYX8rd53MVZ5kJ9wlfWFmCqWwQJUw/8TZawBHI
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	GOAT (Net ID: 00:00:C5:D3:87:1C)
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:80
2023-05-12 03:09:51	Affiliate - Domain Name	No	DNS Resolver	2	0	4	0	None	keyubu.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CableWiFi (Net ID: 00:0D:67:33:68:61)
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Google Trust Services LLC,CN=GTS CA 1P5
2023-05-12 02:46:50	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/carti_2.PNG
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	PLXDevices (Net ID: 00:06:66:30:03:AC)
2023-05-12 03:02:57	Web Analytics ID	No	Web Analytics Extractor	0	0	3	0	None	Google Analytics: UA-105392568-1
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:0C:41:41:40:58)
2023-05-12 03:15:35	Web Content Language	No	Language Detector	0	0	4	0	None	English
2023-05-12 03:23:50	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.20:443
2023-05-12 03:00:51	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.79): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 03:43:29	Country	No	Country Name Extractor	0	0	4	0	None	Netherlands
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	y?maz mef. (Net ID: 00:12:BF:D2:A8:62)
2023-05-12	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	007sair.github.io

03:00:54									
2023-05-12 02:58:04	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur mutants', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 3, u'thre 00000000-00002224]\n "6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442" has type "data"- Location: [%LOCALAPPDATA%\\o [%APPDATA%\\Microsoft\\Windows\\Cookies\\DSG5QH9T.txt]- [targetUID: 00000000-00002224]\n "ce5327c52694093aede79fbdda65cf4496210956_1_. trying to touch file "C:\\Program Files\\Internet Explorer\\EN\\IEXPLORE.EXE.MUI"\n "iexplore.exe" trying to touch file "C:\\Program F
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:37:68:7b:1f:26:29:cd:a4:cc:95:52:df:e2:0a:12:6f:13 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: D9:CF: 21:21:50:dd:de:43:12:b9:29:89:20:37:79:64:39:a0:00:fa: b9:f2:d1:d6:97:d7:a4:ad:65:b2:7e:a9:68:2b:1e:77:25:f0: a5:6a:9b:71:2e:77:c5:cb:
2023-05-12 02:55:15	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive
2023-05-12 02:54:07	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	tumblr (Category: images) https://ayshoo.tumblr.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Coderwall (Category: coding) https://coderwall.com/login/
2023-05-12 03:00:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha2-512-etm@openssh.com
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.233): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	\016\025\016\005\003\005\026\004\004\004\014\016\0 (Net ID: 00:0C:30:12:EC:AE)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	FRATOAP001 (Net ID: 00:02:2D:53:7B:80)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	taxoffice (Net ID: 00:06:25:4B:60:E0)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:98:DE:00)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	cross-origin-embedder-policy: require-corp
2023-05-12 02:57:56	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'description': u'"34.148.97.127:443"'}, {u'category': u'General', u'origin': u'Binary File', u'identifier': u'binary-16', u'name': u' [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\80237EE4964FC9C409AAF55BF996A292_D46D6FA25B74360E1349F9015B5CCE53]- [targe u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level'
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	Twitter (Category: social) https://twitter.com/battleb0t
2023-05-12 02:56:48	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'"\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:4968:304:WilStaging_02"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:4968:120:WilErro [targetUID: N/A]\n "load_statistics.db-wal" has type "SQLite Write-Ahead Log version 3007000"- Location: [%LOCALAPPDATA%\\Microsoft\\E u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 2, u'description': u'Pattern match: "https://minehut.com/"\n Pattern 49741\n TCP traffic to 142.250.217.66 on port 49743\n TCP traffic to 104.18.26.85 on port 49744\n TCP traffic to 104.17.24.14 on port
2023-05-12 03:18:06	Externally Hosted Javascript	No	Page Information	0	0	3	0	None	https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	abay (Net ID: 00:08:5C:FB:81:BF)
2023-05-12 03:16:17	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	ayshu.xyz
2023-05-12 02:57:46	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "UpdatingNewTabPageData"\n "Local\\ZonesLockedCacheCounterMutex"\n "Local\\ZonesCacheCounterMutex"\n "IsoScope_dac_IESQMMUTEX_0_519"\n [%APPDATA%\\Microsoft\\Windows\\Cookies\\NJN6P46V.txt]- [targetUID: 00000000-00003448]\n Dropped file: "OOF6KCM3.txt" - Location: [%AP "background_new.fd3a8456cceb346c0891c03198a60c38_1_.webp" has type "RIFF (little-endian) data Web/P image VP8 encoding 1000x503 Scalin "Cab5348.tmp" has type "Microsoft Cabinet archive data Windows 2000/XP setup 62919 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 d
2023-05-	Web	No	Language	0	0	5	0	None	

12 03:15:35	Content Language		Detector						English
2023-05-12 03:19:17	Web Framework	No	Web Framework Identifier	0	0	3	0	None	Bootstrap
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	babepedia (Category: XXXPORNXXX) https://www.babepedia.com/user/login
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F0:17:4A)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cf-mitigated: challenge
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	trakt (Category: video) https://trakt.tv/users/login
2023-05-12 03:09:04	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.106
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	luna (Net ID: 00:02:2D:2D:B8:C7)
2023-05-12 03:00:24	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	support@lu.ma
2023-05-12 02:54:23	Open TCP Port Banner	No	Censys	0	0	4	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H061ZY9N5FV8EXSVB32WY78R Date: <REDACTED> Content-Length: 0
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	Pornhub Users (Category: XXXPORNXXX) https://www.pornhub.com/users/Battleb0t
2023-05-12 02:44:15	IPv6 Address	No	DNS Resolver	16	0	3	0	None	2606:4700:3030::ac43:a8fc
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	cross-origin-opener-policy: same-origin
2023-05-12 03:01:27	Raw Data from RIRs	No	Tool - WhatWeb	1	0	2	0	None	[{u'request_config': {u'headers': {u'User-Agent': u'Mozilla/5.0'}}, u'target': u'http://oldfluid.battleb0t.xyz', u'http_status': 301,
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Snapchat Stories (Category: social) https://story.snapchat.com/s/login
2023-05-12 02:56:27	Hash	No	Hash Extractor	0	0	3	0	None	[MD5] 02ca825e4901e74c2c2d6f8e59341325
2023-05-12 03:00:58	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	01039402468.github.io
2023-05-12 02:44:31	Internet Name	No	DNS Resolver	17	0	2	0	None	panel.battleb0t.xyz
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:2086
2023-05-12 03:03:55	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	malsup.github.io
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	StartMotor (Net ID: 00:02:CF:A1:A1:06)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	BudgetScottsdale (Net ID: 00:09:5B:29:02:37)
2023-05-	SSL	No	Certificate	1	0	1	0	None	

12 02:55:32	Certificate - Raw Data		Transparency						Certificate: Data: Version: 3 (0x2) Serial Number: 03:aa:0b:fb:f5:72:57:f7:90:57:35:0a:22:0c:3a:41:5a:d1 Signature Algorithm: sha256Wi 0a:e0:67:62:79:dd:4b:90:cc:e8:41:75:b0:89:34:3b:68:0e: 36:40:32:41:3e:6c:17:bc:5d:a4:cc:91:d3:38:4a:ce:c8:1b: ab:60:7c:08
2023-05-12 03:33:13	Web Content Language	No	Language Detector	0	0	5	0	None	English
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	\005\014\006\035\026\027\003\037\003\037\022\032\0 (Net ID: 00:06:25:0B:A9:FE)
2023-05-12 02:47:07	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: c7:83:d8:18:48:a0:26:ac:0e:41:bf:5e:7d:c6:c3:07 Signature Algorithm: sha256WithRSAE 8f:de:2d:05:92:69:48:3c:56:fc:22:08:a2:35:bd:c8:57:65: b5:6f:33:0c:aa:bc:76:e8:1d:42:77:47:bc:ae:0e:80:ed:dd: d3:8e:f7:0f:aa:49:99:2e:
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.68): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Interwrx1 (Net ID: 00:02:2D:A8:7E:D5)
2023-05-12 03:09:36	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	221.30.196.104.bc.googleusercontent.com
2023-05-12 02:44:09	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:4d:72:d7:7c:dd:a7:02:dd:5a:67:f2:a2:3b:bd:d9 Signature Algorithm: sha256WithRSAE - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1-1.crt X509v3 Basic Constraints fa:29:72:01:3e:b7:06:f1:2f:1a:0e:91:c5:ec:35:bf:f5:da: 33:95:de:24:12:0d:f5:c3:23:8d:40:82:d1:5c:eb:de:0a:08: e8:e5:83:e5:0a:8b:3a:5e:
2023-05-12 02:46:49	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	3	0	None	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
2023-05-12 02:53:45	BGP AS Membership	No	Censys	0	0	2	0	None	54113
2023-05-12 03:01:03	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.111): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:06	URL (Uses Javascript)	No	Page Information	0	0	3	0	None	http://fluid.battleb0t.xyz
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.219): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	DCO (Net ID: 00:0C:41:66:5E:C3)
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	6	0	None	Greece
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	Steam (Category: gaming) https://steamcommunity.com/id/Battleb0t
2023-05-12 03:21:08	Account on External Site	No	Account Finder	0	0	2	0	None	Chomikuj.pl (Category: misc) https://chomikuj.pl/dawidsulej/
2023-05-12 03:08:29	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 03:09:39	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	111.48.229.35.bc.googleusercontent.com
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	friday28 (Net ID: 00:06:25:BF:BB:2F)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	U+Net (Net ID: 00:02:A8:81:E3:25)
2023-05-12 03:11:16	Physical Coordinates	No	AbstractAPI	0	0	2	0	None	37.751, -97.822
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:66:AA:84)
2023-05-12 02:54:48	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H06G1PB5R3RGDWCWXWQ2TAMN Date: <REDACTED> Content-Length: 0
2023-05-12 03:19:01	WiFi Access	No	Wigle.net	0	0	3	0	None	ikizler (Net ID: 00:12:BF:32:87:51)

	Point Nearby								
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:64:DA:1A)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	logitecgameuser (Net ID: 00:01:8E:15:D4:A7)
2023-05-12 03:03:23	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:44:15	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 02:5a:61:0f:58:eb:84:f1:ad:53:ae:03:dc:a9:84:7a Signature Algorithm: ecdsa-with-SHA 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: 1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73 Timestamp : Dec 21 09:03:52.857 2022
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	vapor (Net ID: 00:02:2D:09:FB:FD)
2023-05-12 02:53:22	IPv6 Address	No	Mnemonic PassiveDNS	0	0	2	0	None	2606:4700:3030::ac43:a8fc
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:74:92:53:2C)
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://funny.battleb0t.xyz/images/random_5.png
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	studiobleu (Net ID: 00:0C:41:86:C7:5C)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	FOX (Net ID: 00:01:71:0C:5D:4A)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	referrer-policy: same-origin
2023-05-12 02:44:14	IPv6 Address	No	DNS Resolver	15	0	1	0	None	2606:50c0:8003::153
2023-05-12 02:45:48	Internet Name	No	VirusTotal	0	0	2	0	None	www.battleb0t.xyz
2023-05-12 02:53:01	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [34.148.97.127] https://www.virustotal.com/en/ip-address/34.148.97.127/information/
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Pokec (Category: social) https://pokec.azet.sk/login
2023-05-12 02:55:04	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur WIN-CORE-FIBERS-L1-1-1" at base 60c0000\n "msedge.exe" loaded module "API-MS-WIN-CORE-LOCALIZATION-L1-2-1" at base 60c0000\n "msedge.e [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Asset Store\\assets.db\\000003.log]- [targetUID: 00000000-00007516]\n "f_00024d" "UTF-8 Unicode text with very long lines with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\18782bcb-f0 Heuristic match: "https:I/briarproJ\'ect.org/"'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifier': u'string
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	rsi (Category: gaming) https://robertsspaceindustries.com/citizens/login
2023-05-12 03:17:36	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: AHU.XYZ Registry Domain ID: D196165314-CNIC Registrar WHOIS Server: whois.google.com Registrar URL: https://domains.googl presented here for any purpose other than determining ownership of domain names, (2) not to store or reproduce this data in any way, (7151571251 Tech Organization: Contact Privacy Inc. Customer 7151571251 Tech Street: 96 Mowat Ave Tech City: Toronto Tech State/Provinc
2023-05-12 02:44:22	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	referrer-policy: same-origin
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX55154FA6D (Net ID: 00:01:E3:54:FA:6D)
2023-05-12 02:56:01	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur (type is "data")\n Antivirus vendors marked dropped file "Tar17A3.tmp" as clean (type is "data")\n Antivirus vendors marked dropped fi u'Drops files inside appdata directory', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id' "~DFD224B327448F3092.TMP" has type "data"- Location: [%TEMP%\\~DFD224B327448F3092.TMP]- [targetUID: 00000000-00003664]\n "~DF2BFAF84F2 Windows 2000/XP setup 62932 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%LOCALAPPDATA%\\

2023-05-12 03:09:35	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	214.30.196.104.bc.googleusercontent.com
2023-05-12 02:46:53	Affiliate - Domain Name	No	DNS Resolver	2	0	2	0	None	cloudflare.net
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Linktree (Category: social) https://linktr.ee/ayhu
2023-05-12 02:52:59	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	None None
2023-05-12 03:01:15	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.138): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:39	Internet Name	No	DNS Resolver	0	0	2	0	None	battleb0t.xyz
2023-05-12 02:44:30	Internet Name	No	DNS Resolver	0	0	2	0	None	battleb0t.xyz
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Giphy (Category: social) https://giphy.com/channel/ayhu
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=vgB2xlauGELdj%2BVZddouVM4SLWiyGeZvDcjgyrNUJ4TCe9uwaasjv9
2023-05-12 03:11:20	Physical Location	No	AbstractAPI	0	0	3	0	None	Frankfurt am Main, Hesse, 60313, Germany, Europe
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.59): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:EC:0F:F7)
2023-05-12 02:57:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level': 0, u'type': 8, u'description': u'Antivirus vendors marked dropped file "urlblockindex_1_.bin" as clean (type is "data 11E7-B48D-080027D44A30_.dat" has type "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "RecoveryStor [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63]- [targe u'threat_level_human': u'suspicious', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 1, u'type': 7, u'descri
2023-05-12 03:03:43	Internet Name	No	DNS Resolver	0	0	4	0	None	panel.battleb0t.xyz
2023-05-12 03:01:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.249): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:08:54	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.71
2023-05-12 03:31:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	c26pf75p2tc@networksolutionsprivateregistration.com
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	alex-home (Net ID: 00:01:E3:58:87:1F)
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Picsart (Category: art) https://picsart.com/u/ayshoo
2023-05-12 02:44:18	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 03:03:55	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	ebrahemsamir.github.io

2023-05-12 03:13:03	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0001vrn.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:08:57	Vulnerability - CVE Medium	Yes	Tool - Retire.js	0	0	4	0	None	CVE-2020-11022 https://nvd.nist.gov/vuln/detail/CVE-2020-11022 Score: 6.1 Description: In jQuery versions greater than or equal to 1.2
2023-05-12 02:44:22	Internet Name	No	DNS Resolver	0	0	2	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.204): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:44:15	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	185.199.111.153:443
2023-05-12 03:09:53	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 02:53:42	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "Via": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary":
2023-05-12 02:54:12	Linked URL - Internal	No	Web Spider	4	0	1	0	None	https://battleb0t.xyz/
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:8443
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/ein_2.png
2023-05-12 03:08:49	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.112
2023-05-12 03:00:32	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	fl@e9.lb
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 02:44:09	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=*.ayhu.xyz
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	Identity Digital Inc.
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	permissions-policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope
2023-05-12 02:44:27	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi2.battleb0t.xyz
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.118): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:59:58	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	manuel.ebner@ebnerfamily.com
2023-05-12 02:45:53	Raw Data from RIRs	No	AbstractAPI	0	0	4	0	None	{u'city': u'Montreal', u'security': {u'is_vpn': False}, u'city_geoname_id': 6077243, u'region_geoname_id': 6115047, u'country': u'Unit
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Spotify (Category: music) https://open.spotify.com/user/ayhu
2023-05-12 03:00:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-128-etm@openssh.com
2023-05-12	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur

02:53:55									Traffic', u'identifier': u'network-1', u'name': u'Contacts server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u' pre-stable.json, Indicator: "leu.com")\n ""bananasmonkey.com"," (Source: wallet-pre-stable.json, Indicator: "key.com")\n ""baseballmon "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Subresource Filter\\Indexed Rules\\35\\10.34.0.32\\Ruleset Data]- [targ CRLF line terminators"- Location: [%TEMP%\\6140_1593005669\\edge_checkout_page_validator.js]- [targetUID: 00000000-00006140]\n "auto_o
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	mariposa (Net ID: 00:01:24:F1:B8:36)
2023-05-12 02:44:50	Raw Data from RIRs	No	CRXcavator	1	0	1	0	None	[{"platform": "Chrome", "version": "2.1", "data": {"entrypoints": {"window.addEventListener": {"/tmp/ppaeilehlbalfblndppebfpgikeodlaj_ "https://nvd.nist.gov/vuln/detail/CVE-2019-11358", "https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b"] directly from Google Calendar", "icon": "https://lh3.googleusercontent.com/EtDJ1WOrJu9vJxqUpk67gAWSsvf7llrIu3UIxOVFQMS6BIxdN3fKOe0NBBH "short_description": "Record screencasts - record video from your screen. Screen Capture FULL Web page or any part. Edit screenshots." "flliilndjeohchalpbbcdekjklbdgfkk": {"rating": 4.1474295, "users": 6000000, "platform": "", "short_description": "Your surfing made pr
2023-05-12 03:11:18	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'Amsterdam', u'security': {u'is_vpn': False}, u'city_geoname_id': 2759794, u'region_geoname_id': 2749879, u'country': u'Net
2023-05-12 03:00:58	Malicious Affiliate	Yes	VXVault.net	0	1	3	0	None	VXVault Malicious URL List [cdn-185-199-110-153.github.com] http://vxvault.net/URL_List.php
2023-05-12 02:52:11	Malicious IP Address	Yes	VirusTotal	0	1	3	0	None	VirusTotal [172.67.168.252] https://www.virustotal.com/en/ip-address/172.67.168.252/information/
2023-05-12 02:50:16	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Clayton2 (Net ID: 00:02:2D:0E:A8:AC)
2023-05-12 02:53:25	IP Address	No	Mnemonic PassiveDNS	0	0	2	0	None	172.67.168.252
2023-05-12 02:46:24	Netblock Membership	No	RIPE	8	0	2	0	None	185.199.109.0/24
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom6F5C74 (Net ID: 00:0C:F6:6F:5C:74)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MatrixEx BYOD (Net ID: 00:01:21:26:54:31)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:EB:D2:2C)
2023-05-12 02:49:58	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [185.199.110.153] https://www.virustotal.com/en/ip-address/185.199.110.153/information/
2023-05-12 02:54:48	Physical Location	No	Censys	1	0	3	0	None	North Charleston, South Carolina, 29405, United States, North America
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Gravatar (Category: images) http://en.gravatar.com/profiles/login
2023-05-12 02:50:23	Blacklisted IP Address	Yes	Honeypot Checker	0	1	3	0	None	Honeypotproject (172.67.168.252): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.143): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MatrixEx BYOD (Net ID: 00:01:21:26:54:21)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	themeforest (Category: art) https://themeforest.net/user/ayhu
2023-05-12 02:44:20	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Dribbble (Category: art) https://dribbble.com/login
2023-05-12 02:53:06	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	Cloudflare Inc. Cloudflare
2023-05-12 03:18:54	WiFi Access	No	Wigle.net	0	0	4	0	None	MyVolvoLpyPOa (Net ID: 00:10:02:39:B3:DE)

	Point Nearby								
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Persistent_Auth": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Host": "DISPLAY_UTF8", "Server":
2023-05-12 02:53:35	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache_Hits": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Etag": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "
2023-05-12 03:00:13	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	cpcontacts.ayhu.xyz
2023-05-12 02:54:20	Linked URL - External	No	Web Spider	0	0	3	0	None	https://support.cloudflare.com/hc/en-us/articles/200171916-Error-521
2023-05-12 03:18:06	Externally Hosted Javascript	No	Page Information	0	0	3	0	None	https://use.fontawesome.com/9dfc16ed6b.js
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:F4:A6:7E)
2023-05-12 03:00:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.12): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:13:04	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00089.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	1	0	2	0	None	007316.xyz
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Dubtronicssid (Net ID: 00:01:24:F0:BB:A4)
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 26:cc:7f:01:c6:92:25:78:13:50:9e:48:80:75:15:57 Signature Algorithm: sha256WithRSAE 09:9f:cd:b5:43:3b:6a:2f:1d:c9:3b:c0:c8:50:40:4b:85:6c: a4:67:c0:ea:9c:ed:fa:82:03:5a:15:d9:da:e2:17:9e:f5:4d: 17:b3:27:61:b6:b3:76:a2:
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	5	0	None	United States
2023-05-12 03:00:26	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abc@allianzgi.com
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Persistent_Auth": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Host": "DISPLAY_UTF8", "Server":
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	motorola 8A4 (Net ID: 00:0C:E5:4D:D8:A4)
2023-05-12 03:09:34	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	211.30.196.104.bc.googleusercontent.com
2023-05-12 02:56:51	Internet Name	No	DNS Resolver	0	0	2	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:05:5D:EC:D6:A2)
2023-05-12 03:00:36	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abusecomplaints@markmonitor.com
2023-05-12 02:54:16	HTTP Headers	No	Web Spider	6	0	2	0	None	{"nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "alt-svc": "h3=\":443\"; ma=86400, h3-29=\":443\"; ma=
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	postcrossing (Category: social) https://www.postcrossing.com/user/login
2023-05-12 02:56:50	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:09:5B:FC:D9:A0)
2023-05-	Raw Data	No	AbstractAPI	0	0	3	0	None	{u'format': {u'international': u'+14806242599', u'local': u'(480) 624-2599'}, u'country': {u'prefix': u'+1', u'code': u'US', u'name':

12 03:11:26	from RIRs								
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Picsart (Category: art) https://picsart.com/u/login
2023-05-12 02:45:34	Raw DNS Records	No	DNS Raw Records	0	0	1	0	None	battleb0t.xyz. 86400 IN NS daphne.ns.cloudflare.com. battleb0t.xyz. 86400 IN NS skip.ns.cloudflare.com.
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:03:28	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:55:18	Software Used	Yes	Censys	0	0	3	0	None	openssh
2023-05-12 02:45:50	Physical Location	No	AbstractAPI	1	0	2	0	None	Montreal, Quebec, H4X, United States, North America
2023-05-12 02:54:07	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SWKIDNEY1 (Net ID: 00:02:6F:ED:54:F8)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:F6:1A:16)
2023-05-12 02:54:44	Netblock Membership	No	Censys	0	0	3	0	None	35.229.48.0/20
2023-05-12 02:59:59	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	notatestuser@gmail.com
2023-05-12 02:46:53	Affiliate - Domain Name	No	DNS Resolver	2	0	2	0	None	cloudflare.com
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:52:33	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'info extension "png"\n "Elmah.21a45df7_1_.png" has type "PNG image data 836 x 536 8-bit/color RGBA non-interlaced" and extension "png"\n "N u'description': u'"iexplore.exe" writes file "c:\\users\\%osuser%\\appdata\\local\\microsoft\\internet explorer\\recovery\\high\\activ "app.7abc533d_1_.js" has type "UTF-8 Unicode text with very long lines"- [targetUID: N/A]\n "Editor.3586032f_1_.gif" has type "GIF ima
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.160): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:17:44	Account on External Site	No	Account Finder	0	0	1	0	None	Twitter (Category: social) https://twitter.com/ BattleB0t
2023-05-12 02:45:51	Physical Coordinates	No	AbstractAPI	0	0	2	0	None	37.751, -97.822
2023-05-12 03:24:00	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	ayhu.de
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.82): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:2082
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Microsoft acquisitions
2023-05-12 03:23:38	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.14:443
2023-05-12 03:03:34	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-	SSL	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3

12 02:44:05	Certificate - Issued by								
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Open-source software hosting facilities
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SMC (Net ID: 00:04:E2:D0:65:C0)
2023-05-12 02:54:57	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AIRTIES_RT-205 (Net ID: 00:12:BF:FE:00:5F)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	PHK140 (Net ID: 00:01:E3:06:9D:0B)
2023-05-12 03:08:48	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.226
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	eduwifi (Net ID: 00:02:2D:54:36:B1)
2023-05-12 02:56:31	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'relevance': 10, u'threat_level': 0, u'type': 8, u'description': u'"57C8EDB95DF3F0AD4EE2DC2B8CFD4157" has type "Microsoft Cabinet arc 00000000-00002464]\n "RecoveryStore._88B090C0-D917-11E7-B67B-080027A49DD6_.dat" has type "Composite Document File V2 Document Cannot r u'image_file_characteristics': [], u'submissions': [{u'url': u'https://www.rstudio.com/products/rstudio/download/),', u'submission_id'
2023-05-12 03:31:23	Malicious IP on Same Subnet	Yes	blocklist.de	0	0	4	0	None	blocklist.de List [46.101.128.0/17] http://lists.blocklist.de/lists/all.txt
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-cache-hits: 0
2023-05-12 03:00:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-64-etm@openssh.com
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	eAdisyon@ozgen (Net ID: 00:02:6F:C9:2B:E8)
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.62): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:21	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	2	0	None	C=US,ST=California,L=San Francisco,O=GitHub\, Inc.,CN=*.github.io
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cross-origin-embedder-policy: require-corp
2023-05-12 02:54:13	Linked URL - Internal	No	Web Spider	5	0	2	0	None	https://ayhu.xyz/?__cf_chl_f_tk=tLjY4MFl6PFRYsxJBRXXPqgMr4VsmLm23dP5uGlU768-1683860053-0-gaNycGzNCiU
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Apple Network 031c82 (Net ID: 00:02:2D:03:1C:82)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	sofurry (Category: art) https://login.sofurry.com
2023-05-12 02:55:15	Open TCP Port	No	Censys	0	0	3	0	None	165.232.113.85:80
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2083
2023-05-12 03:31:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	abuse@namecheap.com
2023-05-12 02:44:12	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Sectigo
2023-05-12 02:58:47	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	2	1	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco

2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Viking (Net ID: 00:01:71:0B:CD:2E)
2023-05-12 03:20:27	Account on External Site	No	Account Finder	0	0	2	0	None	Pillowfort (Category: social) https://www.pillowfort.social/patrick.pogoda
2023-05-12 03:15:39	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	0	3	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:33:56	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	mntrRGB XYZ desc trXYZ <mluc -mluc 3`-O! 6fD` N@e@8 s$01@H @jlveI B4Pic .E"E3@YB 8RktA -B09: FRp.PD A7e k `kfZb A8tSNJ 4j@Q4 H8@I" `Y@
2023-05-12 03:13:02	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:56:25	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	YouTube User2 (Category: video) https://www.youtube.com/@Altpapier
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Pragma": "DISPLAY_UTF8", "Set_Cookie": "DISPLAY_UTF8", "X_Content_Type_Options": "DISPLAY_UTF8", "Connection": "DISPLA
2023-05-12 02:47:42	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis HTTP/1.1\nAccept: text/html, application/xhtml+xml, */*\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level' None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"sahnawaz786.github.io"'}, {u'category': u [targetUID: 00000000-00003444]\n "PHD1U0AR.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\PHD1U0AR.txt
2023-05-12 02:57:33	Raw Data from RIRs	No	Certificate Transparency	8	0	1	0	None	[{u'not_after': u'2023-07-10T04:54:49', u'not_before': u'2023-04-11T04:54:50', u'issuer_ca_id': 180753, u'name_value': u'*.ayhu.xyz\na u'common_name': u'ayhu.xyz', u'serial_number': u'04897c23d88920d1c5b3ae3091443a2381b8', u'entry_timestamp': u'2022-12-14T04:53:55.433' 13T17:51:43', u'issuer_ca_id': 183267, u'name_value': u'*.ayhu.xyz\nayhu.xyz', u'issuer_name': u"C=US, O=Let's Encrypt, CN=R3", u'comm
2023-05-12 02:44:32	Affiliate - Internet Name	No	DNS Resolver	2	0	2	0	None	cdn-185-199-109-153.github.com
2023-05-12 03:03:28	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:09:47	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	72.170.74.34.bc.googleusercontent.com
2023-05-12 02:44:20	Internet Name	No	DNS Resolver	2	0	2	0	None	nwapi2.battleb0t.xyz
2023-05-12 03:31:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	abuse@support.gandi.net
2023-05-12 03:24:29	Company Name	No	Company Name Extractor	0	0	4	0	None	Netlify\, Inc
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Sprint Drive (Net ID: 00:0A:F5:55:59:00)
2023-05-12 02:44:42	Internet Name	No	DNS Resolver	0	0	2	0	None	panel.battleb0t.xyz
2023-05-12 02:56:57	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:1892:304:WilStaging_02"\n "\\Sessions\\1\\BaseNamedObjects\\SM0:1892:120:WilError_01"\n " None, u'attck_id': u'T1105', u'relevance': 3, u'threat_level': 0, u'type': 8, u'description': u'"load_statistics.db-wal" has type "SQL random domain names', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/001', u'threat_level_human': u'informative', u'cap Pattern match: "https://github.com/angular/angular.js/blob/master/src/ng/urlUtils.js"\n Pattern match: "http://www.aptana.com/referenc
2023-05-12 02:47:48	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:3724:304:WilStaging_02"'}, {u'category': u'General', u'origin': u'Network Traffic', u'ide "PGP symmetric key encrypted data -"- Location: [%TEMP%\\2964_441367473\\Part-NL]- [targetUID: 00000000-00002964]\n "Part-RU" has type

									[%TEMP%\\2964_812909146\\shopping_fre.html]- [targetUID: 00000000-00002964]\n "LOG" has type "ASCII text"- Location: [%LOCALAPPDATA%\\ [%TEMP%\\2964_812909146\\shopping_iframe_driver.js]- [targetUID: 00000000-00002964]\n Dropped file: "product_page.js" - Location: [%TE
2023-05-12 03:03:19	Internet Name	No	DNS Resolver	0	0	3	0	None	kekw.battleb0t.xyz
2023-05-12 03:24:33	Malicious Affiliate	Yes	VXVault.net	0	1	4	0	None	VXVault Malicious URL List [cdn-185-199-111-154.github.com] http://vxvault.net/URL_List.php
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	DTLAMN (Net ID: 00:01:9F:20:3C:A0)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	TOMTSSID (Net ID: 00:02:2D:21:5D:E4)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-ray: 7c5f605affff189d-EWR
2023-05-12 02:44:03	Internal SpiderFoot Root event	No	SpiderFoot UI	12	0	0	0	None	"Battleb0t","Kekwltd","Patrick Pogoda","DawixSulej","Dawid Sulej","ayshoo",battleb0t.xyz,"_BattleB0t_",ayhu.xyz
2023-05-12 02:44:15	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	1	2	0	None	netlify.app
2023-05-12 03:10:20	Malicious IP on Same Subnet	Yes	VoIPBL OpenPBX IPs	0	0	3	0	None	VOIPBL Publicly Accessible PBX List [188.114.97.0/24] http://www.voipbl.org/update
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	TheCs (Net ID: 00:09:0F:BC:AB:26)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-opener-policy: same-origin
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Beens Gast (Net ID: 00:01:21:1F:B1:91)
2023-05-12 03:23:41	Account on External Site	No	Account Finder	0	0	8	0	None	Pillowfort (Category: social) https://www.pillowfort.social/baptiste.vauthey
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+74955801111
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	iskorpit (Net ID: 00:15:D0:36:48:62)
2023-05-12 02:44:07	Internet Name	No	CertSpotter	19	0	1	0	None	fluid.battleb0t.xyz
2023-05-12 02:49:03	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_huma bit/color RGB non-interlaced"- [targetUID: N/A]\n "77EC63BDA74BD0D0E0426DC8F8008506" has type "data"- [targetUID: N/A]\n "68e6dbb3-f4d "https://cytoscape.org"\n Pattern match: "https://creativecommons.org/compatiblelicenses"\n Heuristic match: "syndication.twitter.com" None, u'attck_id': u'T1105', u'relevance': 3, u'threat_level': 1, u'type': 8, u'description': u'"adblock_snippet.js" has type "Unknown
2023-05-12 02:49:38	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relevance': 3, u'threat_level': 0, u'type': 8, u'description': u'"000003.l "e3d08ea3-f64e-454e-b7c9-a3743c49cc7d.tmp" has type "UTF-8 Unicode text with very long lines with no line terminators"- Location: [%LO u'File/Memory', u'identifier': u'string-14', u'name': u'Found potential IP address in binary/memory', u'attck_id_wiki': None, u'threat
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:74:AA:8C:9E)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-github-request-id: 69FA:0168:26C3619:3A6662D:645DAA55
2023-05-12 02:54:12	HTTP Status Code	No	Web Spider	0	0	1	0	None	200
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CoxWiFi (Net ID: 00:0D:67:8C:21:AC)
2023-05-	Linked URL	No	Web Spider	5	0	3	0	None	

12 02:54:22	- Internal								https://www.ayhu.xyz/?__cf_chl_f_tk=JtV8r0GkxGajl1GKjCT6mPEPAroD8NWzOwVMv5NMEkM-1683860062-0-gaNycGzNCiU
2023-05-12 02:55:24	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis "Local\\URLBLOCK_FILEMAPSWITCH_MUTEX_2428"\n "IsoScope_97c_IESQMMUTEX_0_519"\n "Local\\ZonesLockedCacheCounterMutex"\n "Local\\URLBLOC u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_level_ [%APPDATA%\\Microsoft\\Windows\\Cookies\\6VGQERV2.txt]- [targetUID: 00000000-00002428]\n "hero2.2_1_.png" has type "PNG image data 175 /pagead/id?slf_rd=1 HTTP/1.1\nAccept: */*\nReferer: https://www.youtube.com/embed/YVgfHZMFFFQ\nAccept-Language: en-US\nOrigin: https:/
2023-05-12 02:57:23	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	portainer.battleb0t.xyz
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:74:94:30:70)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	PHK140 (Net ID: 00:01:E3:04:F3:9A)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_phone (Net ID: 00:0C:E6:C9:2D:E3)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BeensGroep (Net ID: 00:01:21:1C:17:A0)
2023-05-12 03:32:00	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.1:443
2023-05-12 02:54:20	Raw Data from RIRs	No	Censys	0	0	4	0	None	{"last_updated_at": "2023-05-12T00:39:56.858Z", "ip": "2600:1f18:2489:8200::c8", "location_updated_at": "2023-05-10T21:06:43.663615Z", "2023-03-02T14:27:26.178750795Z"}, "www.oehu.org": {"record_type": "CNAME", "resolved_at": "2023-05-08T21:49:53.230466821Z"}, "amazing "resolved_at": "2023-04-28T21:01:16.210611227Z"}, "www.dealersaver.com.au": {"record_type": "CNAME", "resolved_at": "2023-05-05T12:20: 22T17:15:07.185464982Z"}, "ctrlup-signature.netlify.app": {"record_type": "AAAA", "resolved_at": "2023-03-19T21:38:22.288735403Z"}, "o 11T12:07:42.998596444Z"}, "cupomonline.netlify.app": {"record_type": "AAAA", "resolved_at": "2023-03-09T12:06:38.920516396Z"}, "awu4jx
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	3	0	None	36459
2023-05-12 03:11:16	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'London', u'security': {u'is_vpn': False}, u'city_geoname_id': 2643743, u'region_geoname_id': 6269131, u'country': u'United
2023-05-12 02:54:30	Open TCP Port	No	Censys	0	0	3	0	None	64.226.81.43:22
2023-05-12 02:54:13	HTTP Headers	No	Web Spider	10	0	1	0	None	{"content-encoding": "gzip", "nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "referrer-policy": "same-o
2023-05-12 02:54:38	Raw Data from RIRs	No	Censys	0	0	3	0	None	{"last_updated_at": "2023-05-11T22:46:19.213Z", "ip": "172.67.168.252", "location_updated_at": "2023-05-11T18:33:28.301878Z", "autonom "resolved_at": "2023-03-24T07:24:26.513019486Z"}, "rigophogisvito.tk": {"record_type": "A", "resolved_at": "2023-04-22T20:38:42.905568 03T21:28:23.180761483Z"}, "nnfejv-dkfe.valentiona890.workers.dev": {"record_type": "A", "resolved_at": "2023-04-14T21:16:09.910917494Z {"record_type": "A", "resolved_at": "2023-05-09T21:26:23.147927370Z"}, "aqonecsymtuite.cf": {"record_type": "A", "resolved_at": "2023- "resolved_at": "2023-04-13T18:07:05.732544519Z"}, "lenscarspock.tk": {"record_type": "A", "resolved_at": "2023-05-11T21:41:33.88175689
2023-05-12 02:56:41	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/001', u'threat_level_human': u'informative', u'capec_id': None, u'attck_ HTTP/1.1\nAccept: text/css, */*\nReferer: https://www.uco.es/investiga/grupos/FQM346/?post%2CnjOkEHgROA4\nAccept-Language: en-US\nUser Gecko\nOrigin: https://www.uco.es\nAccept-Encoding: gzip, deflate\nHost: use.fontawesome.com\nDNT: 1\nConnection: Keep-Alive" (Indicat "mozilla/5.0 (")\n "GET /center.js HTTP/1.1\nAccept: application/javascript, */*;q=0.8\nReferer: https://www.uco.es/investiga/grupos/F
2023-05-12 02:54:19	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://fluid.battleb0t.xyz/gp_badge.png
2023-05-12 02:51:15	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'th 00003076]\n "~DFFC90A9F2586EA360.TMP" has type "data"- Location: [%TEMP%\\~DFFC90A9F2586EA360.TMP]- [targetUID: 00000000-00003076]\n " "search_1_.json" has type "JSON data"- [targetUID: N/A]\n "EAMNLP61.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windo u'Found potential URL in binary/memory', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'info
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-ray: 7c5f605ceb464381-EWR
2023-05-12 02:55:56	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:78:81:e1:ef:49:4b:f9:6d:c5:16:34:0e:55:ab:d5:12:44 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 75:02: 2e:6d:c1:ec:f4:03:98:d8:dd:ea:da:88:14:c5:af:7a:46:c1: 65:1f:db:ea:14:67:fb:45:d8:16:12:e2:c1:56:a5:f6:63:45: 0e:7f:b7:be:8a:a0:59:b7:
2023-05-12 03:08:54	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.73
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	MCName (Minecraft) (Category: gaming) https://mcname.info/en/search?q=Battleb0t

2023-05-12 03:00:00	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	madler@alumni.caltech.edu
2023-05-12 03:00:26	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	aes256-gcm@openssh.com
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Eminent (Net ID: 00:14:5C:87:88:F8)
2023-05-12 03:00:56	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.91): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:12:53	Raw Data from RIRs	No	numverify	0	0	3	0	None	{u'international_format': u'+14806242505', u'local_format': u'4806242505', u'number': u'14806242505', u'valid': True, u'line_type': u'
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	tsunami (Net ID: 00:0D:29:AC:D8:F1)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	UTAAPC (Net ID: 00:02:6F:3C:D0:53)
2023-05-12 02:53:39	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Gravatar (Category: images) http://en.gravatar.com/profiles/ayshoo
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00why00.github.io
2023-05-12 02:54:22	Web Content	No	Web Spider	1	0	2	0	None	<!DOCTYPE html> <html> <iframe src="https://cloudways-static-content.s3.us-east-1.amazonaws.com/error_page/maintenance-domain-mapping.
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	linksys_SES_39246 (Net ID: 00:1C:10:3F:F6:58)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	101 (Net ID: 00:01:03:79:1F:E4)
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.145): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:23	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	2	0	None	C=US,ST=California,L=San Francisco,O=GitHub\, Inc.,CN=*.github.io
2023-05-12 03:08:49	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.111
2023-05-12 03:03:41	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:00:54	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.85): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	ELSA (Net ID: 00:02:2D:20:CF:48)
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Pornhub Users (Category: XXXPORNXXX) https://www.pornhub.com/users/ayshoo
2023-05-12 02:54:15	Linked URL - External	No	Web Spider	0	0	3	0	None	https://cdn.discordapp.com/avatars/710143953533403226/02ca825e4901e74c2c2d6f8e59341325.png?size=512
2023-05-12 02:45:57	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [172.67.135.9]
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:21

2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.119
2023-05-12 02:56:58	Raw Data from RIRs	No	Hybrid Analysis	1	0	3	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis marked as clean', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1 Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\RXDGIQPF.txt]- [targetUID: 00000000-00003844]\n Dropped file: "MA7ZTF7R.txt" - Loca [targetUID: N/A]\n "dberr.txt" has type "ASCII text with CRLF line terminators"- Location: [%WINDIR%\\System32\\catroot2\\dberr.txt]- u'suspicious', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 1, u'type': 12, u'description': u'3/90 reputat
2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	104.21.71.14
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:03:B5:60)
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:2053
2023-05-12 02:54:15	HTTP Status Code	No	Web Spider	0	0	2	0	None	200
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	prv.pl (Category: tech) https://www.prv.pl/osoba/login
2023-05-12 02:45:42	Physical Location	No	AbstractAPI	0	0	2	0	None	San Francisco (South Beach), California, 94107, United States, North America
2023-05-12 02:50:19	Physical Location	No	ipstack	0	0	3	0	None	United States
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.95): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:07	Internet Name	No	CertSpotter	25	0	1	0	None	nwapi.battleb0t.xyz
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	0263d4 (Net ID: 0C:EA:C9:05:4C:A3)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	MCName (Minecraft) (Category: gaming) https://mcname.info/en/search?q=login
2023-05-12 03:00:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.32): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	factory (Net ID: 00:01:03:7C:37:39)
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	006blog.github.io
2023-05-12 02:54:22	HTTP Status Code	No	Web Spider	0	2	2	0	None	404
2023-05-12 03:09:41	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	121.48.229.35.bc.googleusercontent.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Duolingo (Category: hobby) https://www.duolingo.com/profile/login
2023-05-12 02:54:21	Linked URL - External	No	Web Spider	0	0	4	0	None	https://www.cloudflare.com/5xx-error-landing?utm_source=errorcode_521&utm_campaign=vscode.battleb0t.xyz
2023-05-12 02:59:47	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	abuse@reg.ru
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BBHWIRELESS (Net ID: 00:00:C5:D7:5E:30)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=6ZH4%2BS7iwGiB1Wu7l%2FAB03y2sKXJwRGFC2pyd%2BZjS4ZmLlnY7X
2023-05-12	Blacklisted IP on Same	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.27): Search Engine Last Activity: 0 days ago Threat Level: 29

03:01:28	Subnet								
2023-05-12 03:01:17	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.143): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless (Net ID: 00:02:2D:45:26:C8)
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.236): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:10	Physical Location	No	Censys	0	0	2	0	None	Rosemont, Illinois, 60018, United States, North America
2023-05-12 03:24:47	Country	No	Country Name Extractor	0	0	5	0	None	United States
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CoxWiFi (Net ID: 00:0D:67:8C:21:B4)
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	0	0	1	0	None	CN=battleb0t.xyz
2023-05-12 03:09:26	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	2	0	None	C=US,ST=California,L=San Francisco,O=Cloudflare\, Inc.,CN=sni.cloudflaressl.com
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	omlet (Category: gaming) https://omlet.gg/profile/battleb0t
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet9102 (Net ID: 00:01:36:5B:91:00)
2023-05-12 02:54:57	Open TCP Port	No	Censys	0	0	2	0	None	2a06:98c1:3120::1:443
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	gjdsdnetwork (Net ID: 00:06:25:98:D4:36)
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Cloud computing providers
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	The Batcave (Net ID: 00:11:32:A4:B5:6B)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	2WIRE169 (Net ID: 00:02:2D:8C:55:BE)
2023-05-12 02:56:27	Hash	No	Hash Extractor	0	0	3	0	None	[MD5] 02ca825e4901e74c2c2d6f8e59341325
2023-05-12 03:09:28	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	3	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:31:07:b9:c0:d0:b8:aa:df:7a:22:9b:22:71:4b:8d:b2:1d Signature Algorithm: sha256Wi 11:75:73:CD:59:65:4E:B8:A9:07:AD:BD:CE:FC:B0:17: 86:D5:66:27:0E:02:20:00:F2:8C:15:A7:57:91:B4:F0: F3:2E:D7:3B:10:54:C8:3E:A6:21:BD:EC:
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	tsunami (Net ID: 00:0D:29:AC:D7:34)
2023-05-12 02:45:49	Physical Coordinates	No	AbstractAPI	0	0	2	0	None	37.751, -97.822
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	LiteSpeed Technologies LiteSpeed Web Server
2023-05-12 02:54:27	Raw Data from RIRs	No	Censys	0	0	4	0	None	{"last_updated_at": "2023-05-11T14:03:34.697Z", "ip": "2600:1f18:2489:8202::c8", "location_updated_at": "2023-05-09T14:45:17.341917Z", 16T00:14:18.592192599Z"}, "develop--admin.glimmerdao.io": {"record_type": "CNAME", "resolved_at": "2023-03-13T00:50:21.694680586Z"}, " "flamboyant-dijkstra-08355c.netlify.app": {"record_type": "AAAA", "resolved_at": "2023-02-22T12:08:18.752220145Z"}, "fervent-nobel-9e2 15T12:14:05.802464120Z"}, "eduardocesb.com.br": {"record_type": "AAAA", "resolved_at": "2023-04-12T22:02:15.081895995Z"}, "maps.worldd {"record_type": "CNAME", "resolved_at": "2023-05-05T12:13:54.357770256Z"}, "launch-highlight-games-bet.netlify.app": {"record_type": "
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	0	0	2	0	None	https://nwapi.battleb0t.xyz/
2023-05-12 02:53:15	IP Address	No	Mnemonic PassiveDNS	0	0	1	0	None	104.21.71.14
2023-05-12	Malicious Co-Hosted	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0047ol.github.io] https://www.openphish.com/feed.txt

03:13:05	Site								
2023-05-12 03:12:14	Affiliate - Domain Whois	No	Whois	4	0	6	0	None	Domain Name: CLIENTIFY.NET Registry Domain ID: 1866957767_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: htt Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the t Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.48062425 otherwise support the dissemination or collection of this data, in part or in its entirety, for any purpose, such as transmission by e
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:97:99:5c:60:ac:40:68:f8:b2:de:0a:67:7a:da:b7:d1:16 Signature Algorithm: sha256Wi Extensions: none Signature : ecdsa-with-SHA256 30:44:02:20:28:F1:70:B2:E6:F5:A1:9C:C3:2A:B9:98: B7:CA:DE:46:06:8A:0D:FD:5D:51:62:6A:9E
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Venmo (Category: finance) https://account.venmo.com/u/login
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Airwolf (Net ID: 00:13:46:15:C7:AA)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet (Net ID: 00:01:36:26:BA:44)
2023-05-12 03:00:56	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.87): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:21	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 02:45:35	Affiliate - Internet Name	No	DNS Raw Records	1	0	2	0	None	battleb0t.github.io
2023-05-12 03:01:18	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.161): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	3	0	None	GitHub\, Inc.
2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.126
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	draadjelos54 (Net ID: 00:01:E3:04:A3:37)
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	Pronouns.Page (Category: social) https://pronouns.page/api/profile/get/Battleb0t?version=2
2023-05-12 02:54:30	Software Used	Yes	Censys	0	0	3	0	None	openssh
2023-05-12 02:54:00	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:23:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.12:80
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: <REDACTED> Cache-Control: no-cache, no-store, must-re
2023-05-12 02:46:25	Netblock Membership	No	RIPE	2	0	2	0	None	104.21.0.0/20
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.48): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:07:57	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 02:44:47	Software Used	Yes	Tool - Wappalyzer	0	0	3	0	None	Cloudflare
2023-05-12 02:54:30	Software Used	Yes	Censys	0	0	3	0	None	Debian Linux 10.2
2023-05-12 02:45:56	Physical Location	No	AbstractAPI	0	0	4	0	None	Ashburn, Virginia, 20149, United States, North America

2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless (Net ID: 00:01:36:0F:6E:91)
2023-05-12 03:00:23	Blacklisted IP Address	Yes	Honeypot Checker	0	1	2	0	None	Honeypotproject (188.114.96.1): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	adm734qwe (Net ID: 00:0D:3A:2C:01:71)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpeedStream (Net ID: 00:01:24:F0:B4:05)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SpeedStream (Net ID: 00:01:24:F0:DA:C3)
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	5	0	2	0	None	+14805058800
2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	TrackmaniaLadder (Category: gaming) https://en.tm-ladder.com/Altpapier_rech.php
2023-05-12 02:57:29	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	{u'count': 21, u'search_terms': [{u'id': u'host', u'value': u'34.148.97.127'}], u'result': [{u'environment_id': 160, u'job_id': u'63b7 u'2022-11-27 01:04:54', u'vx_family': None, u'av_detect': u'0', u'environment_description': u'Windows 10 64 bit', u'threat_score': Non u'analysis_start_time': u'2022-10-20 18:20:42', u'vx_family': None, u'av_detect': u'0', u'environment_description': u'Windows 10 64 bi u'6316da7ad2e049613328acc3', u'analysis_start_time': u'2022-09-06 05:28:27', u'vx_family': None, u'av_detect': u'0', u'environment_des {u'environment_id': 100, u'job_id': u'62fb370d6a44fc65fb5a8ce2', u'analysis_start_time': u'2022-08-16 06:19:58', u'vx_family': None, u
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-cache-status: DYNAMIC
2023-05-12 02:54:54	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Stuhr-WiFi-NA (Net ID: 00:14:D1:AF:C9:6C)
2023-05-12 02:49:11	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relev {d=a.document.getElementsByTagName("script");e=a.navigator&&a.navigator.userAgent||"";e=RegExp("appbankapppuzdradb|daumapps|fban|fbios at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"\n "Cab23C6.tmp" has type "Microsoft Cabinet archive data Windows 2000 "SGRF2RQT.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\SGRF2RQT.txt]- [targetUID: 00000000-00003444]
2023-05-12 03:03:47	Co-Hosted Site	No	ThreatMiner	2	0	2	0	None	etherum-libs.github.io
2023-05-12 02:44:22	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 02:54:18	HTTP Status Code	No	Web Spider	0	0	2	0	None	200
2023-05-12 03:09:39	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	113.48.229.35.bc.googleusercontent.com
2023-05-12 03:11:23	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'format': {u'international': u'+74955801111', u'local': u'8 (495) 580-11-11'}, u'country': {u'prefix': u'+7', u'code': u'RU', u'name
2023-05-12 03:00:25	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-128-etm@openssh.com
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	Snapchat Stories (Category: social) https://story.snapchat.com/s/Battleb0t
2023-05-12 02:54:30	Open TCP Port Banner	No	Censys	0	1	3	0	None	SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.108): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:33	Co-Hosted Site -	No	DNS Resolver	0	0	3	0	None	github.io

	Domain Name								
2023-05-12 02:52:38	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'description': u'"104.21.21.85:443"\n "156.146.53.13:443"\n "142.250.191.74:443"\n "104.17.25.14:443"\n "185.199.108.153:443"\n "151. dropped file "urlblockindex_1_.bin" as clean (type is "data")'}, {u'category': u'Installation/Persistence', u'origin': u'API Call', u' [targetUID: N/A]\n "seaport_1_.js" has type "data"- [targetUID: N/A]\n "modal~app.4224e3d5_1_.js" has type "ASCII text with very long "~DFE8D9E98C1276228A.TMP" has type "data"- Location: [%TEMP%\\~DFE8D9E98C1276228A.TMP]- [targetUID: 00000000-00002760]\n "~DF6F78936BB
2023-05-12 03:03:32	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	bux180 (Net ID: 00:07:7D:16:27:67)
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.3): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	referrer-policy: same-origin
2023-05-12 02:45:46	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'Chantilly', u'security': {u'is_vpn': False}, u'city_geoname_id': 4751935, u'region_geoname_id': 6254928, u'country': u'Uni
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 03:03:22	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:08:45	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.214
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	myLGNet (Net ID: 00:01:36:26:95:98)
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.184): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:22	Linked URL - Internal	No	Web Spider	2	0	2	0	None	https://www.ayhu.xyz/
2023-05-12 02:54:22	Web Content Type	No	Web Spider	0	0	2	0	None	text/html
2023-05-12 03:08:48	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.229
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	+OK Dovecot ready.
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	PM Guest (Net ID: 00:1C:10:F9:53:B8)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Gravatar (Category: images) http://en.gravatar.com/profiles/ayhu
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLG86 (Net ID: 00:01:36:37:73:C0)
2023-05-12 02:46:28	Raw Data from RIRs	No	Hybrid Analysis	3	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "142.250.189.234:443"\n "184.27.80.18:443"\n "52.155.62.95:443"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifi awesome_1_.css" has type "troff or preprocessor input ASCII text with very long lines"- [targetUID: N/A]\n "search_2_.json" has type " 00002768]'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifier': u'string-3', u'name': u'Found potential URL i "http://www.w3.org/TR/2003/WD-DOM-Level-3-Events-20030331/ecma-script-binding.html"\n Pattern match: "http://www.w3.org/TR/2011/REC-cs
2023-05-12 02:59:44	Co-Hosted Site - Domain Whois	No	Whois	3	0	3	0	None	Domain Name: CLOUDWAYSAPPS.COM Registry Domain ID: 1695307151_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar UR commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processe Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Ad
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BurkonAlt (Net ID: 00:18:4D:35:AF:23)

2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	cpcalendars.ayhu.xyz
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	GoDaddy.com, LLC
2023-05-12 03:00:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.17): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:31	Internet Name	No	DNS Resolver	19	0	2	0	None	vscode.battleb0t.xyz
2023-05-12 03:03:35	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:74:79:C8:F8)
2023-05-12 02:54:20	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 67:78:0f:c0:b3:05:0b:42:0e:1c:78:58:8a:88:56:0d Signature Algorithm: sha256WithRSAE 33:ae:dc:a9:41:b2:ff:76:d8:16:a0:d6:b1:5d:1b:db:3c:51: 93:a6:fd:af:36:c1:59:1e:4b:0d:e6:0a:68:f5:5b:67:34:d6: 7c:a2:8f:90:10:2f:aa:b0:
2023-05-12 03:01:49	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.110.153:443
2023-05-12 02:56:54	IPv6 Address	No	DNS Resolver	0	0	2	0	None	2606:4700:3031::6815:6a6
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	1001mem (Category: social) http://1001mem.ru/login
2023-05-12 02:59:49	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	bradsdevemail@gmail.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	FriendFinder-X (Category: dating) https://www.friendfinder-x.com/profile/login
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	default (Net ID: 00:08:5C:63:7B:B5)
2023-05-12 02:50:19	Physical Location	No	ipstack	0	0	3	0	None	United States
2023-05-12 02:46:33	Netblock Membership	No	RIPE	1	0	3	0	None	104.196.16.0/20
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Marshside Village (Net ID: 00:0F:CC:E2:DF:E8)
2023-05-12 02:55:15	Open TCP Port	No	Censys	0	0	3	0	None	165.232.113.85:22
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.187): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:37	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	677814ebbbc94b77b8833f353c860afe.protect@withheldforprivacy.com
2023-05-12 02:52:59	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	Cloudflare Inc. Cloudflare
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:75:F1:53)
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2095
2023-05-12 03:09:08	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	165.232.113.92

2023-05-12 02:44:15	SSL Certificate Host Mismatch	Yes	SSL Certificate Analyzer	0	0	2	0	None	*.netlify.app, netlify.app
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2087
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:5D:6A:5B)
2023-05-12 03:09:37	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	227.30.196.104.bc.googleusercontent.com
2023-05-12 02:44:19	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2600:1f18:2489:8200::c8
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:60:35:51)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	krillnet (Net ID: 00:01:8E:15:D4:A6)
2023-05-12 02:47:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "204.141.43.48:443"\n "142.250.72.214:443"\n "142.251.214.129:443"'}, {u'category': u'General', u'origin': u'Network Traffic', u'ident u'Binary File', u'identifier': u'binary-5', u'name': u'Drops cabinet archive files', u'attck_id_wiki': None, u'threat_level_human': u' [targetUID: N/A]\n "5fb4d2c611b6f7021b7a90b6_nav-healthcare_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUID: N/A]\n Alive" (Indicator: "twitter")\n "GET /s/player/7862ca1f/fetch-polyfill.vflset/fetch-polyfill.js HTTP/1.1\nAccept: application/javascri
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	gamecocks (Net ID: 00:12:17:02:13:1F)
2023-05-12 03:11:27	Physical Location	No	AbstractAPI	0	0	3	0	None	Arizona, United States
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	700 (Net ID: 00:00:85:2B:6E:C9)
2023-05-12 02:45:06	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'CA', u'country_tld': u'.us', u'ip': u'2606:50c0:8003::153', u'currency_name': u'Dollar', u'currency': u'USD', u'cou
2023-05-12 03:09:28	Co-Hosted Site	No	SSL Certificate Analyzer	1	0	3	0	None	donation.ecash-pay.com
2023-05-12 02:48:23	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "%WINDIR%\\System32\\ntmarta.dll" at 71EF0000\n "msedge.exe" loaded module "%WINDIR%\\System32\\ucrtbase.dll" at 72E80000\n "msedge.ex "msedge.exe" loaded module "%WINDIR%\\System32\\twinapi.appcore.dll" at 716C0000\n "msedge.exe" loaded module "%WINDIR%\\System32\\rmc controls_6595b64144ccf1df_6.0.16299.248_none_15ced204935f55d7\\comctl32.dll" at 632C0000\n "msedge.exe" loaded module "%WINDIR%\\Syste loaded module "%WINDIR%\\System32\\propsys.dll" at 6D2C0000\n "msedge.exe" loaded module "%WINDIR%\\System32\\DataExchange.dll" at 5E6
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:443
2023-05-12 03:00:56	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.90): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:2096
2023-05-12 02:54:22	Web Content	No	Web Spider	3	0	2	0	None	<!DOCTYPE html> <html lang="en-US"> <head> <title>Just a moment...</title> <meta http-equiv="Content-Type" content="text/html; charset rMcf1K_RyJAW0Q63e569MyoALgsa5LuF6A9Fao0NuRtVokTtKXFjE683wyQoxz2rVadCdcz1SAkPujj4gsPBtzmyTzaZ0eAhZEu4ZktRZ3yW_kCzFaoZlWWXPLmMSYOISs0fLm 'TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgMTAuMDsgV2luNjQ7IHg2NDsgcnY6NjIuMCkgR2Vja28vMjAxMDAxMDEgRmlyZWZveC82Mi4w', rm: 'R0VU', d: 'TOYbkC9rgC [0].appendChild(cpo); }()); </script> </body> </html>
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=B2wOcEimTwCYfDusQJnMA%2FeK3vnM4eWqJiKh4VAlhBD7SojZQVBe5%
2023-05-12 03:03:21	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.229): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	joe2-suddenlink_sucks (Net ID: 58:19:F8:9D:C6:A0)

2023-05-12 03:01:20	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.184): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:03	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"htmlprev 0800272B9531_.dat" has type "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "htmlpreview_1_.js" has Found http requests in header "GET /?"'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifier': u'string-3', u'n "SUIDMmicrosoft.com/9216256238860831025177145958099031025060*MUID3057AB3DCDCB69982AA2B9D7CC4F6801microsoft.com/10252694877824311035311
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	yigitcan (Net ID: 00:13:49:EC:E1:85)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomE65548 (Net ID: 00:0C:F6:E6:55:48)
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	6	0	None	Austria
2023-05-12 03:09:13	Vulnerability - General	Yes	Tool - Retire.js	0	0	4	0	None	CVE-2018-14041 Score: Unknown Description: Unknown
2023-05-12 03:15:09	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: battleb0t.wtf Registry Domain ID: 210affc107bd4562ba433c931d79c2d0-DONUTS Registrar WHOIS Server: whois.namecheap.com Reg FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTE further queries for a period of time to prevent disruption of Whois service access. Abuse of the Whois system through data mining is m Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registr
2023-05-12 02:45:57	Physical Coordinates	No	AbstractAPI	0	0	4	0	None	39.0469, -77.4903
2023-05-12 02:44:29	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	2	0	None	github.com
2023-05-12 03:24:29	Company Name	No	Company Name Extractor	0	0	4	0	None	Netlify\, Inc
2023-05-12 02:54:35	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'th Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Extension Scripts\\000003.log]- [targetUID: 00000000-00007548]\n "toke data max compression original size modulo 2^32 56403"- [targetUID: N/A]\n "shopping.js" has type "UTF-8 Unicode text with very long li "https://easylist.to/"\n Pattern match: "https://github.com/easylist"\n Pattern match: "https://llink.to/?u=https%3A%2F%2Frabetsanatko
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Content_Type": "DISPLAY_UTF8", "Set_Cookie": "DISPLAY_UTF8", "X_Content_Type_Options": "DISPLAY_UTF8", "Connection": "
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	5	0	None	China
2023-05-12 02:46:24	Malicious IP Address	Yes	MetaDefender	0	1	3	0	None	webroot.com [104.196.30.220]
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	CA-IL (Net ID: 00:00:C5:FA:44:D4)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:85:9E:97:C1)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	GWS (Net ID: 00:06:25:A0:D7:AA)
2023-05-12 02:46:18	Affiliate Description - Abstract	No	DuckDuckGo	0	0	2	0	None	Cloudflare, Inc. is an American company that provides content delivery network services, cloud cybersecurity, DDoS mitigation, and ICA
2023-05-12 02:54:44	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:62:27:a6:dc:16:28:de:ae:a0:a4:7d:7e:a0:02:81:25:0e Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 1A:29:
2023-05-12 03:13:01	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-th.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.42): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.93): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12	Account on External Site	No	Account Finder	0	0	6	0	None	Internet Archive Account (Category: misc) https://archive.org/details/@login

03:19:09									
2023-05-12 02:46:00	Physical Coordinates	No	AbstractAPI	0	0	3	0	None	37.751, -97.822
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0000magda0000.github.io
2023-05-12 03:12:12	Co-Hosted Site - Domain Whois	No	Whois	3	0	4	0	None	Domain Name: RATHOOK.CC Registry Domain ID: 163793658_DOMAIN_CC-VRSN Registrar WHOIS Server: whois.porkbun.com Registrar URL: http://p the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high Admin Fax: Admin Fax Ext: Admin Email: d3fc0n6@protonmail.com Registry Tech ID: Tech Name: d3f c0n6 Tech Organization: Boat Rolling In
2023-05-12 03:16:21	Physical Location	No	ipapi.co	0	0	2	0	None	London, England, ENG, United Kingdom, GB
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomAE9EF4 (Net ID: 00:0C:F6:AE:9E:F4)
2023-05-12 03:19:24	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.109.154:80
2023-05-12 02:47:42	Open TCP Port	No	Pulsedive	0	0	3	0	None	35.229.48.116:443
2023-05-12 02:52:01	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'Contacts domains', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relev "HTML document ASCII text"- [targetUID: N/A]\n "urchin_1_.js" has type "C source ASCII text"- [targetUID: N/A]\n "shCore_1_.js" has ty "shBrushXml_1_.js" has type "exported SGML document ASCII text"- [targetUID: N/A]\n "testng_1_.css" has type "ASCII text"- [targetUID:
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	2	0	None	(c) CentralNic Ltd
2023-05-12 02:44:44	Software Used	Yes	Tool - Wappalyzer	0	0	3	0	None	HTTP/3
2023-05-12 03:36:14	Blacklisted IP on Same Subnet	Yes	DroneBL	0	0	4	0	None	dronebl.org - HTTP Proxy (45.131.109.106)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Heisenberg (Net ID: 00:0C:F6:D0:27:08)
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:8880
2023-05-12 02:55:22	Raw Data from RIRs	No	Google	0	0	1	0	None	{'webSearchUrl': u'https://www.google.com/search?q=site:ayhu.xyz&aq=t&oe=utf-8&client=firefox-a&ie=utf-8&rls=org.mozilla%3Aen-US%3Aoff
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pfa (Net ID: 00:02:6F:C4:70:30)
2023-05-12 03:09:51	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	PACSStemp (Net ID: 00:0F:66:D6:82:2B)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Mistrzowie (Category: images) https://mistrzowie.org/user/login
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	InkBunny (Category: XXXPORNXXX) https://inkbunny.net/login
2023-05-12 03:13:01	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-range.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:13:09	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [01010101coder.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:23:44	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.17:443
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:80
2023-05-12	WiFi Access	No	Wigle.net	0	0	3	0	None	XTN-25BD34 (Net ID: 70:F8:E7:25:BD:34)

03:18:51	Point Nearby								
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Guest (Net ID: 00:01:21:30:AF:A1)
2023-05-12 03:23:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.6:443
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpaceStation (Net ID: 00:02:2D:01:CF:F8)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MatrixEx Guest (Net ID: 00:01:21:26:42:60)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet8682 (Net ID: 00:01:36:5B:86:80)
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:74:c7:69:09:be:bf:85:53:83:95:0e:84:5e:23:6b:8f:95 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 1F:80: d8:d8:3b:7d:a5:0b:bf:d3:08:d9:73:26:67:23:22:51:a7:9a: 35:1e:3d:5b:8d:37:8d:5a:13:a6:11:a6:6e:3f:57:92:c4:df: b9:a6:2d:3e:a3:ac:33:74:
2023-05-12 02:56:55	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	files.battleb0t.xyz
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 02:59:57	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	mery.robinson@ftb.ca.gov
2023-05-12 03:03:38	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:44:38	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Google Analytics
2023-05-12 02:53:52	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Etag": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary"
2023-05-12 03:09:44	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	126.97.148.34.bc.googleusercontent.com
2023-05-12 02:53:03	Raw Data from RIRs	No	Tool - WAFW00F	1	0	2	0	None	[{"url": "https://pics.battleb0t.xyz", "firewall": "None", "detected": false, "manufacturer": "None"}]
2023-05-12 02:55:46	Linked URL - Internal	No	Hybrid Analysis	0	0	3	0	None	http://kekw.battleb0t.xyz/jar
2023-05-12 02:59:56	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	korea@netflix.com
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	default (Net ID: 00:01:24:F1:84:FA)
2023-05-12 03:33:59	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	IDATx _Z19l ?_ILPJ C $/@ 0\Mjf! /VppGp ChPwap fzcoAC P6s>W 4q:P? _6Wp@ T'V51 >Lv t0 qDXT<?95 @pjrR _ij>g rd-2mp :!xn2@ V4vbR isgWO fRO
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ATTFiQVKTA (Net ID: E8:33:81:CE:14:60)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Moneysavingexpert (Category: finance) https://forums.moneysavingexpert.com/profile/ayhu
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cross-origin-opener-policy: same-origin
2023-05-12 03:32:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.9:8443

2023-05-12 03:03:55	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	rathook.cc
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	referrer-policy: strict-origin-when-cross-origin
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:2078
2023-05-12 02:45:47	Physical Location	No	AbstractAPI	0	0	2	0	None	Chantilly, Virginia, 20151, United States, North America
2023-05-12 03:03:26	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:11:13	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	3	0	None	CVE-2011-3389 https://nvd.nist.gov/vuln/detail/CVE-2011-3389 Score: 4.3 Description: The SSL protocol, as used in certain configuratio
2023-05-12 02:54:57	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 03:38:37	Blacklisted Affiliate IP Address	Yes	UCEPROTECT	0	0	4	0	None	UCEPROTECT - Level 2 (some false positives) (207.154.228.160)
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.67): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:59	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	eliaspinheironeto.github.io
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	5	0	None	France
2023-05-12 02:55:21	Open TCP Port	No	Censys	0	0	3	0	None	207.154.228.169:22
2023-05-12 03:33:49	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	MiCCPICC Profile U$JLQ clc$1 pHYs iTXtXML:com.adobe.xmp <exif:PixelYDimension>1024</exif:PixelYDimension> <exif:PixelXDimension>1024</
2023-05-12 03:13:04	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [000b000.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:46:50	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	3	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 02:5a:61:0f:58:eb:84:f1:ad:53:ae:03:dc:a9:84:7a Signature Algorithm: ecdsa-with-SHA 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: 1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73 Timestamp : Dec 21 09:03:52.857 2022
2023-05-12 02:44:31	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3030::ac43:a8fc
2023-05-12 02:55:27	BGP AS Membership	No	URLScan.io	0	0	1	0	None	14061
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	000407.github.io
2023-05-12 03:11:27	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'format': {u'international': u'+14806242598', u'local': u'(480) 624-2598'}, u'country': {u'prefix': u'+1', u'code': u'US', u'name':
2023-05-12 03:00:54	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.84): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:09:04	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.109
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.213): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Paradiso Films - NL (Net ID: 00:01:21:31:1A:19)
2023-05-12 03:04:14	Malicious Affiliate	Yes	abuse.ch	0	1	3	0	None	abuse.ch URLhaus (Domain) [cdn-185-199-110-153.github.com] https://urlhaus.abuse.ch/downloads/csv_recent/
2023-05-12 03:19:01	WiFi Access	No	Wigle.net	0	0	3	0	None	PARPUDAR (Net ID: 00:02:CF:AD:76:95)

	Point Nearby								
2023-05-12 03:01:17	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.146): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	Pronouns.Page (Category: social) https://pronouns.page/api/profile/get/Altpapier?version=2
2023-05-12 02:46:42	Physical Location	No	Fraudguard	0	0	3	0	None	United States, South Carolina, North Charleston
2023-05-12 02:44:21	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Ziggo04216 (Net ID: 00:0C:F6:5A:10:78)
2023-05-12 03:16:19	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'ENG', u'country_tld': u'.uk', u'ip': u'2a06:98c1:3121::1', u'currency_name': u'Pound', u'currency': u'GBP', u'count
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.97): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	XFINITY (Net ID: 00:0D:67:8C:21:B1)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	krillnet (Net ID: 00:01:8E:15:D4:A6)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys-g (Net ID: 00:06:25:C0:3E:05)
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.193): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://funny.battleb0t.xyz/images/master058_2.PNG
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	MyBuilder.com (Category: social) https://www.mybuilder.com/profile/view/ayshoo
2023-05-12 02:45:51	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [104.21.6.166]
2023-05-12 03:00:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha2-512-etm@openssh.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:0C:41:37:F0:E0)
2023-05-12 03:24:19	Account on External Site	No	Account Finder	0	0	8	0	None	YouTube User2 (Category: video) https://www.youtube.com/@baptistevauthey
2023-05-12 02:54:16	HTTP Status Code	No	Web Spider	0	0	2	0	None	200
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:2052
2023-05-12 02:54:18	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2023-05-12 02:44:18	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Varnish
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.197): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:EF:F5:78)

2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.190): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:50	Open TCP Port	No	SSL Certificate Analyzer	0	0	3	0	None	34.148.97.127:443
2023-05-12 02:53:48	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "185.199.109.153:443"\n "104.18.136.59:443"\n "157.240.22.25:443"\n "104.16.121.190:443"\n "77.88.21.119:443"\n "104.18.25.196:443"\n href="https://am.linkedin.com/company/luckycarrot" target="_blank">" (Indicator: "linkedin.com")\n "<a href="https://www.youtube.com/c 0:Math.round(q/p*100),t=G.hidden?!1:.5<=Pi(c);d();var u=void 0;void 0!==b&&(u=[b]);var v=lv(c,"gtm.video",u);v["gtm.videoProvider"]="y N/A]\n "lucky%20carrot%20logo_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUID: N/A]\n "bring-visibility_1_.svg" has
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	imgur (Category: images) https://imgur.com/user/Altpapier/about
2023-05-12 02:44:27	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi2.battleb0t.xyz
2023-05-12 03:00:58	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	010101011zy.github.io
2023-05-12 03:01:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.123): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:36:51	Physical Location	No	MetaDefender	0	0	2	0	None	Medellin, Colombia
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	6566 1651 (Net ID: 00:00:C5:D7:63:6C)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WaveLAN Network VHome2B (Net ID: 00:02:2D:03:03:11)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MDD (Net ID: 00:02:2D:21:9D:34)
2023-05-12 03:11:21	Physical Coordinates	No	AbstractAPI	0	0	3	0	None	50.1188, 8.6843
2023-05-12 02:44:22	Internet Name	No	DNS Resolver	0	0	2	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	AUMWLAN (Net ID: 00:02:2D:1F:4C:85)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	3126416304 (Net ID: 00:01:03:7B:F5:4B)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Cracked (Category: social) https://www.cracked.com/members/login
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:2082
2023-05-12 03:01:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.253): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:58:32	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'Binary File', u'identifier': u'binary-5', u'name': u'Drops cabinet archive files', u'attck_id_wiki': None, u'threat_level_human': u' compression"- Location: [%TEMP%\\Cab475D.tmp]- [targetUID: 00000000-00003456]\n "RecoveryStore._DE97F9DD-7012-11ED-8A21-080027C90619_. Windows 2000/XP setup 62932 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%LOCALAPPDATA%\\ u'Unknown', u'entrypoint_section': None, u'md5': u'28f8b4c39853b6bc34686712011e8493', u'network_mode': u'default', u'processes': [], u
2023-05-12 03:13:03	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [000000014286.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	villagio (Net ID: 00:01:24:F0:87:66)
2023-05-12 03:04:46	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray

2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:0C:41:C6:10:31)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Ziggo07501 (Net ID: 00:0C:F6:5C:1D:4D)
2023-05-12 03:03:29	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:44:05	SSL Certificate Expiring	Yes	CertSpotter	0	0	1	0	None	2023-05-25 03:02:52
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Naver (Category: social) https://blog.naver.com/login
2023-05-12 02:46:02	Physical Location	No	AbstractAPI	0	0	3	0	None	North Charleston, South Carolina, 29415, United States, North America
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/random_2.jpeg
2023-05-12 03:36:07	Open UDP Port Information	No	Tool - nbtscan	0	0	4	0	None	NetBIOS Name Table for Host 45.131.109.53: Incomplete packet, 155 bytes long. Name Service Type ----------
2023-05-12 02:46:48	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_huma index 3284796353 field type 0 dBase III DBT version number 0 next free block index 3238251203"- Location: [%LOCALAPPDATA%\\Microsoft\\ None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 2, u 142.250.189.227"'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifier': u'string-14', u'name': u'Found potenti
2023-05-12 03:03:47	Co-Hosted Site	No	ThreatMiner	2	0	2	0	None	ebrahemsamir.github.io
2023-05-12 02:53:44	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level': 0, u'type': 7, u'description': u'"185.199.109.153:443"\n "172.66.40.106:443"\n "102.37.125.193:443"\n "35.186.254.174 u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': u'htt line terminators"- Location: [%TEMP%\\7008_1698674626\\edge_checkout_page_validator.js]- [targetUID: 00000000-00007008]\n "auto_open_c u=https%3A%2F%2Ftamannigeria.org%2FNUNEZ%2Fascensia.com%2Ffelicia.xu%40ascensia.com"\n Pattern match: "https://llink.to"\n Heuristic m
2023-05-12 03:13:02	Malicious Affiliate IP Address	Yes	Threat Jammer	0	1	3	0	None	Threat Jammer - Risk score: 40 (MEDIUM) https://threatjammer.com/info/87.248.157.93
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-mitigated: challenge
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.29): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:27:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.128:80
2023-05-12 02:53:35	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache_Hits": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "
2023-05-12 02:53:49	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:50c0:8000::/48
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	la_vieve (Net ID: 00:06:25:7B:45:13)
2023-05-12 03:24:21	HTTP Status Code	No	Web Spider	0	0	4	0	None	403
2023-05-12 03:09:28	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	2	0	2	0	None	acilacikveteriner.com
2023-05-12 03:35:25	Malicious IP on Same Subnet	Yes	VoIPBL OpenPBX IPs	0	0	4	0	None	VOIPBL Publicly Accessible PBX List [45.131.109.0/24] http://www.voipbl.org/update
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	sflan39 (Net ID: 00:02:6F:08:21:FC)
2023-05-12 03:19:47	Account on External Site	No	Account Finder	0	0	2	0	None	giters (Category: coding) https://giters.com/patrickpogoda
2023-05-12	WiFi Access	No	Wigle.net	0	0	4	0	None	HOME-0582 (Net ID: 00:1D:D4:13:05:80)

03:18:54	Point Nearby								
2023-05-12 03:17:38	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: AYHA.XYZ Registry Domain ID: D293590239-CNIC Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www. here for any purpose other than determining ownership of domain names, (2) not to store or reproduce this data in any way, (3) not to Tech Street: 26-1 Sakuragaoka-cho Tech Street: Cerulean Tower 11F Tech City: Shibuya-ku Tech State/Province: Tokyo Tech Postal Code: 1
2023-05-12 02:55:18	Physical Location	No	Censys	0	0	3	0	None	Frankfurt am Main, Hesse, 60306, Germany, Europe
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	008security.github.io
2023-05-12 02:46:50	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	3	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
2023-05-12 02:53:08	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:78:81:e1:ef:49:4b:f9:6d:c5:16:34:0e:55:ab:d5:12:44 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 75:02:
2023-05-12 03:23:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.11:8080
2023-05-12 03:00:50	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.72): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.115
2023-05-12 03:01:20	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.175): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	3dtoday (Category: hobby) https://3dtoday.ru/blogs/login
2023-05-12 02:55:18	Software Used	Yes	Censys	0	0	3	0	None	linux
2023-05-12 03:03:16	IP Address	No	DNS Resolver	0	0	2	0	None	172.67.168.252
2023-05-12 03:31:58	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.0:80
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Newgrounds (Category: gaming) https://login.newgrounds.com/
2023-05-12 03:12:58	Malicious Affiliate	Yes	OpenPhish	0	0	3	0	None	OpenPhish [frabjous-lebkuchen-324004.netlify.app] https://www.openphish.com/feed.txt
2023-05-12 02:46:42	Physical Location	No	Fraudguard	0	0	3	0	None	United States, South Carolina, North Charleston
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	3	0	None	GitHub\, Inc.
2023-05-12 03:09:26	Co-Hosted Site - Domain Whois	No	Whois	1	0	4	0	None	% Hello, this is the DOMREG whois service. % % By submitting a query you agree not to use the information made % available to: % - all
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	au.ru (Category: misc) https://au.ru/user/login/
2023-05-12 02:56:38	Raw Data from RIRs	No	Hybrid Analysis	1	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur launched with changed environment', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': Non None, u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"104.196.30.220:443"\n "172.67.128.152:443"\n "23.32.45.191:8 "~DF71962694B43492EC.TMP" has type "data"- Location: [%TEMP%\\~DF71962694B43492EC.TMP]- [targetUID: 00000000-00002536]\n "80237EE4964F Cabinet archive data 61712 bytes 1 file"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\77EC63BDA74BD0D0E0426DC
2023-05-12 03:43:29	Country	No	Country Name Extractor	0	0	6	0	None	United States
2023-05-12 03:24:29	Company Name	No	Company Name Extractor	0	0	3	0	None	Cloudflare\, Inc.
2023-05-12 03:22:54	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.1:8443
2023-05-12 02:55:11	Physical Location	No	Censys	1	0	2	0	None	Bursa, Bursa Province, 16250, Turkey, Asia
2023-05-12 02:46:36	Physical Location	No	MetaDefender	0	0	3	0	None	North Charleston, United States

2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	HNG (Net ID: 00:01:E3:0D:91:90)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	HackerRank (Category: tech) https://www.hackerrank.com/profile/login
2023-05-12 03:41:52	Software Used	Yes	Censys	0	0	3	0	None	Microsoft Windows
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	RIA-FRANKFURT (Net ID: 00:01:E3:5C:A6:A3)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 02:54:34	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.50): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	linksys (Net ID: 00:16:B6:2D:FB:6B)
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00x44.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:46:54	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	cloudflare.com
2023-05-12 02:57:24	Internet Name	No	Certificate Transparency	0	0	1	0	None	fluid.battleb0t.xyz
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ZyXEL (Net ID: 00:02:CF:4A:E5:0D)
2023-05-12 02:44:42	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.117
2023-05-12 03:08:51	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.124
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Nesrin (Net ID: 00:02:61:71:AB:40)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	ELSA1 (Net ID: 00:02:2D:29:60:79)
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	6	0	None	United States
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.239): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:10	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 400 Bad Request Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 253 Connection: close CF-RAY: -
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	kwejk.pl (Category: images) https://kwejk.pl/uzytkownik/login#/tablica/
2023-05-12 02:55:15	Software Used	Yes	Censys	0	0	3	0	None	linux
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	5	0	None	cloudflare
2023-05-12 03:09:34	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	01def.io
2023-05-	Account on	No	Account Finder	0	0	5	0	None	

12 03:18:26	External Site								Chess.com (Category: gaming) https://www.chess.com/member/Altpapier
2023-05-12 03:21:08	Account on External Site	No	Account Finder	0	0	2	0	None	wattpad (Category: social) https://www.wattpad.com/user/dawidsulej
2023-05-12 02:57:09	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:d8:ac:1a:31:df:8f:f8:c7:c3:27:35:9c:31:39:5f:60:e8 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: D4:B4:
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-A822 (Net ID: 00:1D:D4:64:A8:20)
2023-05-12 02:46:04	Physical Coordinates	No	AbstractAPI	0	0	3	0	None	32.8608, -79.9746
2023-05-12 02:59:58	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	name@example.com
2023-05-12 03:09:45	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	135.97.148.34.bc.googleusercontent.com
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	arpej (Net ID: 00:1A:2A:02:1A:E6)
2023-05-12 02:56:56	Internet Name	No	DNS Resolver	0	0	5	0	None	www.ayhu.xyz
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.214): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:80
2023-05-12 03:32:02	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.2:8080
2023-05-12 03:36:42	Physical Location	No	MetaDefender	0	0	2	0	None	Medellin, Colombia
2023-05-12 02:44:24	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 03:24:21	HTTP Headers	No	Web Spider	10	0	4	0	None	{"content-encoding": "gzip", "nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "referrer-policy": "same-o
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:2087
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	TF2 Backpack Examiner (Category: gaming) http://www.tf2items.com/id/Battleb0t/
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	vsco (Category: social) https://vsco.co/ayshoo/gallery
2023-05-12 02:54:07	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3031::ac43:8709:80
2023-05-12 02:55:22	Raw Data from RIRs	No	Google	0	0	1	0	None	{'webSearchUrl': u'https://www.google.com/search?q=site:battleb0t.xyz&aq=t&oe=utf-8&client=firefox-a&ie=utf-8&rls=org.mozilla%3Aen-US%
2023-05-12 03:32:19	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.10:443
2023-05-12 02:49:17	Raw Data from RIRs	No	Hybrid Analysis	2	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"185.199.110.153:443"\n "172.66.43.150:443"\ "twitter")\n "<script>!function(d,s,id){var js,fjs=d.getElementsByTagName(s)[0],p=/^http:/.test(d.location)?\'http\':\'https\';if(!d.g "GJU2ZIBE.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\GJU2ZIBE.txt]- [targetUID: 00000000-00001012] "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has type "MS Windows icon resource - 1 icon 32x32 32 bits/pixel"- [targetUID: N/A]
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	DaltonInt (Net ID: 00:0A:04:99:14:E2)
2023-05-12 02:54:21	Linked URL - Internal	No	Web Spider	0	0	3	0	None	http://vscode.battleb0t.xyz
2023-05-	Affiliate -	No	DNS Resolver	0	0	4	0	None	

12 03:09:45	Internet Name								133.97.148.34.bc.googleusercontent.com
2023-05-12 02:54:20	Web Content Type	No	Web Spider	0	0	4	0	None	text/css;charset=utf-8
2023-05-12 02:46:50	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 03:36:17	Blacklisted IP on Same Subnet	Yes	DroneBL	0	0	4	0	None	dronebl.org - Brute force attackers (45.131.109.177)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	tom1 (Net ID: 00:06:25:9C:ED:D2)
2023-05-12 03:12:11	Co-Hosted Site - Domain Whois	No	Whois	2	0	3	0	None	Domain Name: ACILACIKVETERINER.COM Registry Domain ID: 2652209212_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.nicproxy.com Registrar automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other Province: Redacted for Privacy Admin Postal Code: Redacted for Privacy Admin Country: Redacted for Privacy Admin Phone: Redacted for P related to domain name registration records. NICS Telekomunikasyon A.S. does not guarantee its accuracy. By submitting a WHOIS query,
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ZyXEL (Net ID: 00:02:CF:DB:DC:87)
2023-05-12 03:31:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	abuse@godaddy.com
2023-05-12 03:14:48	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	WSTOCK (Net ID: 00:1C:DF:E5:DC:4B)
2023-05-12 02:56:05	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'"\\Sessions\\1\\BaseNamedObjects\\IsoScope_e20_IESQMMUTEX_0_519"\n "Local\\ZonesCacheCounterMutex"\n "{5312EE61-79E3-4A24-BFE1-132B8 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"\n "77EC63BDA74BD0D0E0426DC8F8008506" has type "Microsoft Cabinet archive [targetUID: 00000000-00003616]\n "~DF261B847065F69F2A.TMP" has type "data"- Location: [%TEMP%\\~DF261B847065F69F2A.TMP]- [targetUID: 0 u'capec_id': None, u'attck_id': u'T1573', u'relevance': 3, u'threat_level': 0, u'type': 7, u'description': u'"HTTPS traffic to 104.196
2023-05-12 02:45:04	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SR.Mandant (Net ID: 00:01:21:30:6F:28)
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/favicon.png
2023-05-12 03:10:12	Malicious IP on Same Subnet	Yes	VoIPBL OpenPBX IPs	0	0	4	0	None	VOIPBL Publicly Accessible PBX List [64.226.80.0/20] http://www.voipbl.org/update
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.206): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:53	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	cloudflare.net
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Reddit (Category: social) https://www.reddit.com/user/ayshoo
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.6): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:25	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:d5:98:ae:2a:84:a2:19:ac:80:9a:6c:74:76:20:f8:3f:d8 Signature Algorithm: sha256Wi Web Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 6D 32:ae:7e:03:f4:0b:1f:cf:e7:b2:0f:1e:53:51:4d:d4:41:52: 82:77:57:35:05:af:16:cf:55:87:95:55:14:cd:4c:80:d7:09: 00:5e:46:ac:87:47:23:25:
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Flipboard (Category: tech) https://flipboard.com/@ayshoo
2023-05-12 03:00:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.14): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:17:05	Username	No	Account Finder	17	0	1	0	None	battleb0t

2023-05-12 02:54:01	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'informative', u'capec_id': None, u'attck_id': u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"kurt info"- [targetUID: N/A]\n "2UHLR4HR.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\2UHLR4HR.txt]- [tar u'relevance': 3, u'threat_level': 0, u'type': 2, u'description': u'Potential IP "5.1.0.0" found in string "Microsoft.Windows.Shell.run u'malicious_identifiers': [], u'malicious_identifiers_count': 0, u'technique': u'Ingress Tool Transfer', u'informative_identifiers': [
2023-05-12 02:54:20	BGP AS Membership	No	Censys	0	0	4	0	None	14618
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AitchBee13 (Net ID: 00:02:2D:68:90:A6)
2023-05-12 02:44:13	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	2	0	None	github.io
2023-05-12 02:44:28	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/random_6.PNG
2023-05-12 02:55:18	Open TCP Port	No	Censys	0	0	3	0	None	46.101.229.70:22
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:DD:2B:69)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Pornhub Users (Category: XXXPORNXXX) https://www.pornhub.com/users/login
2023-05-12 02:45:16	Physical Location	No	ipapi.co	0	0	4	0	None	Toronto, Ontario, ON, Canada, CA
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	nocwap (Net ID: 00:04:5A:CC:3F:27)
2023-05-12 02:44:27	IP Address	No	DNS Resolver	51	0	2	0	None	172.67.168.252
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	MIP (Net ID: 00:01:29:EE:B3:03)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	DD-WRT (Net ID: 00:14:BF:30:AA:54)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	20:35:09 (Net ID: 00:02:2D:05:BE:2A)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	RyanLG (Net ID: 00:01:36:4F:9A:F0)
2023-05-12 03:08:53	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.69
2023-05-12 03:00:10	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	cpanel.ayhu.xyz
2023-05-12 03:08:59	Affiliate - IP Address	No	DNS Look-aside	3	0	2	0	None	87.248.157.93
2023-05-12 03:01:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.251): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:58	Physical Coordinates	No	AbstractAPI	93	0	3	0	None	50.1188, 8.6843
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 09:cc:cb:40:35:8f:10:16:7b:c7:37:cb:94:7e:31:1a Signature Algorithm: ecdsa-with-SHA
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	1	2	0	None	220-cp.keyubu.net ESMTP Exim 4.95 #2 Wed, 10 May 2023 17:29:11 +0300 220-We do not authorize the use of this system to transport unsol
2023-05-12 03:32:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.7:443
2023-	Affiliate - IP	No	DNS Look-	1	0	3	0	None	

12 03:08:52	Address		aside						34.148.97.132
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	FizzyPop (Net ID: 00:02:2D:0F:C8:E1)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	07:55:46 (Net ID: 00:02:2D:05:BB:87)
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+74955801111
2023-05-12 02:44:09	Software Used	Yes	Tool - Wappalyzer	0	0	1	0	None	HTTP/3
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX55154D2E3 (Net ID: 00:01:E3:54:D2:E3)
2023-05-12 03:41:56	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	tjdev.de
2023-05-12 02:44:10	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	1	0	None	githubusercontent.com
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://funny.battleb0t.xyz
2023-05-12 03:18:50	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Horizontal (normal) @ 18}
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	#LG@Vo1P*Service& (Net ID: 00:01:36:57:A4:17)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	GZN00674 (Net ID: 00:00:00:00:00:F0)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F1:C3:85)
2023-05-12 02:54:13	HTTP Headers	No	Web Spider	9	0	3	0	None	{"content-length": "1591", "via": "1.1 varnish", "vary": "Accept-Encoding", "etag": "W/\"642b434c-1999\"", "x-cache-hits": "0", "cache
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	AUMWLAN (Net ID: 00:02:2D:0A:E6:C5)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	2WIRE271 (Net ID: 00:02:2D:8F:2B:40)
2023-05-12 03:03:32	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	000panther.github.io
2023-05-12 03:03:22	Co-Hosted Site - Domain Name	No	DNS Resolver	2	0	3	0	None	dontkillmyapp.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	jbnowires (Net ID: 00:06:25:F6:CF:DC)
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 02:55:15	Open TCP Port	No	Censys	0	0	3	0	None	165.232.113.85:443
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.69): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	PMV (Net ID: 00:05:5D:FA:C1:BE)
2023-05-	Software	Yes	Tool -	0	0	1	0	None	Cloudflare Turnstile

12 02:44:09	Used		Wappalyzer						
2023-05-12 03:22:52	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.1:8443
2023-05-12 03:00:51	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.78): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	141205 (Net ID: 00:0B:85:50:7F:90)
2023-05-12 03:03:21	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:55:07	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"185.199. u'origin': u'YARA Signature', u'identifier': u'yara-104', u'name': u'YARA signature match - RC4 Encryption', u'attck_id_wiki': u'https e48d-4dfb-a27d-6c7bdb483d29.tmp" has type "very short file (no magic)"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default u'"ojack.xyz" seems to be random'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifier': u'string-3', u'name':
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	x-timer: S1683860056.740489,VS0,VE2
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Reddit (Category: social) https://www.reddit.com/user/login
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=u1lyJPU0WioZJ7gW30pw%2F1QYGnEvSi6VguD4iZQLy9JFxNjUYX7Kn2
2023-05-12 03:03:21	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:08:49	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.110
2023-05-12 02:46:53	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	permissions-policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+74955801111
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	prettyflyforawifi 5 (Net ID: 00:01:9F:34:7C:4C)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	kathyncrew (Net ID: 00:05:3C:08:76:43)
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.214): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:35	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 03:00:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.18): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:53:17	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis "IsoScope_ab8_IESQMMUTEX_0_331"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-1', u'name': u'Co u'name': u'Drops files with image extension', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u 11ed-a4f7-08002766a00c}.dat"'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'na [%TEMP%\\~DF4FE4EBD509D90D4A.TMP]- [targetUID: 00000000-00002744]\n "imagestore.dat" has type "data"- Location: [%LOCALAPPDATA%\\Micro

2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet55FA (Net ID: 00:01:36:59:55:F8)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ENHLG (Net ID: 00:01:36:5B:37:00)
2023-05-12 03:08:54	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.70
2023-05-12 02:47:10	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\ZonesLockedCacheCounterMutex"\n "Local\\URLBLOCK_HASHFILESWITCH_MUTEX"\n "IsoScope_970_IESQMMUTEX_0_331"\n "Local\\VERMGMTBloc "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "214677895-b5497a9f-b78c-4c26-8ef3-880594c67e7a_1_. type "ASCII text with very long lines"- [targetUID: N/A]'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifier' en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: thewiki.moe\nD
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:01:24:F0:65:67)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	JIVE5.02025B0 (Net ID: 00:01:9F:20:25:B4)
2023-05-12 03:03:23	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	dontkillmyapp.com
2023-05-12 02:51:18	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/ u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relevance': 3, u'threat_level': 0, u'type': 8, u'description': u'"urlblock section info"- [targetUID: N/A]\n "~DFBF16C55F4A9DB7BF.TMP" has type "data"- Location: [%TEMP%\\~DFBF16C55F4A9DB7BF.TMP]- [targetUID: type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 0000
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	E3 (Net ID: 00:00:72:20:5B:C1)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	guventip (Net ID: 00:15:56:68:31:96)
2023-05-12 03:08:51	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.123
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	1	2	0	None	87.248.157.102:3306
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<hidden ssid> (Net ID: 00:01:E3:55:27:34)
2023-05-12 02:45:53	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\HKEY_LOCAL_MACHINE_SOFTWARE_Microsoft_Speech_OneCore_Voices_Tokens_MSTTS_V110_enUS_MarkM_Mutex"\n "\ u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 7, u'threat_level': 0, u'type': 2, u'descri stable.json, Indicator: "ubs.com")\n ""augustbleu.com"," (Source: wallet-stable.json, Indicator: "leu.com")\n ""bananasmonkey.com"," ("data_1" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Cache\\Cache_Data\\data_1]- [targetUID: 0000
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cross-origin-resource-policy: same-origin
2023-05-12 03:01:19	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.172): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.149): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	sflan7_1 (Net ID: 00:02:6F:04:08:D7)
2023-05-12 02:54:03	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:54:13	Linked URL - Internal	No	Web Spider	4	0	2	0	None	https://battleb0t.xyz/main.built.js
2023-05-12 02:54:18	HTTP Headers	No	Web Spider	6	0	2	0	None	{"nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "x-powered-by": "Express", "transfer-encoding": "chunk
2023-05-12 03:18:56	WiFi Access	No	Wigle.net	0	0	5	0	None	CATYLN (Net ID: 00:01:38:86:06:1F)

	Point Nearby								
2023-05-12 02:46:03	Physical Coordinates	No	AbstractAPI	0	0	3	0	None	32.8608, -79.9746
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.234): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:41:28	Country	No	Country Name Extractor	0	0	4	0	None	Netherlands
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:01:24:F2:17:BC)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	G5 Base (Net ID: 00:02:2D:1B:5B:C9)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ProCare-Guest (Net ID: 00:01:21:1C:31:00)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-ray: 7c5f60498977c3f0-EWR
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	ImageShack (Category: images) https://imageshack.com/user/ayshoo
2023-05-12 03:00:10	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:10:b4:30:a3:e0:72:2f:ec:4e:bc:95:e3:12:bb:83:8d:6f Signature Algorithm: ecdsa-wi F7:C7:09:DA:02:20:1E:EF:33:8E:F5:7A:6D:A5:37:EA: 0D:F2:52:F7:31:2F:0F:C3:A2:0E:FC:59:37:68:C1:0E: F3:7B:09:D9:73:6E Signature Algorith
2023-05-12 03:12:15	Affiliate - Domain Whois	No	Whois	5	0	6	0	None	Domain Name: NETCRAFT.COM Registry Domain ID: 509179_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http:/ enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, di +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: fd796f83a89a42f2a69f4b9f2c757b8f.protect@withheldforprivacy.com R
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-resource-policy: same-origin
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	55 2nd PMO (Net ID: 00:01:21:10:85:60)
2023-05-12 03:09:24	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	3	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BBHWIRELESS (Net ID: 00:00:C5:D7:5E:40)
2023-05-12 03:11:42	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	1	3	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 02:44:20	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 03:13:10	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [eliaspinheironeto.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:01:28	Web Server	No	Tool - WhatWeb	0	0	2	0	None	cloudflare
2023-05-12 03:00:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.16): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:00	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.102): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Steam (Category: gaming) https://steamcommunity.com/id/Altpapier
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	TOMTSSID (Net ID: 00:02:2D:76:6D:DF)
2023-05-12 03:32:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.7:8080
2023-05-12 02:44:06	Domain Registrar	No	Whois	0	0	1	0	None	Registrar of domain names REG.RU LLC

2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	WLAN (Net ID: 00:01:24:F1:42:27)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ZyXEL (Net ID: 00:02:CF:59:0A:CB)
2023-05-12 02:54:22	Linked URL - Internal	No	Web Spider	0	0	3	0	None	http://panel.battleb0t.xyz
2023-05-12 02:55:15	BGP AS Membership	No	Censys	0	0	3	0	None	14061
2023-05-12 03:09:32	Affiliate - Internet Name	No	DNS Resolver	2	0	3	0	None	cdn-185-199-109-154.github.com
2023-05-12 02:56:13	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"104.196.30.220:443"'}, {u'ca info"- [targetUID: N/A]\n "~DFF7760DEF9A5B2935.TMP" has type "data"- Location: [%TEMP%\\~DFF7760DEF9A5B2935.TMP]- [targetUID: 00000000 type "Microsoft Cabinet archive data Windows 2000/XP setup 62919 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 comp u'technique': u'Encrypted Channel', u'informative_identifiers': [], u'tactic': u'Command and Control', u'informative_identifiers_count
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom460A18 (Net ID: 00:0C:F6:46:0A:18)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	akniga (Category: hobby) https://akniga.org/profile/login
2023-05-12 02:47:23	Open TCP Port	No	Pulsedive	0	0	2	0	None	185.199.110.153:443
2023-05-12 03:31:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	abuse@porkbun.com
2023-05-12 02:45:47	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'Chantilly', u'security': {u'is_vpn': False}, u'city_geoname_id': 4751935, u'region_geoname_id': 6254928, u'country': u'Uni
2023-05-12 03:03:38	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:00:51	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.74): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WaveLAN Network (Net ID: 00:02:2D:03:8E:D3)
2023-05-12 03:31:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	abuse@godaddy.com
2023-05-12 02:53:17	IPv6 Address	No	Mnemonic PassiveDNS	0	0	1	0	None	2606:4700:3031::6815:6a6
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MIFI-LIBERATE-EPQS (Net ID: 00:15:FF:31:01:09)
2023-05-12 02:45:51	Physical Location	No	MetaDefender	0	0	2	0	None	Amsterdam, Netherlands
2023-05-12 03:00:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-128-etm@openssh.com
2023-05-12 02:57:10	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\IsoScope_724_ConnHashTable<1828>_HashTable_Mutex"\n "\\Sessions\\1\\BaseNamedObjects\\{5312EE61-79E3 "manifest_1_.webmanifest" has type "ASCII text with very long lines with no line terminators"- [targetUID: N/A]\n "6DB145CFEEC544B1582 9C6D-080027EE4932_.dat" has type "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "Tar231B.tmp" has 144x144.png?v=7ae7a1e080cabd99fd5784f81afc9125","sizes":"144x144","type":"image/png"},{"src":"icons/icon-192x192.png?v=7ae7a1e080cabd9
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:2077
2023-05-12	Account on External Site	No	Account Finder	0	0	2	0	None	Trello (Category: social) https://trello.com/patrickpogoda

03:19:47									
2023-05-12 03:31:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	a922252a687d4937a189d1d7289125ed.protect@withheldforprivacy.com
2023-05-12 03:09:18	Vulnerability - General	Yes	Tool - Retire.js	0	0	4	0	None	Bootstrap before 4.0.0 is end-of-life and no longer maintained. Severity: low Info: https://github.com/twbs/bootstrap/issues/20631
2023-05-12 03:08:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.80
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	zoom (Net ID: 00:01:38:44:83:6D)
2023-05-12 02:54:07	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3031::ac43:8709:443
2023-05-12 02:45:44	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'Chantilly', u'security': {u'is_vpn': False}, u'city_geoname_id': 4751935, u'region_geoname_id': 6254928, u'country': u'Uni
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Revolut (Category: finance) https://revolut.me/ayhu
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless (Net ID: 00:01:36:06:1C:1A)
2023-05-12 03:00:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.58): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	speedrun (Category: gaming) https://www.speedrun.com/user/login/
2023-05-12 03:03:41	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:03:59	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	scoop.sh
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Elijah Sadee (Net ID: 00:1D:D3:6D:1D:D0)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Ziggo1 (Net ID: 00:02:6F:D8:57:09)
2023-05-12 03:33:38	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	cHRM IDATx 9RD@R 6_:f Q3ot<@ :_w$`i 8vw8uLk iZpj bI@kd IDAT> !H?RZ Rz`8< e RmZ !heNN ZZ@"U P>HZD xq5E H!wqlM qkR` Z9wq-'C ghdf9egC O'
2023-05-12 02:54:13	HTTP Status Code	No	Web Spider	0	0	3	0	None	200
2023-05-12 02:45:58	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'city': u'Frankfurt am Main', u'security': {u'is_vpn': False}, u'city_geoname_id': 2925533, u'region_geoname_id': 2905330, u'country
2023-05-12 02:46:49	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	3	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
2023-05-12 02:44:20	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	1620 Guest (Net ID: 00:01:21:30:37:50)
2023-05-12 03:41:52	Physical Location	No	Censys	0	0	3	0	None	Frankfurt am Main, Hesse, 60306, Germany, Europe
2023-05-12 03:00:55	Co-Hosted Site	No	HackerTarget	3	0	2	0	None	00ffcc.cn
2023-05-12 02:44:28	Affiliate - Domain Name	No	DNS Resolver	0	0	3	0	None	netlify.app
2023-05-12 02:54:44	BGP AS Membership	No	Censys	0	0	3	0	None	396982
2023-05-	Raw Data	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur

12 02:55:34	from RIRs								domains', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'thre gs=new RegExp(/^(.*\\.)?(google|youtube|blogger|withgoogle)(\\.com?)?(\\.[a-z]{2})?\\.?$/),hs={cl:["ecl"],customPixels:["nonGooglePixe handlers.min_1_.js" has type "ASCII text with very long lines"- [targetUID: N/A]\n "webpack.runtime.min_1_.js" has type "ASCII text wi >\ufffd\ufffd\ufffd\u0785R\ufffd\ufffd`\uac7e\ufffdQ\ufffd$z/\ufffd2\ufffd\ufffdx\ufffdM\ufffdG\ufffdk\ufffdf6Ip\ufffd\ufffd\ufffd\uff
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	089070 (Net ID: 00:02:2D:08:90:70)
2023-05-12 03:33:40	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	IDATx _Z19l ?_ILPJ C $/@ 0\Mjf! /VppGp ChPwap fzcoAC P6s>W 4q:P? _6Wp@ T'V51 >Lv t0 qDXT<?95 @pjrR _ij>g rd-2mp :!xn2@ V4vbR isgWO fRO
2023-05-12 02:53:15	IPv6 Address	No	Mnemonic PassiveDNS	0	0	1	0	None	2606:4700:3037::6815:470e
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	5	0	2	0	None	+14806242505
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX5515724F5 (Net ID: 00:01:E3:57:24:F5)
2023-05-12 02:46:25	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:4a:0e:8c:1b:d3:a5:34:69:b6:32:8e:46:29:d8:95:17:d9 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 40:6C: 59:03:3d:d2:aa:47:fb:09:53:87:e3:c8:82:e2:86:64:89:77: d1:60:50:5c:4a:fa:5f:c3:d3:98:9d:1d:83:27:60:ff:97:a3: 81:ce:78:29:a2:b7:68:63:
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	000000jihyun.github.io
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	FRBEACH (Net ID: 00:02:2D:8A:07:06)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetCBD2 (Net ID: 00:01:36:59:CB:D0)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	championat (Category: news) https://www.championat.com/user/login/
2023-05-12 02:45:11	Physical Location	No	ipapi.co	0	0	2	0	None	Toronto, Ontario, ON, Canada, CA
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	4	0	3	0	None	https://pics.battleb0t.xyz/gallery.css
2023-05-12 02:55:28	Linked URL - Internal	No	URLScan.io	0	0	2	0	None	https://kekw.battleb0t.xyz/jar
2023-05-12 03:16:17	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	ayha.xyz
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	EWireless (Net ID: 00:06:25:B0:C4:C9)
2023-05-12 02:54:54	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'ransomware'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analys u'File/Memory', u'identifier': u'string-63', u'name': u'Found a potential E-Mail address in binary/memory', u'attck_id_wiki': u'https: "youtube")\n "px.ads.linkedin.com" (Indicator: "linkedin.com")\n "ds.linkedin.com" (Indicator: "linkedin.com")\n "https://px.ads.linke (x86)\\Microsoft\\Edge\\Application\\\\.\\pipe\\\\??\\pipe\\chrome.'}, {u'category': u'General', u'origin': u'File/Memory', u'identifi u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': u'htt
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	cf-ray: 7c5f60363a5a178c-EWR
2023-05-12 03:09:41	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	122.48.229.35.bc.googleusercontent.com
2023-05-12 03:01:19	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.167): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:16	HTTP Headers	No	Web Spider	6	0	4	0	None	{"nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "alt-svc": "h3=\":443\"; ma=86400, h3-29=\":443\"; ma=
2023-05-12 03:32:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.11:80
2023-05-12 02:58:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\VERMGMTBlockListFileMutex"\n "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "IsoScope_330_IE_EarlyTabStart_0xd98_Mutex"\n "\\Sessi

									has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\80237EE4964FC9C409AAF55BF996A292_D46D6FA25B7436 u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1573', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': 08/31/2022 13:38:03)\n URL: https://www.toprankedtechgadgetsnow.com/p/fl?affid=8929&provider=Affiliati&click_id=1912bde62d05461889c7b8
2023-05-12 03:17:37	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: ASHU.XYZ Registry Domain ID: D279374777-CNIC Registrar WHOIS Server: whois.namecheap.com Registrar URL: https://namecheap determining ownership of domain names, (2) not to store or reproduce this data in any way, (3) not to use any high-volume, automated, for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Count
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	referrer-policy: same-origin
2023-05-12 03:00:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.60): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:32:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.12:8080
2023-05-12 03:32:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.15:8080
2023-05-12 02:54:54	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:21:08	Account on External Site	No	Account Finder	0	0	2	0	None	Instagram (Category: social) https://instagram.com/dawidsulej
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00ty.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:44:13	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	2	0	None	github.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	4170004919 (Net ID: 00:0B:6B:20:D9:EC)
2023-05-12 03:09:51	Affiliate - Internet Name	No	DNS Resolver	1	0	3	0	None	dgn.keyubu.com
2023-05-12 02:54:15	HTTP Headers	No	Web Spider	8	0	2	0	None	{"content-length": "690", "via": "1.1 varnish", "vary": "Accept-Encoding", "etag": "W/\"642b434c-4fb\"", "x-cache-hits": "1", "cache-c
2023-05-12 02:44:15	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	2WIRE070 (Net ID: 98:2C:BE:4F:F5:49)
2023-05-12 03:09:36	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	218.30.196.104.bc.googleusercontent.com
2023-05-12 03:09:43	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	124.97.148.34.bc.googleusercontent.com
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.134): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Disqus (Category: social) https://disqus.com/by/login/
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-F8E2 (Net ID: 00:1D:D6:B4:F8:E0)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:EB:09:56)
2023-05-12 02:54:13	HTTP Status Code	No	Web Spider	0	0	4	0	None	403
2023-05-12 02:54:23	Netblock IPv6 Membership	No	Censys	0	0	4	0	None	2600:1f18:2000::/35
2023-05-12 02:54:25	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_ 4c82-9c12-a950739b1d75.tmp" has type "UTF-8 Unicode text with very long lines with no line terminators"- [targetUID: N/A]\n "83213497a prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE4wqHh?ver=0f07,copyright:Yuanping"\n Pattern match: "www.playstatio "%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Trust Protection Lists\\1.0.0.23"\n Potential IP "1.0.0.23" found in string "%LOCALAPPDAT
2023-05-	Co-Hosted	No	DNS Resolver	0	0	3	0	None	

12 03:03:40	Site - Domain Name								github.io
2023-05-12 02:53:56	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-12T02:29:53.974Z", "ip": "2606:50c0:8001::153", "location_updated_at": "2023-05-09T09:29:28.098368Z", "au "resolved_at": "2023-05-07T14:38:55.332333650Z"}, "shashank.im": {"record_type": "CNAME", "resolved_at": "2023-03-12T15:49:01.99295747 "2023-04-22T16:50:15.076942224Z"}, "montecarlo.mardh.eu": {"record_type": "CNAME", "resolved_at": "2023-03-16T04:12:54.462076635Z"}, " "blog.669.icu": {"record_type": "CNAME", "resolved_at": "2023-04-30T23:01:16.804648755Z"}, "www.nino.ie": {"record_type": "CNAME", "re "CNAME", "resolved_at": "2023-03-23T13:22:41.980546226Z"}, "pansypotter.gq": {"record_type": "AAAA", "resolved_at": "2023-01-05T15:01:
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	default (Net ID: 00:11:95:71:3F:FA)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	55 2nd PMO (Net ID: 00:01:21:10:85:60)
2023-05-12 02:44:40	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Google Analytics
2023-05-12 02:56:57	Internet Name	No	DNS Resolver	0	0	2	0	None	funny.battleb0t.xyz
2023-05-12 03:09:18	Vulnerability - General	Yes	Tool - Retire.js	0	0	4	0	None	CVE-2018-20677 Score: Unknown Description: Unknown
2023-05-12 03:00:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.48): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	Kongregate (Category: gaming) https://www.kongregate.com/accounts/battleb0t
2023-05-12 02:45:34	Affiliate - Internet Name	No	DNS Raw Records	6	0	1	0	None	skip.ns.cloudflare.com
2023-05-12 03:10:37	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.108.154:80
2023-05-12 03:08:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.79
2023-05-12 03:13:03	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [000000jihyun.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.194): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	phi (Net ID: 00:06:B1:2D:D2:D1)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	curealty (Net ID: 00:0C:41:49:32:21)
2023-05-12 03:05:41	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2011-3389 https://nvd.nist.gov/vuln/detail/CVE-2011-3389 Score: 4.3 Description: The SSL protocol, as used in certain configuratio
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	42 (Net ID: 00:01:03:7C:0D:EE)
2023-05-12 02:59:56	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	benjamin.mckenzie@atimetals.com
2023-05-12 02:44:15	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	2	0	None	C=US,ST=California,L=San Francisco,O=Netlify\, Inc,CN=*.netlify.app
2023-05-12 03:04:14	Malicious Affiliate	Yes	abuse.ch	0	1	3	0	None	abuse.ch URLhaus (Domain) [cdn-185-199-108-153.github.com] https://urlhaus.abuse.ch/downloads/csv_recent/
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	104.21.71.14
2023-05-12 03:09:08	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	165.232.113.94

2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.121): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [01-edu.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:53:06	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	None None
2023-05-12 03:09:35	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	215.30.196.104.bc.googleusercontent.com
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-ray: 7c5f8c5a3bb81a1b-EWR
2023-05-12 02:44:27	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:29:bb:71:26:4f:a3:73:c9:d3:c4:af:c8:b3:a3:33:dc:41 Signature Algorithm: ecdsa-wi AD:CF:EB:D0:94:75:7F:1F:5A:28:FD:93:B5:75:02:8F: D1:C6:87:41:2E:02:20:7C:52:E6:58:A4:8D:55:6A:69: 9C:2C:54:4C:7F:AC:22:28:8D:2B:54:D7:
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Reddit (Category: social) https://www.reddit.com/user/Altpapier
2023-05-12 03:31:32	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@dynadot.com
2023-05-12 02:54:41	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["0"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "
2023-05-12 03:09:28	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	acilacikveteriner.com
2023-05-12 03:33:34	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	!2222222222222222222222222222222222222222222222222 3 zVm Y7a5mH LyBu5 @rO$T gt@G<U rCrV8 e$?>z DvgsWuM_ w"$RO WW uvW_c KT`\d Vb /'T T
2023-05-12 02:51:33	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'"89667lpjzo.thebassbite.com"\n "ajax.googleapis.com"\n "api.edgeoffer.microsoft.com"\n "assets.adobedtm.com"\n "c.go-mpulse.net"\n " wallet-checkout-eligible-sites-pre-stable.json, Indicator: "key.com")\n ""order.firehousesubs.com"," (Source: wallet-checkout-eligible 0, u'type': 8, u'description': u'"urlref_https89667lpjzo.thebassbite.comfr-revenue-eservices-craindex.php_112726_redrisky%40icloud.com [targetUID: 00000000-00002300]\n "auto_open_controller.js" has type "UTF-8 Unicode text with very long lines with CRLF line terminator
2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	MCName (Minecraft) (Category: gaming) https://mcname.info/en/search?q=Altpapier
2023-05-12 03:27:00	Linked URL - External	No	Web Server Identifier	0	0	4	0	None	http://127.0.0.1:*
2023-05-12 02:54:13	Open TCP Port	No	Censys	0	0	4	0	None	2606:4700:3030::ac43:a8fc:443
2023-05-12 03:00:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.6): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:09:41	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	126.48.229.35.bc.googleusercontent.com
2023-05-12 03:03:17	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	S-lan (Net ID: 00:01:24:F1:91:41)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	sflan50 (Net ID: 00:02:6F:32:A9:45)
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	YouTube User (Category: video) https://www.youtube.com/user/ayshoo/about
2023-05-12 02:56:54	Affiliate - Internet Name	No	DNS Resolver	1	0	2	0	None	cp.keyubu.net
2023-05-12 03:09:40	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	117.48.229.35.bc.googleusercontent.com
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	5	0	None	United States
2023-05-	WiFi	No	Wigle.net	0	0	3	0	None	

12 03:18:53	Access Point Nearby								BJNPSETUP (Net ID: 00:00:85:F6:C3:DF)
2023-05-12 02:56:45	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:97:99:5c:60:ac:40:68:f8:b2:de:0a:67:7a:da:b7:d1:16 Signature Algorithm: sha256Wi 1e:b1:21:17:9e:36:0c:2a:fd:f3:0a:f5:98:b6:cc:3c:01:67: f2:0d:fc:88:12:e2:d6:83:96:22:f2:3a:bb:54:5e:67:b9:fa: 0b:ad:7a:8d:5d:db:b1:9d:
2023-05-12 02:45:24	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'HE', u'country_tld': u'.de', u'ip': u'64.226.81.43', u'currency_name': u'Euro', u'currency': u'EUR', u'country_popu
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Steve (Net ID: 00:16:E3:41:0D:E8)
2023-05-12 02:48:19	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:50:55:6d:e5:64:92:a0:7f:d0:de:03:2b:af:77:c2:fc:fe Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: CB:34:
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Maingau (Net ID: 00:02:2D:66:94:73)
2023-05-12 03:01:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.242): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Mastodon-API (Category: social) https://mastodon.social/api/v2/search?q=login
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Gamespot (Category: gaming) https://www.gamespot.com/profile/login/
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	default (Net ID: 00:01:71:0A:12:B3)
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	Chess.com (Category: gaming) https://www.chess.com/member/battleb0t
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BARWN-Public (Net ID: 00:02:6F:03:AE:69)
2023-05-12 03:01:10	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.123): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:F7:8C:15)
2023-05-12 02:56:50	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur zacharyburdette.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GET /index.webmanifest HTTP/1.1\nAccept: text/htm 62932 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"\n "Cab87C2.tmp" has type "Microsoft Cabinet archiv 00002800]\n "Tar87C3.tmp" has type "data"- Location: [%TEMP%\\Tar87C3.tmp]- [targetUID: 00000000-00002800]\n "Cab87C0.tmp" has type "M [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 00000000-00002800]\n "4WUOR
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=qVGOB1rQJjQIM8j8t5Spm5SzuRznIdJDuYO5Jbpn3fZk%2BJxIqln47O
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SX55154A43F (Net ID: 00:01:E3:54:A4:3F)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:F7:35:6D)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	LCPSSTAFF (Net ID: 00:0B:85:50:7F:91)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	likeevideo (Category: social) https://likee.video/@login
2023-05-12 03:11:17	Physical Location	No	AbstractAPI	1	0	2	0	None	Amsterdam, North Holland, 1012, Netherlands, Europe
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	MCUUID (Minecraft) (Category: gaming) https://mcuuid.net/?q=ayshoo
2023-05-12 02:53:18	Internet Name	No	Mnemonic PassiveDNS	25	0	1	0	None	www.ayhu.xyz
2023-05-12 03:01:20	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.182): Search Engine Last Activity: 0 days ago Threat Level: 29

2023-05-12 02:50:42	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7, OpenType (EOT) Font Awesome 5 Pro Light family"- [targetUID: N/A]\n "fa-regular-400_1_.eot" has type "Embedded OpenType (EOT) Font Awe "RecoveryStore._D7A145BF-EF99-11ED-9F88-080027F31822_.dat" has type "Composite Document File V2 Document Cannot read section info"- [t [targetUID: N/A]'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifier': u'string-3', u'name': u'Found potentia
2023-05-12 03:32:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.20:80
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.183): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:47:17	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'mutant-0', u'name': u'Creates mutants', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id document ASCII text with CRLF line terminators"- [targetUID: N/A]\n "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has type "MS W Encoding: gzip, deflate\nDNT: 1\nConnection: Keep-Alive\nHost: rakha360.github.io"\n "GET /facebook/ HTTP/1.1\nAccept: text/html, appl https://rakha360.github.io/facebook/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Geck
2023-05-12 02:46:54	Affiliate - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-l.github.io
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Apple Network 0a20a8 (Net ID: 00:02:2D:0A:20:A8)
2023-05-12 03:00:49	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.71): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MainSurf (Net ID: 00:02:2D:67:EF:87)
2023-05-12 02:45:19	Physical Location	No	ipapi.co	1	0	4	0	None	Ashburn, Virginia, VA, United States, US
2023-05-12 03:11:24	Physical Location	No	AbstractAPI	0	0	3	0	None	Arizona, United States
2023-05-12 03:00:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	chacha20-poly1305@openssh.com
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys-g (Net ID: 00:06:25:C0:74:7C)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX551573A43 (Net ID: 00:01:E3:57:3A:43)
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.181): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.222): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:34:24	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	45.131.109.48
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Interwrx1 (Net ID: 00:02:2D:A8:7E:D5)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	My Passport (2.4 GHz) - 07B79D (Net ID: 00:00:C0:07:B7:9D)
2023-05-12 03:15:08	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	battleb0t.wtf
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	hhcpatp (Net ID: 00:06:25:49:AE:74)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Caymen-ENT (Net ID: 00:00:C5:DE:B8:F1)
2023-05-12 02:44:03	Username	No	SpiderFoot UI	36	0	0	0	None	ayshoo

2023-05-12 03:01:19	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.170): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	wullbrandt (Net ID: 00:06:25:51:EC:E1)
2023-05-12 02:44:15	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:2052
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ENDOMED (Net ID: 00:02:CF:87:A5:FB)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=fiT%2Fr8CwWrAQPZkt8VpkeQoVoGOR6HuHPRasaTPIcW93tfGJar9pTi
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	RPOWER1 (Net ID: 00:02:6F:B3:3B:A8)
2023-05-12 02:53:04	Raw Data from RIRs	No	Tool - WAFW00F	1	0	2	0	None	[{"url": "https://fluid.battleb0t.xyz", "firewall": "Cloudflare", "detected": true, "manufacturer": "Cloudflare Inc."}, {"url": "https
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:05:5D:EC:C1:DE)
2023-05-12 03:24:22	Web Content	No	Web Spider	1	0	2	0	None	<!DOCTYPE html> <html> <iframe src="https://cloudways-static-content.s3.us-east-1.amazonaws.com/error_page/maintenance-domain-mapping.
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	imgur (Category: images) https://imgur.com/user/battleb0t/about
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 03:13:04	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [001cat.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:3C:1A:6D)
2023-05-12 02:54:13	Software Used	Yes	Censys	0	0	4	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.148): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	celikpalas (Net ID: 00:12:17:69:2B:2C)
2023-05-12 03:00:58	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.99): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.25): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.36): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:74:7D:E7:23)
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Trello (Category: social) https://trello.com/Altpapier
2023-05-12 02:55:15	Software Used	Yes	Censys	0	0	3	0	None	Laravel Laravel
2023-05-12	Physical Location	No	AbstractAPI	0	0	2	0	None	Chantilly, Virginia, 20151, United States, North America

02:45:45									
2023-05-12 02:59:02	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"34.74.170.74 (with BOM) text with CRLF line terminators"- [targetUID: N/A]\n "7423F88C7F265F0DEFC08EA88C3BDE45_D975BBA8033175C8D112023D8A7A8AD6" ha http://brittanysdesigns.com/ (AV positives: 1/88 scanned on 08/26/2022 07:14:28)\n URL: http://musing-khorana-e13644.netlify.app/ (AV False, u'error_type': None, u'state': u'SUCCESS', u'entrypoint': None, u'mitre_attcks': [], u'certificates': [], u'hosts': [u'34.74.17
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 03:13:06	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0080004.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	w1r3L3ss (Net ID: 00:01:24:F3:0B:65)
2023-05-12 02:44:23	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:b3:d3:7f:a8:50:41:aa:70:38:c6:ab:16:2e:24:50:f9:66 Signature Algorithm: sha256Wi Extensions: none Signature : ecdsa-with-SHA256 30:45:02:20:28:6D:42:8E:49:9E:0C:06:C1:19:32:87: BF:75:CE:80:8F:D6:EA:C5:3B:07:D6:4C:75
2023-05-12 03:24:19	Account on External Site	No	Account Finder	0	0	8	0	None	Picsart (Category: art) https://picsart.com/u/baptistevauthey
2023-05-12 02:50:17	Internet Name	No	DNS Resolver	0	0	2	0	None	www.battleb0t.xyz
2023-05-12 03:03:32	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	U+Net149B-CHO (Net ID: 00:01:36:93:14:99)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	TF2 Backpack Examiner (Category: gaming) http://www.tf2items.com/id/login/
2023-05-12 02:57:27	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"35.229.48.116:443"'}, {u'category': u'General', %USERPROFILE%\\Downlo ..." (UID: 00000000-00003484)'}, {u'category': u'Unusual Characteristics', u'origin': u'Binary File', u'identifi [%TEMP%\\~DFD6CAA9D81E87A12A.TMP]- [targetUID: 00000000-00002440]\n "JavaDeployReg.log" has type "ASCII text with CRLF line terminator u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 6, u'description': u'"rundll32.exe" connecting to "\\ThemeApiPort"'},
2023-05-12 02:56:12	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"Local\\InternetShortcutMutex"\n "{5312EE61-79E3 62919 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"\n "77EC63BDA74BD0D0E0426DC8F8008506" has type "Mic "MS Windows icon resource - 1 icon 32x32 32 bits/pixel"- [targetUID: N/A]\n "2NV4DI3M.txt" has type "ASCII text"- Location: [%APPDATA% network traffic', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1573', u'threat_level_human': u'informative', u'capec_id':
2023-05-12 03:12:58	Malicious Affiliate	Yes	OpenPhish	0	0	3	0	None	OpenPhish [battleb0t.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:54:15	HTTP Status Code	No	Web Spider	0	0	2	0	None	200
2023-05-12 03:11:18	Physical Coordinates	No	AbstractAPI	0	0	2	0	None	52.3759, 4.8975
2023-05-12 02:53:32	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.52): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:23:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.15:8080
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomAABCE4 (Net ID: 00:0C:F6:AA:BC:E4)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	medyczka.pl (Category: health) http://medyczka.pl/user/login
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WestEd (Net ID: 00:02:2D:05:7E:93)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AIRTIES (Net ID: 00:12:BF:53:F6:5F)

2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	1	3	0	None	nginx
2023-05-12 02:44:39	Internet Name	No	DNS Resolver	0	0	2	0	None	battleb0t.xyz
2023-05-12 02:47:32	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.135.9:8080
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	USR9110 (Net ID: 00:14:C1:13:AB:45)
2023-05-12 02:44:30	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Netlify
2023-05-12 03:00:49	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.70): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:52:24	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'T1071', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"185.199.108.153:443"\n "151.101.1.229:443"\n "104.18.22. data 640 x 480 8-bit/color RGBA non-interlaced" and extension "png"\n "device-pile-in_1_.png" has type "PNG image data 640 x 480 8-bit "c:\\users\\%osuser%\\appdata\\local\\microsoft\\internet explorer\\recovery\\high\\active\\{1585a87b-ebb4-11ed-8e6c-080027e195af}.dat "free-v4-shims.min_1_.css" has type "ASCII text with very long lines"- [targetUID: N/A]\n "en-US.4" has type "data"- Location: [%LOCAL
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	KP51 (Net ID: 00:01:71:0A:07:87)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	200WMadison (Net ID: 00:01:21:30:9B:23)
2023-05-12 02:54:30	Software Used	Yes	Censys	0	0	3	0	None	OpenBSD OpenSSH 7.9
2023-05-12 03:31:32	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@resellercamp.com
2023-05-12 02:54:22	Linked URL - External	No	Web Spider	0	0	4	0	None	https://pbs.twimg.com/profile_images/1513617779546595336/ojFIrGXM_400x400.jpg
2023-05-12 02:54:17	Open TCP Port	No	Censys	0	0	4	0	None	2606:4700:3037::6815:470e:80
2023-05-12 03:23:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.9:8080
2023-05-12 03:12:12	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 5.9 Description: OpenVPN, when using a 64-bit block cipher, makes
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-cache-status: MISS
2023-05-12 03:03:51	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	ply.gg
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wlan (Net ID: 00:01:71:0A:19:07)
2023-05-12 03:03:16	IP Address	No	DNS Resolver	0	0	2	0	None	104.21.71.14
2023-05-12 02:45:12	Physical Location	No	ipapi.co	0	0	2	0	None	Toronto, Ontario, ON, Canada, CA
2023-05-12 02:53:42	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:01:00	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.104): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	3	0	None	GitHub\, Inc.
2023-05-12 03:09:08	Vulnerability - General	Yes	Tool - Retire.js	0	1	4	0	None	CVE-2019-8331 Score: Unknown Description: Unknown
2023-05-12	Co-Hosted Site -	No	DNS Resolver	0	0	3	0	None	github.io

03:03:26	Domain Name								
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	tsunami (Net ID: 00:0D:29:AC:D7:1D)
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	2	0	None	REG.RU LLC
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.43): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-cache-hits: 0
2023-05-12 02:53:49	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	exim exim 4.95
2023-05-12 03:08:51	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.125
2023-05-12 03:09:05	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.111
2023-05-12 03:35:10	Malicious Co-Hosted Site	Yes	Comodo	0	1	3	0	None	Blocked by Comodo DNS [00ffcc.cn]
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	VGF-KonstablerWache (Net ID: 00:02:6F:84:5C:04)
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	007-liang.github.io
2023-05-12 03:12:14	Affiliate - Domain Whois	No	Whois	6	0	6	0	None	Domain Name: 01def.io Registry Domain ID: e5ba8be85003487fa75e094c9481d3b7-DONUTS Registrar WHOIS Server: whois.namecheap.com Registra PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FO further queries for a period of time to prevent disruption of Whois service access. Abuse of the Whois system through data mining is m Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registr
2023-05-12 02:59:54	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	dave@bradshaw.net
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	NettWork2 (Net ID: 00:01:E3:0E:70:8B)
2023-05-12 03:09:41	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	124.48.229.35.bc.googleusercontent.com
2023-05-12 03:24:22	HTTP Status Code	No	Web Spider	0	1	2	0	None	403
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Filmweb (Category: hobby) https://www.filmweb.pl/user/login
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	tsunami (Net ID: 00:0D:29:AC:D1:67)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	non-specified SSID !! (Net ID: 00:02:2D:8E:B2:0E)
2023-05-12 03:11:21	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'city': u'Frankfurt am Main', u'security': {u'is_vpn': False}, u'city_geoname_id': 2925533, u'region_geoname_id': 2905330, u'country
2023-05-12 02:45:36	Affiliate - Internet Name	No	DNS Raw Records	1	0	2	0	None	frabjous-lebkuchen-324004.netlify.app
2023-05-12 02:44:15	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	2	0	None	C=US,ST=California,L=San Francisco,O=GitHub\, Inc.,CN=*.github.io

2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	LILLY_BURSA (Net ID: 00:1A:2A:05:D4:D0)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Dowling_Network (Net ID: 00:1D:D5:13:CA:40)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-ray: 7c5f60465c67192a-EWR
2023-05-12 03:00:12	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	cpcalendars.ayhu.xyz
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	3	0	None	GitHub\, Inc.
2023-05-12 03:41:52	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: <REDACTED> Connection: close Cont
2023-05-12 03:41:58	Internet Name	No	DNS Resolver	0	0	4	0	None	vm.battleb0t.xyz
2023-05-12 02:54:16	Web Content	No	Web Spider	1	0	2	0	None	<!DOCTYPE html> <html> <head> <meta charset="utf-8"> <meta http-equiv="Cache-Control" content="no-cache"> <meta name="viewport" conten
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	RossAviation206 (Net ID: 00:0C:42:6C:BE:A6)
2023-05-12 03:08:53	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.65
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<hidden ssid> (Net ID: 00:01:E3:54:AE:E3)
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.38): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:11:17	Physical Coordinates	No	AbstractAPI	90	0	2	0	None	52.3759, 4.8975
2023-05-12 02:52:59	Raw Data from RIRs	No	Tool - WAFW00F	1	0	2	0	None	[{"url": "https://www.battleb0t.xyz", "firewall": "Fastly", "detected": true, "manufacturer": "Fastly CDN"}, {"url": "https://www.batt
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.51): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:13:09	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [01010101lzy.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:45:48	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': bits/pixel"- [targetUID: N/A]\n "script_1_.js" has type "ASCII text"- [targetUID: N/A]\n "VOPKN6EE.htm" has type "HTML document ASCII vincentgarreau.com"\n Pattern match: "http://opensource.org/licenses/MIT"\n Pattern match: "vincentgarreau.com/particles.js"\n Pattern
2023-05-12 02:45:48	Physical Location	No	AbstractAPI	1	0	2	0	None	Chicago, Illinois, 60666, United States, North America
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	5	0	None	cloudflare
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	NGMH (Net ID: 00:09:5B:B3:C8:70)
2023-05-12 02:45:48	Internet Name	No	VirusTotal	0	0	2	0	None	funny.battleb0t.xyz
2023-05-12 02:54:13	HTTP Status Code	No	Web Spider	0	0	3	0	None	200
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	4	0	None	cloudflare
2023-05-12 02:44:26	Internet Name	No	DNS Resolver	0	0	2	0	None	battleb0t.xyz

2023-05-12 03:03:29	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:10:00	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	shop.telleria.com
2023-05-12 03:03:22	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	0.church
2023-05-12 03:08:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.84
2023-05-12 03:18:06	URL (Uses Javascript)	No	Page Information	0	0	3	0	None	http://oldfluid.battleb0t.xyz
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wavelan network (Net ID: 00:02:2D:0D:63:6F)
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	DevOps - DevOps is a methodology in the software development and IT industry. Used as a set of practices and tools, DevOps integrates
2023-05-12 02:44:20	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 03:32:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.14:443
2023-05-12 02:56:33	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\Local\\!BrowserEmulation!SharedMemory!Mutex"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\VERMGMTBlock [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\80237EE4964FC9C409AAF55BF996A292_D46D6FA25B74360E1349F9015B5CCE53]- [targe u'https://attack.mitre.org/techniques/T1573', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1573', u'relev ++-,,-,,-,,-,,-,,100wvv-,,-,,-,,-,,-,,-,,-,,-,,wvv100-,,-,,-,,-,,-,,+++,++-,,-,,-,,-,,-,,ONN0//-,,-,,100ZYYZYY100-,,-,,0//ONN-,,-,,-,,
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Chris (Net ID: 00:1D:D1:A7:3B:10)
2023-05-12 02:56:54	IPv6 Address	No	DNS Resolver	0	0	2	0	None	2606:4700:3031::ac43:8709
2023-05-12 03:03:24	Co-Hosted Site - Domain Name	No	DNS Resolver	2	0	3	0	None	000.lt
2023-05-12 03:32:18	Malicious Affiliate	Yes	abuse.ch	0	1	4	0	None	abuse.ch URLhaus (Domain) [cdn-185-199-109-154.github.com] https://urlhaus.abuse.ch/downloads/csv_recent/
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Mariner (Net ID: 00:14:C1:0D:F8:10)
2023-05-12 03:01:17	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.153): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:09:43	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	123.97.148.34.bc.googleusercontent.com
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:00:C5:D7:47:EC)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	XFINITY (Net ID: 00:0D:67:33:68:5F)
2023-05-12 03:01:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.125): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AIRTIES (Net ID: 00:12:BF:30:97:DD)
2023-05-12	Internet Name	No	Certificate Transparency	0	1	1	0	None	nuke.battleb0t.xyz

2023-05-12 02:57:25									
2023-05-12 02:53:20	IP Address	No	Mnemonic PassiveDNS	28	0	2	0	None	207.154.228.169
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	BDSMLR (Category: XXXPORNXXX) https://login.bdsmlr.com
2023-05-12 02:44:15	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:4d:72:d7:7c:dd:a7:02:dd:5a:67:f2:a2:3b:bd:d9 Signature Algorithm: sha256WithRSAE - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1-1.crt X509v3 Basic Constraints fa:29:72:01:3e:b7:06:f1:2f:1a:0e:91:c5:ec:35:bf:f5:da: 33:95:de:24:12:0d:f5:c3:23:8d:40:82:d1:5c:eb:de:0a:08: e8:e5:83:e5:0a:8b:3a:5e:
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/fredo.PNG
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Twitter (Category: social) https://twitter.com/Altpapier
2023-05-12 02:48:53	Malicious Co-Hosted Site	Yes	VirusTotal	0	0	2	0	None	VirusTotal [githubusercontent.com] https://www.virustotal.com/en/domain/githubusercontent.com/information/
2023-05-12 02:45:35	Raw DNS Records	No	DNS Raw Records	0	0	1	0	None	ayhu.xyz. 86400 IN NS brett.ns.cloudflare.com. ayhu.xyz. 86400 IN NS leanna.ns.cloudflare.com.
2023-05-12 03:09:55	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	plesk.keyubu.net
2023-05-12 02:54:15	Web Content Type	No	Web Spider	0	0	2	0	None	text/html;charset=utf-8
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	TF2 Backpack Examiner (Category: gaming) http://www.tf2items.com/id/battleb0t/
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	x-github-request-id: 1AD4:4FA0:AFAB37:106D10A:645DA7F4
2023-05-12 03:31:19	Malicious IP on Same Subnet	Yes	blocklist.de	0	0	4	0	None	blocklist.de List [64.226.80.0/20] http://lists.blocklist.de/lists/all.txt
2023-05-12 02:44:05	Raw Data from RIRs	No	CertSpotter	10	0	1	0	None	[{u'pubkey_sha256': u'b1d8ad495b85281ccdd8ee8835d1b0223d8372b54869daf463e92de6ed172160', u'cert_sha256': u'3d687aa671181674e4491f35d4a u'MIIGKzCCBROgAwIBAgISBDdoex8mKc2kzJVS3+IKEm8TMA0GCSqGSIb3DQEBCwUAMDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQDEwJS u'sha256': u'3d687aa671181674e4491f35d4a504fe8ede2a23edcb11a1a5f1573f42d7a75d', u'type': u'cert'}, u'dns_names': [u'nuke.battleb0t.xyz u'MIIFKjCCBBKgAwIBAgISA5eZXGCsQGj4st4KZ3rat9EWMA0GCSqGSIb3DQEBCwUAMDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQDEwJS u'friendly_name': u"Let's Encrypt", u'name': u"C=US, O=Let's Encrypt, CN=R3"}}, {u'pubkey_sha256': u'5a0559923d0fdaac1fc6a74472ffcb94c u'MIIFMTCCBBmgAwIBAgISBJEIZbRWlOOJN2vI7lr89IBSMA0GCSqGSIb3DQEBCwUAMDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQDEwJS u'8d02536c887482bc34ff54e41d2ba659bf85b341a0a20afadb5813dcfbcf286d', u'friendly_name': u"Let's Encrypt", u'name': u"C=US, O=Let's Encr u'MIIFNTCCBB2gAwIBAgISBLY5M6/eHjLz/C523LwIUYYQMA0GCSqGSIb3DQEBCwUAMDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQDEwJS u'8d02536c887482bc34ff54e41d2ba659bf85b341a0a20afa
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F0:97:C1)
2023-05-12 02:54:23	HTTP Status Code	No	Web Spider	0	0	5	0	None	403
2023-05-12 02:45:35	Internet Name	No	DNSDumpster	0	0	1	0	None	kekw.battleb0t.xyz
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.61): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.123
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Troop (Net ID: 00:0E:F4:ED:81:91)
2023-05-12 03:00:57	Malicious Co-Hosted Site	Yes	VXVault.net	0	1	2	0	None	VXVault Malicious URL List [github.com] http://vxvault.net/URL_List.php
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	0	0	1	0	None	CN=oldfluid.battleb0t.xyz
2023-05-12 03:23:35	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.13:8443
2023-05-12 03:08:49	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.108

2023-05-12 02:44:24	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi.battleb0t.xyz
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-opener-policy: same-origin
2023-05-12 03:00:58	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0101.github.io
2023-05-12 03:33:13	Web Content Language	No	Language Detector	0	0	5	0	None	English
2023-05-12 02:54:07	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-resource-policy: same-origin
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.4): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MSCI (Net ID: 00:11:93:03:4B:10)
2023-05-12 03:23:09	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.0:80
2023-05-12 03:34:01	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	"Exif sgssso <Qwm7 >6x.O x>t7? g$sy? .b97< /Ggy! l/5-o ggs43Z x.o.n> NNEsz gmuss Mswy5 dIys6 >t6w6 03Ryr\G a>0xM g_on8 9!6sBsmms ?r:\t
2023-05-12 02:48:47	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\{5312EE61-79E3-4A24-BFE1-132B85B23C3A}"\n "\\Sessions\\1\\BaseNamedObjects\\IsoScope_fc4_IESQMMUTEX_ {state:0,transportUrl:b,context:c,parent:ki()},J(91);else{var f="/gtag/destination?id="+encodeURIComponent(a)+"&l="+ke.ca+"&cx=c";No() u'threat_level': 0, u'type': 8, u'description': u'"Cab27BE.tmp" has type "Microsoft Cabinet archive data Windows 2000/XP setup 62582 b with very long lines"- [targetUID: N/A]\n "nr-spa-1212.min_1_.js" has type "ASCII text with very long lines"- [targetUID: N/A]\n "2.6b
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.191): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	avanticom (Net ID: 00:02:6F:09:A3:B6)
2023-05-12 02:53:28	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"154.82.100.211:80"\n "154.82.100.211:443"\n "142.250.189.202:443"\ "Twitter" (Indicator: "dir "; File: "downloa dropped file "mm-logo_1_.svg" as clean (type is "SVG Scalable Vector Graphics image")\n Antivirus vendors marked dropped file "urlbloc u'Installation/Persistence', u'origin': u'API Call', u'identifier': u'api-243', u'name': u'Read files', u'attck_id_wiki': u'https://at
2023-05-12 02:56:54	IP Address	No	DNS Resolver	0	0	2	0	None	172.67.135.9
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	JBZD (Category: images) https://jbzd.com.pl/uzytkownik/login
2023-05-12 03:01:48	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	0	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	1	3	0	None	nginx
2023-05-12 03:13:42	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	0	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:27:54	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.138:8080
2023-05-12 02:44:03	Human Name	No	SpiderFoot UI	2	0	0	0	None	Patrick Pogoda
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	nore (Net ID: 00:01:E3:0B:96:F0)
2023-05-12 03:23:50	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.20:8080
2023-05-12	Physical Location	No	URLScan.io	0	0	1	0	None	DE

02:55:27									
2023-05-12 03:11:12	Physical Coordinates	No	OpenStreetMap	74	0	4	0	None	33.617190550339146,-111.90827887019054
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-opener-policy: same-origin
2023-05-12 02:53:19	Malicious IP Address	Yes	VirusTotal	0	1	3	0	None	VirusTotal [34.74.170.74] https://www.virustotal.com/en/ip-address/34.74.170.74/information/
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	6	0	None	permissions-policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope
2023-05-12 02:44:38	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Cloudflare
2023-05-12 02:45:29	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'SC', u'country_tld': u'.us', u'ip': u'104.196.30.220', u'currency_name': u'Dollar', u'currency': u'USD', u'country_
2023-05-12 03:09:50	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	82.170.74.34.bc.googleusercontent.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	200WMadison (Net ID: 00:01:21:30:9B:24)
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.166): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:24	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	HTTP/3
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Wayport_Access (Net ID: 00:14:6A:5B:53:91)
2023-05-12 03:00:58	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	01101101.github.io
2023-05-12 03:01:14	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.131): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Room 229 (Net ID: 00:02:2D:8B:9E:AE)
2023-05-12 03:41:56	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	mn2.tjdev.de
2023-05-12 02:44:13	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	1	2	0	None	github.io
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:2083
2023-05-12 02:55:25	Raw Data from RIRs	No	Google	1	0	2	0	None	{'webSearchUrl': u'https://www.google.com/search?q=site:www.ayhu.xyz&aq=t&oe=utf-8&client=firefox-a&ie=utf-8&rls=org.mozilla%3Aen-US%3
2023-05-12 03:43:57	URL (Form)	No	Page Information	0	0	4	0	None	https://ayhu.xyz/lol.html?__cf_chl_f_tk=74dxVi7F6QcjSPoVNIU8T6Tlsy4wHV.ukI6aTAD9tk4-1683861861-0-gaNycGzNCiU
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	cpanel.ayhu.xyz
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.81): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SWLFO (Net ID: 00:11:95:4C:CD:45)
2023-05-12 02:54:41	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H06QWFV48ACFBYY7E5EAJW1H Date: <REDACTED> Content-Length: 0
2023-05-12 02:54:20	Linked URL - External	No	Web Spider	0	0	3	0	None	https://www.cloudflare.com/5xx-error-landing?utm_source=errorcode_521&utm_campaign=nuke.battleb0t.xyz
2023-05-12 02:46:49	SSL Certificate - Issued to	No	SSL Certificate Analyzer	0	0	3	0	None	CN=*.cloudwaysapps.com

2023-05-12 02:54:20	Netblock IPv6 Membership	No	Censys	0	0	4	0	None	2600:1f18:2000::/35
2023-05-12 03:03:33	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:54:30	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Connection": "DISPLAY_UTF8", "Etag": "DISPLAY_UTF8", "Content_Type":
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:00:21:01)
2023-05-12 02:54:18	Web Content Type	No	Web Spider	0	0	4	0	None	text/css;charset=utf-8
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cross-origin-opener-policy: same-origin
2023-05-12 03:01:17	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.148): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet8FBA (Net ID: 00:01:36:5C:8F:B8)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Ziggo8BC690 (Net ID: 00:0C:F6:8B:C6:90)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	referrer-policy: same-origin
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	permissions-policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	21880a (Net ID: 00:02:2D:21:88:0A)
2023-05-12 03:00:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	curve25519-sha256@libssh.org
2023-05-12 02:52:35	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071', u'relev {u'category': u'Installation/Persistence', u'origin': u'API Call', u'identifier': u'api-243', u'name': u'Read files', u'attck_id_wiki' u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relev has type "MS Windows icon resource - 1 icon 32x32 32 bits/pixel"- [targetUID: N/A]\n "CE6PK5S8.txt" has type "ASCII text"- Location: [
2023-05-12 03:03:26	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:32:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.12:80
2023-05-12 02:51:54	Raw Data from RIRs	No	Hybrid Analysis	2	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "stats.g.doubleclick.net"\n "webrtc.github.io"\n "www.bigmarker.com"'}, {u'category': u'General', u'origin': u'File/Memory', u'identif "urlref_httpswww.bigmarker.comtaxadminThe-Inbound-Customer-Experiencebmid_5673cc9137db_bmid_type_member")'}, {u'category': u'Unusual C (Source: wallet-pre-stable.json, Indicator: "key.com")\n ""baseballmonkey.com"," (Source: wallet-pre-stable.json, Indicator: "key.com" data\\leveldb\\log"\n "msedge.exe" writes file "c:\\users\\%osuser%\\appdata\\local\\microsoft\\edge\\user data\\default\\7c516a82-27f
2023-05-12 02:44:11	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	2	1	1	0	None	github.com
2023-05-12 02:44:05	SSL Certificate Expiring	Yes	CertSpotter	0	0	1	0	None	2023-05-26 01:39:24
2023-05-12 03:09:26	Co-Hosted Site	No	SSL Certificate Analyzer	1	0	2	0	None	cdnjs.cloudflare.com
2023-05-12 03:09:28	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12	Internet Name	No	DNS Resolver	0	0	2	0	None	nuke.battleb0t.xyz

02:50:16									
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Tanuki.pl (Category: hobby) https://tanuki.pl/profil/login
2023-05-12 02:50:28	Raw Data from RIRs	No	GLEIF	0	0	3	0	None	[{u'attributes': {u'highlighting': u'C/O CENTRALNIC LTD', u'value': u'C/O CENTRALNIC LTD'}, u'type': u'autocomple
2023-05-12 02:45:06	Physical Location	No	ipapi.co	0	0	2	0	None	San Francisco, California, CA, United States, US
2023-05-12 02:46:38	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 7, u'descri [],nonGoogleScripts:["nonGooglePixels"],nonGoogleIframes:["nonGooglePixels"]},Mo={cl:["ecl"],customPixels:["customScripts","html"]," (image data JFIF standard 1.01 resolution (DPI) density 72x72 segment length 16 baseline precision 8 600x250 components 3"- [targetUID: "http://static.flowplayer.org/swf/expressinstall.swf,cachebusting:true},t"\n Pattern match: "https://cct.google/taggy/agent.js"\n Patt
2023-05-12 02:50:48	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', extension "png"'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Droppe "logo_1_.png" has type "PNG image data 329 x 88 8-bit/color RGBA non-interlaced"- [targetUID: N/A]\n "RecoveryStore._B6073E9B-EF99-11E Location: [%TEMP%\\Cab2E9E.tmp]- [targetUID: 00000000-00003584]\n "Cab2821.tmp" has type "data"- Location: [%TEMP%\\Cab2821.tmp]- [tar
2023-05-12 02:44:16	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:d7:56:4b:39:cd:63:5b:72:07:1e:ba:15:c9:f7:2c:e7:33 Signature Algorithm: sha256Wi f8:42:f9:9c:fc:f0:39:70:2a:ec:b3:e8:e8:27:a3:e2:22:80: 9f:b5:25:f6:b8:88:47:5f:86:6d:fa:80:87:2b:27:3e:0f:10: 6e:32:3f:e2:3c:74:e0:3c:
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.31): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Juggernaut (Net ID: 00:0C:41:D7:E4:AF)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Ricos Loft 5 (Net ID: 00:01:9F:34:7B:CC)
2023-05-12 03:09:45	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	136.97.148.34.bc.googleusercontent.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Patriots Win (Category: political) https://patriots.win/u/login/
2023-05-12 02:55:11	Open UDP Port	No	Censys	0	0	2	0	None	87.248.157.102:53
2023-05-12 03:12:52	Raw Data from RIRs	No	numverify	0	0	3	0	None	{u'international_format': u'+14805058800', u'local_format': u'4805058800', u'number': u'14805058800', u'valid': True, u'line_type': u'
2023-05-12 03:28:39	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.160:8443
2023-05-12 02:50:21	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 50, u'search_terms': [{u'id': u'host', u'value': u'185.199.108.153'}], u'result': [{u'environment_id': 160, u'job_id': u'64 u'sha256': u'2b8ddeb1ac7750da80502b1322e14c3de7bb618006fe7ddf37f47b9324d3bb67', u'type': None, u'type_short': u'url', u'size': 72}, {u Support)', u'threat_score': 100, u'verdict': u'malicious', u'submit_name': u'sample.url', u'sha256': u'be1d588c403275660b01eca90094a46 u'av_detect': u'0', u'environment_description': u'Windows 10 64 bit', u'threat_score': None, u'verdict': u'no specific threat', u'subm 23:19:06', u'vx_family': u'Phishing site', u'av_detect': u'60', u'environment_description': u'Windows 7 32 bit (HWP Support)', u'threa
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	NETGEAR (Net ID: 00:0B:7D:08:41:CB)
2023-05-12 03:32:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.13:80
2023-05-12 02:45:31	Raw Data from RIRs	No	PhishStats	0	0	2	0	None	[{u'page_text': u' ', u'domain': None, u'virus_total': None, u'n_times_seen_ip': None, u'abuse_contact': None, u'ip': u'185.199.110.15
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	x-timer: S1683860053.987504,VS0,VE2
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	2WIRE623 (Net ID: 00:00:85:F5:03:9F)
2023-05-12 02:46:01	Physical Location	No	AbstractAPI	1	0	3	0	None	North Charleston, South Carolina, 29415, United States, North America
2023-05-12 03:01:29	Web Server	No	Tool - WhatWeb	0	0	2	0	None	cloudflare

2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MobileInternet (Net ID: 00:02:B3:AE:E3:AC)
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:110
2023-05-12 03:00:58	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	01001101ck.github.io
2023-05-12 02:55:05	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Collaborative intelligence - Collaborative intelligence characterizes multi-agent, distributed systems where each agent, human or mach
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	WLAN (Net ID: 00:01:24:F3:FD:65)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	home (Net ID: 00:06:25:61:49:C4)
2023-05-12 03:31:27	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	6779e29dade44d91b5a12e78669866ac.protect@withheldforprivacy.com
2023-05-12 02:44:19	IPv6 Address	No	DNS Resolver	15	0	3	0	None	2600:1f18:2489:8200::c8
2023-05-12 03:03:55	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	eliaspinheironeto.github.io
2023-05-12 03:34:36	Netblock Membership	No	RIPE	5	0	3	0	None	45.131.109.0/24
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Disqus (Category: social) https://disqus.com/by/Altpapier/
2023-05-12 02:55:25	Social Media Presence	No	Social Network Identifier	0	0	4	0	None	Github: https://github.com/Altpapier/SkyHelperAPI/issues
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.224): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.43): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:38	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	zoom (Net ID: 00:01:38:3F:26:0C)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Teespring (Category: business) https://login.creator-spring.com
2023-05-12 03:00:58	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.96): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless2 (Net ID: 00:01:36:03:07:83)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MatrixEx Guest (Net ID: 00:01:21:26:42:50)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	TechAir (Net ID: 00:01:21:30:60:FE)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:62:CF:8A)
2023-05-12 02:54:14	HTTP Status Code	No	Web Spider	0	1	2	0	None	403
2023-05-12	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	2	0	None	netlify.app

02:44:15									
2023-05-12 02:47:25	Open TCP Port	No	Pulsedive	0	0	2	0	None	185.199.108.153:443
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:7B:56:15)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	7732 1224 (Net ID: 00:0F:CC:FD:AD:58)
2023-05-12 02:59:59	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	jhruby.web@gmail.com
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Computing websites
2023-05-12 03:03:40	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	472 (Net ID: 00:02:2D:C3:4A:5F)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom1372 (Net ID: 00:01:38:85:A8:E5)
2023-05-12 03:01:30	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.40): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:08:54	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.72
2023-05-12 02:55:25	Linked URL - Internal	No	Google	0	0	2	0	None	https://www.ayhu.xyz/
2023-05-12 03:24:19	Account on External Site	No	Account Finder	0	0	8	0	None	YouTube User (Category: video) https://www.youtube.com/user/baptistevauthey/about
2023-05-12 02:56:09	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:37:68:7b:1f:26:29:cd:a4:cc:95:52:df:e2:0a:12:6f:13 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: D9:CF: 21:21:50:dd:de:43:12:b9:29:89:20:37:79:64:39:a0:00:fa: b9:f2:d1:d6:97:d7:a4:ad:65:b2:7e:a9:68:2b:1e:77:25:f0: a5:6a:9b:71:2e:77:c5:cb:
2023-05-12 03:23:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.9:8443
2023-05-12 03:03:16	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	mail.ayhu.xyz
2023-05-12 03:24:21	Linked URL - Internal	No	Web Spider	5	0	2	0	None	https://ayhu.xyz/lol.html?__cf_chl_f_tk=74dxVi7F6QcjSPoVNIU8T6Tlsy4wHV.ukI6aTAD9tk4-1683861861-0-gaNycGzNCiU
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Allstate 2.4G (Net ID: 00:02:6F:F8:0A:40)
2023-05-12 03:00:49	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.67): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:49	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	3	0	None	cloudwaysapps.com
2023-05-12 03:00:51	Co-Hosted Site	No	HackerTarget	1	0	2	0	None	000.ovh
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	phi (Net ID: 00:06:B1:2D:D2:D1)
2023-05-12 02:57:44	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level_human': u'suspicious', u'capec_id': None, u'attck_id': u'T1005', u'relevance': 5, u'threat_level': 1, u'type': 2, u'des annotation=channel= --annotation=chromium-version=103.0.5060.53 "--annotation=exe=%PROGRAMFILES%\\(x86)\\Microsoft\\Edge\\Application\ u'minor_os_version': None, u'domains': [], u'extracted_files': [], u'type_short': []}]
2023-05-	HTTP	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect

12 02:54:54	Headers								
2023-05-12 02:56:50	Internet Name	No	DNS Resolver	0	0	2	0	None	funny.battleb0t.xyz
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Apple Network 079699 (Net ID: 00:02:2D:07:96:99)
2023-05-12 02:45:34	Email Gateway (DNS MX Records)	No	DNS Raw Records	0	0	1	0	None	route1.mx.cloudflare.net
2023-05-12 03:12:16	Co-Hosted Site - Domain Whois	No	Whois	3	0	5	0	None	Domain Name: ECASH-PAY.COM Registry Domain ID: 2607738264_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: h facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilatio Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: b7a6addeb33844c5b2bc9f82a64406e6.protect
2023-05-12 03:03:27	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2011-3389 https://nvd.nist.gov/vuln/detail/CVE-2011-3389 Score: 4.3 Description: The SSL protocol, as used in certain configuratio
2023-05-12 03:01:22	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.203): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	5526 7041 (Net ID: 00:00:C5:B5:6E:E5)
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.217): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:13:02	Blacklisted Affiliate IP Address	Yes	Threat Jammer	0	1	3	0	None	Threat Jammer - Risk score: 40 (MEDIUM) https://threatjammer.com/info/87.248.157.93
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Belkin_G_Wireless_ (Net ID: 00:1C:DF:B6:B6:F1)
2023-05-12 03:31:34	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@gmo.jp
2023-05-12 03:10:00	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	netherlands-18708423.mongo.ondigitalocean.com
2023-05-12 03:00:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.21): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BJNPSETUP (Net ID: 00:00:85:F3:6A:27)
2023-05-12 02:46:17	Physical Location	No	MetaDefender	0	0	3	0	None	San Francisco, United States
2023-05-12 03:32:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.15:80
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	02:30:14 (Net ID: 00:02:2D:03:B5:67)
2023-05-12 03:23:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.10:80
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:D1:F0:AA:05)
2023-05-12 03:12:41	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 5.9 Description: OpenVPN, when using a 64-bit block cipher, makes
2023-05-12 02:44:28	IP Address	No	DNS Resolver	73	0	2	0	None	34.148.97.127
2023-05-12 03:31:33	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namesilo.com
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=funny.battleb0t.xyz
2023-05-12 02:56:19	Netblock Membership	No	RIPE	0	0	2	0	None	188.114.97.0/24

2023-05-12 03:00:50	Co-Hosted Site	No	HackerTarget	1	0	2	0	None	0.dontkillmyapp.com
2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	104.21.71.14
2023-05-12 03:31:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	abuse@namecheap.com
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.117): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX551572EC4 (Net ID: 00:01:E3:57:2E:C4)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Wireless (Net ID: 00:09:5B:26:F3:E2)
2023-05-12 03:13:05	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0036labs.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:00:36	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	abuse@namecheap.com
2023-05-12 02:55:25	Social Media Presence	No	Social Network Identifier	0	0	4	0	None	Github: https://github.com/Altpapier/SkyHelperAPI/tree/master/examples
2023-05-12 02:45:44	Physical Location	No	AbstractAPI	1	0	2	0	None	Chantilly, Virginia, 20151, United States, North America
2023-05-12 02:54:19	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://fluid.battleb0t.xyz/logo.png
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:76:57:05)
2023-05-12 02:56:51	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 03:32:08	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.5:8443
2023-05-12 03:08:59	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.92
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Samsung Galaxy S8_5419 (Net ID: A2:C9:A0:CE:8F:DC)
2023-05-12 02:54:19	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://fluid.battleb0t.xyz/app_badge.png
2023-05-12 02:46:29	Netblock Membership	No	RIPE	5	0	3	0	None	64.226.80.0/20
2023-05-12 03:00:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.35): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:59:16	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 1, u'search_terms': [{u'id': u'host', u'value': u'188.114.96.1'}], u'result': [{u'environment_id': 100, u'job_id': u'631a66
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	3035 3464 (Net ID: 00:0F:CC:61:D8:F8)
2023-05-12 02:46:49	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 02:46:50	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Eijsbouts (Net ID: 00:01:E3:04:C3:19)
2023-05-	Internet	No	DNS Resolver	0	0	2	0	None	

12 02:44:42	Name								funny.battleb0t.xyz
2023-05-12 03:01:15	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.139): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.244): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:18	Internet Name	No	DNS Resolver	0	0	2	0	None	www.ayhu.xyz
2023-05-12 03:01:00	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.103): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Collaborative projects
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	RTL867x-ADSL (Net ID: 00:08:A1:C5:5A:46)
2023-05-12 02:54:54	Open TCP Port	No	Censys	0	0	2	0	None	2a06:98c1:3121::1:443
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Matrix (Net ID: 00:06:25:B5:6B:A4)
2023-05-12 03:01:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.238): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:32:02	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.2:443
2023-05-12 02:53:39	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-12T01:06:26.588Z", "ip": "185.199.108.153", "location_updated_at": "2023-05-11T02:22:47.949696Z", "autono 20T15:36:01.064188731Z"}, "devxchange.io": {"record_type": "A", "resolved_at": "2023-03-07T16:15:10.934357942Z"}, "www.2briley.com": { "www.mishamol.ru": {"record_type": "CNAME", "resolved_at": "2023-04-24T22:01:44.486211723Z"}, "alzhao.com": {"record_type": "CNAME", " "jianli.hogancn.com": {"record_type": "CNAME", "resolved_at": "2023-05-10T14:40:00.667151420Z"}, "prohlaseni.altair.blog": {"record_ty {"record_type": "CNAME", "resolved_at": "2023-05-03T20:11:29.826302413Z"}, "vishvak.com": {"record_type": "A", "resolved_at": "2023-05
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	200WMadison (Net ID: 00:01:21:30:9B:1A)
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00theway.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:44:16	Internet Name	No	DNS Resolver	4	0	2	0	None	www.battleb0t.xyz
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetFBC6 (Net ID: 00:01:36:5A:FB:C4)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	TraventHome (Net ID: 00:01:24:F0:1D:C3)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-mitigated: challenge
2023-05-12 03:00:13	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	webdisk.ayhu.xyz
2023-05-12 03:09:56	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	dgn.keyubu.com
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.15): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	social_msdn (Category: social) https://social.msdn.microsoft.com/profile/login
2023-05-	WiFi	No	Wigle.net	0	0	3	0	None	

12 03:18:51	Access Point Nearby								<no ssid> (Net ID: 00:02:2D:20:8C:1A)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:05:5D:ED:08:8A)
2023-05-12 03:38:36	Blacklisted Affiliate IP Address	Yes	UCEPROTECT	0	0	4	0	None	UCEPROTECT - Level 2 (some false positives) (46.101.229.68)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Twist Studio (Net ID: 00:02:2D:07:96:23)
2023-05-12 03:01:20	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.174): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	VEBNG (Net ID: 00:02:6F:75:9C:1E)
2023-05-12 02:58:57	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 0d:40:8d:d9:7c:a1:bd:4c:0d:06:c5:3f:c3:e9:2e:bc Signature Algorithm: sha256WithRSAE 84:de:17:e3:7f:b0:fd:4c:e4:f5:d9:c1:87:4a:b8:32:d6:97: 13:2d:ab:c3:d8:0c:ce:60:02:7a:3d:d5:8b:4f:9b:89:37:1e: 07:e8:65:4f:13:db:bc:f2:
2023-05-12 03:25:17	Internet Name	No	DNS Brute-forcer	0	0	1	0	None	www.ayhu.xyz
2023-05-12 02:54:16	Linked URL - Internal	No	Web Spider	3	0	2	0	None	https://oldfluid.battleb0t.xyz/
2023-05-12 02:51:40	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', pre-stable.json, Indicator: "key.com")\n ""order.firehousesubs.com"," (Source: wallet-checkout-eligible-sites-pre-stable.json, Indicat u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Cache\\Cache_Data\\data_1]- [targetUID: 00000000-00001340]\n "wallet-drawer.bund
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	remraz wd pro 2g (Net ID: 00:00:C0:01:7B:3F)
2023-05-12 03:24:22	Linked URL - Internal	No	Web Spider	1	0	2	0	None	https://ayhu.xyz/
2023-05-12 02:55:52	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'"\\Sessions\\1\\BaseNamedObjects\\UpdatingNewTabPageData"\n "Local\\InternetShortcutMutex"\n "IsoScope_b04_IE_EarlyTabStart_0xeac_Mu [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 00000000-00003088]\n "_87BE6 [%APPDATA%\\Microsoft\\Windows\\Cookies\\33YQJ8LX.txt]- [targetUID: 00000000-00002820]\n "favicon_3_.ico" has type "MS Windows icon re u'interesting': False, u'error_type': None, u'state': u'SUCCESS', u'entrypoint': None, u'mitre_attcks': [{u'parent': {u'attck_id_wiki'
2023-05-12 03:15:36	Physical Location	No	ipstack	0	0	3	0	None	Germany
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-experiments.github.io
2023-05-12 03:15:35	Web Content Language	No	Language Detector	0	0	3	0	None	English
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:04:09:0C)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	TEO Network Enterprise (Net ID: 00:01:24:F0:B7:E1)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Pornhub Users (Category: XXXPORNXXX) https://www.pornhub.com/users/ayhu
2023-05-12 02:44:27	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Patreon
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom67E1E4 (Net ID: 00:0C:F6:67:E1:E4)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:0E:F4:FC)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F2:68:C6)

2023-05-12 03:23:35	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.13:80
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Chili Bean Cafe (Net ID: 00:02:61:19:70:71)
2023-05-12 02:57:52	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 00000000-00006936), Spawned process "msedge.exe" with commandline "--type=renderer --disable-client-side-phishing-detection --displ .. Launches browser "msedge.exe" (UID: 00000000-00006928)\n Launches browser "msedge.exe" (UID: 00000000-00006236)\n Launches browser "ms {i[\'GoogleAnalyticsObject\']=r;i[r]=i[r]||function(){\n(i[r].q=i[r].q||[]).push(arguments)}\ni[r].l=1*new Date();a=s.createElement(o) [tabindex="-1"]:focus:not(:focus-visible){outline:0!important}hr{box-sizing:content-box;height:0;overflow:visible}h1\nh2\nh3\nh4\nh5\n
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	2	0	3	0	None	https://funny.battleb0t.xyz/images/withat_3.jpg
2023-05-12 02:44:22	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 02:53:49	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 02:44:14	IPv6 Address	No	DNS Resolver	16	0	1	0	None	2606:4700:3031::ac43:8709
2023-05-12 03:00:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	curve25519-sha256@libssh.org
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=nwapi2.battleb0t.xyz
2023-05-12 03:03:27	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:09:36	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	223.30.196.104.bc.googleusercontent.com
2023-05-12 03:09:59	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	inbox.clientify.net
2023-05-12 03:02:53	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 03:00:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.30): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet2C26 (Net ID: 00:01:36:4F:2C:24)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:3C:B8:8B)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 03:23:11	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.1:8080
2023-05-12 02:54:30	Open TCP Port	No	Censys	0	0	3	0	None	64.226.81.43:80
2023-05-12 02:45:58	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "35.186.254.174:443"\n "104.18.10.207:443"\n "104.26.8.175:443"\n "142.251.214.131:443"'}, {u'category': u'General', u'origin': u'Netw u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relev with very long lines"- [targetUID: N/A]\n "KFOlCnqEu92Fr1MmEU9fBBc9_1_.ttf" has type "TrueType Font data 18 tables 1st "GDEF" 8 names files', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'at
2023-05-12 02:54:13	Netblock IPv6 Membership	No	Censys	0	0	4	0	None	2606:4700:3030::/48
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	CORGI-2 (Net ID: 00:14:6C:7C:72:22)

2023-05-12 03:41:52	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["315"], "_encoding": {"Date": "DISPLAY_UTF8", "Content_Length": "DISPLAY_UTF8", "Connection": "DISPLAY_UTF8", "Con
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	4	0	None	Guernsey
2023-05-12 03:33:53	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	http://ns.adobe.com/xap/1.0/ XPhotoshop 3.0 Photo Booth ICC_PROFILE mntrRGB XYZ acspAPPL -appl bdscm vcgt 0ndin >chad 8bTRC aagg desc
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Bug and issue tracking software
2023-05-12 03:04:46	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2023-05-12 02:56:58	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 02:44:15	Web Technology	No	Tool - Wappalyzer	0	0	2	0	None	Express
2023-05-12 03:13:05	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [007-liang.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:55:02	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\!BrowserEmulation!SharedMemory!Mutex"\n "Local\\VERMGMTBlockListFileMutex"\n "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "\\Sessions\\1 [%APPDATA%\\Microsoft\\Windows\\Cookies\\LHCS4QQD.txt]- [targetUID: 00000000-00003336]\n "_1B7C6C58-B789-11ED-93A4-080027456658_.dat" u'Network Related', u'origin': u'File/Memory', u'identifier': u'string-102', u'name': u'Decrypted SSL network traffic', u'attck_id_wik <<M#>0%6wm&@MI:w.YW-]7.],d,^)E5y`>sVl[oNAp9![*/GTa<\'9leK1w@=->~Q05V8hv(xh@u_VOk6\'d\n2~rvH5}\n p;,Qj!zY U9Ra" V}ach\')&\'!Gm:", "mID#
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:02:DD:85:3E:34)
2023-05-12 02:46:49	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	3	0	None	C=US,ST=California,L=San Francisco,O=Netlify\, Inc,CN=*.netlify.app
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:80
2023-05-12 03:09:40	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	114.48.229.35.bc.googleusercontent.com
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-ray: 7c5f605fb97f4259-EWR
2023-05-12 02:57:23	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur BFE1-132B85B23C3A}"\n "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "Local\\ZonesCacheCounterMutex"\n "IsoScope_f1c_IESQMMUTEX_0_519"\n "IsoScope 10, u'threat_level': 0, u'type': 8, u'description': u'"Cab38F6.tmp" has type "Microsoft Cabinet archive data 61712 bytes 1 file"\n "57 [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\57C8EDB95DF3F0AD4EE2DC2B8CFD4157]- [targetUID: 00000000-00003868]\n "~DFC9E u'informative', u'capec_id': None, u'attck_id': u'T1573', u'relevance': 3, u'threat_level': 0, u'type': 2, u'description': u'"GET /fav
2023-05-12 03:08:51	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.121
2023-05-12 02:44:28	Co-Hosted Site - Domain Name	No	DNS Resolver	2	0	2	0	None	cloudflaressl.com
2023-05-12 02:44:21	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS RSA SHA256 2020 CA1
2023-05-12 03:08:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.77
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	6	0	None	referrer-policy: same-origin
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Trello (Category: social) https://trello.com/ayhu
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.157): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:37	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	registrar-abuse@cloudflare.com
2023-05-	HTTP	No	Web Spider	1	0	2	0	None	

12 02:54:22	Headers								{"content-encoding": "gzip", "transfer-encoding": "chunked", "vary": "Accept-Encoding", "server": "nginx", "connection": "keep-alive",
2023-05-12 03:01:49	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.110.153:80
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	ArcorWirelessLAN3mKh (Net ID: 00:01:E3:57:D5:DD)
2023-05-12 02:44:26	Internet Name	No	DNS Resolver	0	0	2	0	None	battleb0t.xyz
2023-05-12 02:59:45	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: TAYHU.XYZ Registry Domain ID: D286586654-CNIC Registrar WHOIS Server: whois.cloudflare.com Registrar URL: http://cloudfla not to store or reproduce this data in any way, (3) not to use any high-volume, automated, electronic processes to obtain data from th https://domaincontact.cloudflareregistrar.com/tayhu.xyz Registry Billing ID: Billing Name: DATA REDACTED Billing Organization: DATA RE
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-ray: 7c5f8c5eeb1a42bf-EWR
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	6562 7451 (Net ID: 00:00:C5:D7:2F:EC)
2023-05-12 02:44:15	Internet Name	No	DNS Resolver	2	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	U+ACN (Net ID: 00:02:A8:81:E3:26)
2023-05-12 03:04:07	Malicious IP on Same Subnet	Yes	Greensnow	0	0	4	0	None	greensnow.co [165.232.112.0/20] https://blocklist.greensnow.co/greensnow.txt
2023-05-12 02:55:01	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 02:54:14	Web Content Type	No	Web Spider	0	0	2	0	None	text/html
2023-05-12 02:52:31	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:4e:82:1a:86:ae:7d:8a:39:3c:25:24:c6:46:df:b3:a2:f4 Signature Algorithm: sha256Wi 70:c6:b9:f9:5c:8e:b6:f6:c9:24:b6:77:0f:70:91:82:5f:ac: 56:6c:08:4c:23:f5:3c:83:00:83:99:51:65:02:cf:77:c0:85: ba:ab:a0:9d:95:f2:a4:6b:
2023-05-12 02:56:57	Internet Name	No	DNS Resolver	0	0	4	0	None	kekw.battleb0t.xyz
2023-05-12 02:48:16	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': u'Windows Gui', u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [{u'file_proces u'file_process_sha256': u'3fba8f17cfa66d0984dd5016c50e2b7f323a37f213a8c67f04c27d3be67dc77a', u'address': u'00020000', u'verdict': u'ma a parameter VerQueryValueW (UID: 00000000-00002400)\n "YuzuUpdater.exe" called "GetProcAddress" with a parameter InitializeCriticalSec "YuzuUpdater.exe" failed to load missing module "%WINDIR%\\Microsoft.Net\\assembly\\GAC_MSIL\\System.Windows.Forms\\v4.0_4.0.0.0__b77a "YuzuUpdater.exe" failed to load missing module "%WINDIR%\\Microsoft.NET\\Framework\\v4.0.30319\\CRYPT32.dll" - [base:0; Status:c00001
2023-05-12 02:44:17	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:50c0:8000::153
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	RowanLofts (Net ID: 00:02:2A:F0:3C:C7)
2023-05-12 03:07:25	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	binkyandwooby (Net ID: 00:01:24:F0:A5:3F)
2023-05-12 02:46:09	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'identifier': u'network-1', u'name': u'Contacts server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_lev url=https://virtualvacation.us/multiplayer&text=Play City Guesser Multiplayer with me. You have to guess the location from the shown v u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', 8abc-477a-bbc1-d1a29a1132a8.tmp" has type "gzip compressed data from FAT filesystem (MS-DOS OS/2 NT) original size modulo 2^32 188574"

2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	x-nf-request-id: 01H06Y2WDQHNHJAAXWWVJBZZ5B
2023-05-12 02:44:18	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 03:08:51	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.122
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Ziggo13797 (Net ID: 00:04:E2:D8:5E:98)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=lshBmhR4GSBYjKDefqIGkygGexG96Rixvbfv4WfP5q9iY7bD%2BJ8d%2
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ORANJA (Net ID: 00:01:24:F4:53:15)
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	001cat.github.io
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.208): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:22	HTTP Headers	No	Web Spider	8	0	3	0	None	{"cf-access-domain": "panel.battleb0t.xyz", "cf-ray": "7c5f606c5dec334e-EWR", "x-content-type-options": "nosniff", "content-security-p
2023-05-12 02:54:27	Open TCP Port Banner	No	Censys	0	0	4	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H05GB7HXKZRW69FWMYAA1JFJ Date: <REDACTED> Content-Length: 0
2023-05-12 02:46:40	Malicious IP Address	Yes	Fraudguard	0	1	2	0	None	abuse_tracker (risk level: 4) [185.199.108.153]
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	WTH (Net ID: 00:02:6F:21:EA:89)
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha1-etm@openssh.com
2023-05-12 03:08:52	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.130
2023-05-12 02:57:19	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis "\\Sessions\\1\\BaseNamedObjects\\Local\\VERMGMTBlockListFileMutex"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_FILEMAPSWITCH_ [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776]- [targe application/xhtml+xml, */*\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept- caf16699abb61a32fc60f7e822749eeb2f93bae1d29c037c3741a62e3b99d03f (AV positives: 8/73 scanned on 07/28/2022 23:29:37)\n File SHA256: 16
2023-05-12 02:56:28	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'description': u'"\\Sessions\\1\\BaseNamedObjects\\IsoScope_dd0_IESQMMUTEX_0_519"\n "Local\\InternetShortcutMutex"\n "Local\\VERMGMTB "6BADA8974A10C4BD62CC921D13E43B18_28DEA62A0AE77228DD387E155AD0BA27" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptne [targetUID: N/A]\n "~DF73B96DA26F860992.TMP" has type "data"- Location: [%TEMP%\\~DF73B96DA26F860992.TMP]- [targetUID: 00000000-000035 d;c=document;b=b||c;if(b.querySelectorAll&&b.querySelector)b=b.querySelectorAll(".yt-player");else if(b.getElementsByClassName){var e=
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	StreamElements (Category: finance) https://streamelements.com/login
2023-05-12 02:54:21	HTTP Status Code	No	Web Spider	0	0	5	0	None	200
2023-05-12 03:03:33	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 02:44:14	IPv6 Address	No	DNS Resolver	15	0	1	0	None	2606:50c0:8001::153
2023-05-12 03:13:04	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [000hen.github.io] https://www.openphish.com/feed.txt
2023-05-12	WiFi Access	No	Wigle.net	0	0	4	0	None	CableWiFi (Net ID: 00:0D:67:65:A6:FC)

03:18:54	Point Nearby								
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	C=US,ST=California,L=San Francisco,O=Cloudflare\, Inc.,CN=sni.cloudflaressl.com
2023-05-12 02:52:24	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.111.133:443
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Andrea Schwartz Gallery (Net ID: 00:01:9F:3D:4F:68)
2023-05-12 03:33:36	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	PLTE$ kyhNlC2D kShPAJ esyS_S@? txkST`ANdNO rXYuPYXHR XajGc dzvRt IDATx :7MV- '@crrX QK>@W vWP`Z tmv1q XEFi" 4@1hb a'c:3 2FRB> LHiiB YF
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HinaJasmin (Net ID: 00:01:E3:08:AE:FB)
2023-05-12 03:00:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.44): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	3Com (Net ID: 00:14:7C:52:C6:E4)
2023-05-12 03:00:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	sntrup761x25519-sha512@openssh.com
2023-05-12 03:00:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	aes128-gcm@openssh.com
2023-05-12 03:00:54	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	007ayong.github.io
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	DNA (Net ID: 00:01:71:0B:C5:CC)
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	GitLab - GitLab Inc. is an open-core company that operates GitLab, a DevOps software package which can develop, secure, and operate so
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	cpcontacts.ayhu.xyz
2023-05-12 02:54:30	Software Used	Yes	Censys	0	0	3	0	None	nginx nginx
2023-05-12 02:55:21	Software Used	Yes	Censys	0	0	3	0	None	CaddyServer Caddy
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:09:26	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 09:6b:82:e9:73:99:94:ba:fd:55:b0:21:db:c7:c8:bf Signature Algorithm: ecdsa-with-SHA : 35:CF:19:1B:BF:B1:6C:57:BF:0F:AD:4C:6D:42:CB:BB: B6:27:20:26:51:EA:3F:E1:2A:EF:A8:03:C3:3B:D6:4C Timestamp : Aug 3 19:12:00.017 2022
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Blogspot (Category: blog) http://ayhu.blogspot.com
2023-05-12 02:54:13	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://kekw.battleb0t.xyz
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	DCO (Net ID: 00:0C:41:66:5E:C3)
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:01:24:F0:62:49)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Sobe5 (Net ID: 00:14:C1:15:47:B3)
2023-05-	WiFi	No	Wigle.net	0	0	5	0	None	xfinitywifi (Net ID: 00:0D:67:2F:5E:C6)

12 03:18:53	Access Point Nearby								
2023-05-12 03:03:30	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:38:37	Blacklisted Affiliate IP Address	Yes	UCEPROTECT	0	0	4	0	None	UCEPROTECT - Level 2 (some false positives) (207.154.228.159)
2023-05-12 02:45:35	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	brett.ns.cloudflare.com
2023-05-12 03:03:22	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:54:44	Open TCP Port	No	Censys	0	0	3	0	None	35.229.48.116:80
2023-05-12 02:54:17	Open TCP Port	No	Censys	0	0	4	0	None	2606:4700:3037::6815:470e:443
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX55157320C (Net ID: 00:01:E3:57:32:0C)
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet55FA (Net ID: 00:01:36:59:55:F8)
2023-05-12 02:58:40	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'description': u'Antivirus vendors marked dropped file "urlblockindex_1_.bin" as clean (type is "data")\n Antivirus vendors marked dr [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442]- [targe "Microsoft Cabinet archive data 4817 bytes 1 file"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\57C8EDB95DF3 "Wk(Ak(j)4FFB".....g}n~le.g\ng\ng\n)F F F!..I....Dt9vvvvvwxiuNG!<F%>F$_4b1xc0c0c01F$FF[.....imnnnnon\'KF\'sE)E\'F&[8^6p_5_4_4_4,E(E(
2023-05-12 02:45:54	Physical Coordinates	No	AbstractAPI	94	0	4	0	None	39.0469, -77.4903
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.35): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:12:12	Co-Hosted Site - Domain Whois	No	Whois	3	0	4	0	None	Domain Name: scoop.sh Registry Domain ID: 688a2dc7e3804150a8a7bd65025fc26d-DONUTS Registrar WHOIS Server: whois.gandi.net Registrar UR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please quer queries for a period of time to prevent disruption of Whois service access. Abuse of the Whois system through data mining is mitigated Phone: REDACTED FOR PRIVACY Registrant Phone Ext: Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: Registrant Email: 09e034915 courts. For additional information, please contact us via the following form: https://www.gandi.net/support/contacter/mail/
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.231): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:27	Raw Data from RIRs	No	URLScan.io	1	0	1	0	None	[{u'sort': [1679937961810, u'be713cda-cf3f-49bd-91b6-e8517dc017bf'], u'task': {u'domain': u'kekw.battleb0t.xyz', u'uuid': u'be713cda-c [u'https://phish.report', u'@phish_report'], u'url': u'http://kekw.battleb0t.xyz/', u'visibility': u'public', u'time': u'2023-03-11T22 u'country': u'DE', u'redirected': u'https-only', u'apexDomain': u'battleb0t.xyz', u'tlsAgeDays': 43, u'asn': u'AS14061'}}]
2023-05-12 03:31:30	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	6	0	None	abuse@nicproxy.com
2023-05-12 03:00:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	aes128-gcm@openssh.com
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:00:21:01)
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	PHP 7.4.33
2023-05-12 03:09:44	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	129.97.148.34.bc.googleusercontent.com
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.120): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.207): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12	Affiliate Description	No	DuckDuckGo	0	0	5	0	None	Information technology companies of England

03:12:10	- Category								
2023-05-12 03:11:19	Raw Data from RIRs	No	AbstractAPI	0	0	2	0	None	{u'city': u'Bursa', u'security': {u'is_vpn': False}, u'city_geoname_id': 750269, u'region_geoname_id': 750268, u'country': u'Turkey',
2023-05-12 02:44:15	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3037::6815:470e
2023-05-12 02:54:27	BGP AS Membership	No	Censys	0	0	4	0	None	14618
2023-05-12 02:55:15	Software Used	Yes	Censys	0	0	3	0	None	nginx nginx 1.18.0
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CableWiFi (Net ID: 00:0D:67:37:7A:7B)
2023-05-12 03:02:26	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Cloudflare
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	BIGO Live (Category: gaming) https://www.bigo.tv/user/ayshoo
2023-05-12 02:54:44	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H06KNWSV7RTZ7MSA7BNCK843 Date: <REDACTED> Content-Length: 0
2023-05-12 02:50:27	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'"59e3fd97d0784951aaf980d5dbb23a79.events.ubembed.com"\n "59e3fd97d0784951aaf980d5dbb23a79.js.ubembed.com"\n "59e3fd97d0784951aaf980d "arvest.com")\n ""highkey.com"," (Source: wallet-checkout-eligible-sites-pre-stable.json, Indicator: "key.com")\n ""mandalascrubs.com" stable.json, Indicator: "ubs.com")'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0' Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\EdgeCoupons\\coupons_data.db\\000009.log]- [targetUID: 00000000-000058
2023-05-12 02:44:12	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	adrilankha (Net ID: 00:06:25:66:F5:F2)
2023-05-12 03:09:43	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	125.97.148.34.bc.googleusercontent.com
2023-05-12 03:00:50	Co-Hosted Site	No	HackerTarget	1	0	2	0	None	0.church
2023-05-12 03:13:09	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [01001101ck.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CarlsJr_Wireless (Net ID: 00:0C:42:6B:5A:82)
2023-05-12 02:58:30	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level': 0, u'type': 8, u'description': u'Antivirus vendors marked dropped file "urlblockindex_1_.bin" as clean (type is "data 62932 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"\n "Cab1512.tmp" has type "Microsoft Cabinet archiv has type "Web Open Font Format TrueType length 51152 version 1.1"- [targetUID: N/A]\n "_692F3876-7577-11ED-BDC3-080027DA0E36_.dat" has [], u'attck_id': u'T1071.004', u'malicious_identifiers': [], u'malicious_identifiers_count': 0, u'technique': u'DNS', u'informative_id
2023-05-12 02:44:08	Internet Name	No	CertSpotter	33	0	1	0	None	funny.battleb0t.xyz
2023-05-12 03:00:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.28): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:25	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 02:54:20	HTTP Headers	No	Web Spider	2	0	2	0	None	{"content-length": "1200", "content-encoding": "gzip", "accept-ranges": "bytes", "strict-transport-security": "max-age=31536000", "var
2023-05-12 02:54:34	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	rsi (Category: gaming) https://robertsspaceindustries.com/citizens/ayhu
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	mail.ayhu.xyz
2023-05-12	Raw Data from RIRs	No	Tool - WhatWeb	1	0	2	0	None	[{u'request_config': {u'headers': {u'User-Agent': u'Mozilla/5.0'}}, u'target': u'http://nwapi2.battleb0t.xyz', u'http_status': 301, u'

03:01:26									
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	Snapchat Stories (Category: social) https://story.snapchat.com/s/battleb0t
2023-05-12 02:44:09	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Google Trust Services LLC,CN=GTS CA 1P5
2023-05-12 03:24:22	HTTP Status Code	No	Web Spider	0	0	4	0	None	403
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	2	0	None	permissions-policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope
2023-05-12 02:44:12	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Nginx
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	AOSS-DESKTOP1-47290 (Net ID: 00:00:5C:81:7F:C0)
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.244): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Maingau (Net ID: 00:02:2D:66:97:3D)
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.253): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:30	Physical Location	No	Fraudguard	0	0	3	0	None	Germany, Hesse, Frankfurt am Main
2023-05-12 02:44:13	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	1	2	0	None	githubusercontent.com
2023-05-12 03:33:45	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	IDATx ? `sm b"0N9 3@N:vn yj4BZu:- pqmVU hEC0s c@ h' 6FcPkh4 2:Eu` IDAT nfwPH jniEDkf 9uCGxN MWFGv '!hXQf 6WoW' hRoWW 68ZQ$ 8Ro7Tr 2j3y
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	DONNYMC (Net ID: 00:09:5B:CF:7C:14)
2023-05-12 02:44:44	Software Used	Yes	Tool - Wappalyzer	0	0	3	0	None	Cloudflare
2023-05-12 03:01:20	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.177): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:14	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.133): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.224): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Tacklebox AirNet (Net ID: 00:02:2D:0D:4F:2B)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	hollyhome (Net ID: 00:04:5A:FD:2E:C9)
2023-05-12 03:08:47	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.219
2023-05-12 03:03:34	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:54:15	Linked URL - External	No	Web Spider	2	0	3	0	None	https://github.com/Altpapier/SkyHelperAPI/tree/master/examples
2023-05-12 02:44:10	Co-Hosted Site -	No	SSL Certificate Analyzer	2	1	1	0	None	githubusercontent.com

	Domain Name								
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	MariaDB MariaDB 10.5.19
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Gettr (Category: social) https://gettr.com/user/login
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MatrixEx BYOD (Net ID: 00:01:21:26:42:61)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	P2d8T7f2d$ (Net ID: 00:18:0A:DF:7D:60)
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.216): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:04:E2:FB:95:10)
2023-05-12 02:53:23	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'File/Memory', u'identifier': u'string-10', u'name': u'Found a reference to a known community page', u'attck_id_wiki': None, u'threat pre-stable.json, Indicator: "ubs.com")\n ""6whiskey.com"," (Source: wallet-pre-stable.json, Indicator: "key.com")\n ""99centsubs.com", u'name': u'Dropped files', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'ca "load_statistics.db" has type "SQLite 3.x database last written using SQLite version 3039003"- Location: [%LOCALAPPDATA%\\Microsoft\\E
2023-05-12 02:56:18	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"keyzstoreoracle.org"'}, {u'category': u'General None, u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 8, u'description': u'"urlblockindex_1_.bin" has type "data"- [t "data"- Location: [%TEMP%\\~DF4BEE67FCFB6399A9.TMP]- [targetUID: 00000000-00003516]\n "57C8EDB95DF3F0AD4EE2DC2B8CFD4157" has type "Mic max-age=0, no-cache, no-store\nPragma: no-cache\nDate: Sat, 15 Oct 2022 06:47:48 GMT\nConnection: keep-alive\nStrict-Transport-Securit
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	logitec-a197d9 (Net ID: 00:01:8E:A1:97:D8)
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.19): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:41	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	TSMD 5 (Net ID: 00:02:6F:FD:8B:6F)
2023-05-12 03:32:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.11:8443
2023-05-12 03:01:31	Raw Data from RIRs	No	Tool - WhatWeb	1	0	2	0	None	[{u'request_config': {u'headers': {u'User-Agent': u'Mozilla/5.0'}}, u'target': u'http://funny.battleb0t.xyz', u'http_status': 301, u'p
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-cache: MISS
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet4862 (Net ID: 00:01:36:5B:48:60)
2023-05-12 03:09:30	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:15:35	Web Content Language	No	Language Detector	0	0	3	0	None	English
2023-05-12 03:12:55	Raw Data from RIRs	No	numverify	0	0	3	0	None	{u'international_format': u'+14806242598', u'local_format': u'4806242598', u'number': u'14806242598', u'valid': True, u'line_type': u'
2023-05-12 03:24:30	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	Network Solutions, LLC
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:0C:41:A1:42:A6)

2023-05-12 02:58:21	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'"\\Sessions\\1\\BaseNamedObjects\\Local\\!BrowserEmulation!SharedMemory!Mutex"\n "Local\\InternetShortcutMutex"\n "{5312EE61-79E3-4A "MRKVEKYP.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\MRKVEKYP.txt]- [targetUID: 00000000-00001592]'}, {u'category': u'I "index_1_.webmanifest" has type "JSON data"- [targetUID: N/A]\n "RecoveryStore._D73640FF-8192-11ED-8425-080027616BD6_.dat" has type "C (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nHost: hui-zhou.netlify.app\nDNT: 1\nConnection: Keep-Alive"\n "HTTP/1.1 404 Not Fou
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.164): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:53:02	Raw Data from RIRs	No	Tool - WAFW00F	1	0	2	0	None	[{"url": "https://nwapi.battleb0t.xyz", "firewall": "Cloudflare", "detected": true, "manufacturer": "Cloudflare Inc."}, {"url": "https
2023-05-12 03:03:59	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	akashpmani.github.io
2023-05-12 02:54:22	HTTP Headers	No	Web Spider	10	0	2	0	None	{"content-encoding": "gzip", "nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "referrer-policy": "same-o
2023-05-12 02:54:15	Linked URL - External	No	Web Spider	0	0	3	0	None	https://www.patreon.com/skyhelper
2023-05-12 02:54:54	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-11T12:33:03.766Z", "ip": "2a06:98c1:3121::1", "location_updated_at": "2023-05-06T23:05:13.627091Z", "auto "askapkmod.com": {"record_type": "AAAA", "resolved_at": "2022-12-26T12:52:46.077237913Z"}, "gbdfdm.cn": {"record_type": "AAAA", "resol cgi/styles/main.css\" />\n\n\n<script>\n(function(){if(document.addEventListener&&window.XMLHttpRequest&&JSON&&JSON.stringify){var e=f id=\"what-happened-section\" class=\"w-1/2 md:w-full\">\n <h2 class=\"text-3xl leading-tight font-normal mb-4 text-black-dark antialia ip\">2620:96:e000:b0cc:e:2:2:7\n <span class=\"cf-footer-separator sm:hidden\">•\n \n <span class=\"cf-foote
2023-05-12 02:53:06	Raw Data from RIRs	No	Tool - WAFW00F	1	0	2	0	None	[{"url": "https://nuke.battleb0t.xyz", "firewall": "Cloudflare", "detected": true, "manufacturer": "Cloudflare Inc."}, {"url": "https:
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	lichess (Category: gaming) https://lichess.org/@/login
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 02:45:59	Physical Location	No	AbstractAPI	0	0	3	0	None	Chicago, Illinois, 60666, United States, North America
2023-05-12 02:54:15	Web Content	No	Web Spider	4	0	2	0	None	<!DOCTYPE html> <html> <head> <meta charset="utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0" /> <link header) </td> </tr> <tr> <td>403</td> <td>The provided token does not exist</td> </tr> <tr> <td>404</td> <td>There is no player with t <code>GET</code> /v1/items/:user</h3> <h3 id="get-v1profileuserprofileitems"><code>GET</code> /v1/items/:user/:profile</h3> <h3 id="ge
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	BIGO Live (Category: gaming) https://www.bigo.tv/user/ayhu
2023-05-12 03:32:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.12:443
2023-05-12 03:15:36	Physical Location	No	ipstack	0	0	3	0	None	United States
2023-05-12 02:50:50	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', "PNG image data 329 x 88 8-bit/color RGBA non-interlaced" and extension "png"'}, {u'category': u'Installation/Persistence', u'origin': [targetUID: 00000000-00003172]\n "~DF840616A128F2225A.TMP" has type "data"- Location: [%TEMP%\\~DF840616A128F2225A.TMP]- [targetUID: 0 [targetUID: N/A]\n "PMD3JQRI.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\PMD3JQRI.txt]- [targetUID:
2023-05-12 03:09:49	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	78.170.74.34.bc.googleusercontent.com
2023-05-12 02:55:28	BGP AS Membership	No	URLScan.io	0	0	2	0	None	14061
2023-05-12 03:00:32	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	contact@millcityloans.com
2023-05-12 02:54:16	Web Content Type	No	Web Spider	0	0	2	0	None	text/html;charset=utf-8
2023-05-12 03:03:36	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	ConnectionPoint (Net ID: 00:01:E3:0B:31:F9)

2023-05-12 03:28:39	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.160:443
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 03:12:12	Co-Hosted Site - Domain Whois	No	Whois	0	0	4	0	None	Domain: ply.gg Domain Status: Active Transfer Prohibited by Registrar Registrant: Developed Methods LLC Registrar: NameCheap, Inc (htt
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Capsmanagement (Net ID: 00:01:21:1C:AD:50)
2023-05-12 03:33:13	Web Content Language	No	Language Detector	0	0	4	0	None	English
2023-05-12 02:44:14	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	1	2	0	None	github.com
2023-05-12 02:55:05	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom1330 (Net ID: 00:01:38:92:E5:07)
2023-05-12 03:31:33	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	pw-55286b4dad8e2523890cab5484722bf1@privacyguardian.org
2023-05-12 02:51:26	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"185.199.108.153:80"\n "185.199.108.153:443"\n "156.146.53.12:443"\ 16 progressive precision 8 1280x537 components 3" and extension "jpg"\n "mobile-0819_1_.jpg" has type "JPEG image data JFIF standard 1 [targetUID: N/A]\n "~DFEC2B4905E636D1C9.TMP" has type "data"- Location: [%TEMP%\\~DFEC2B4905E636D1C9.TMP]- [targetUID: 00000000-000031 "newnetflix_1_.htm" has type "HTML document ASCII text with CRLF line terminators"- [targetUID: N/A]\n "J560SO9O.txt" has type "ASCII
2023-05-12 03:00:25	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	hmac-sha2-512-etm@openssh.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Geocaching (Category: social) https://www.geocaching.com/p/?u=login
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	BJNPSETUP (Net ID: 00:00:85:F4:1C:9A)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	ArmorGames (Category: gaming) https://armorgames.com/user/login
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	art_vacation2.4 (Net ID: 00:01:9F:30:06:78)
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Collaborative projects
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	4	0	None	13335
2023-05-12 03:08:47	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.223
2023-05-12 02:45:10	Linked URL - Internal	No	Hybrid Analysis	4	0	1	0	None	http://kekw.battleb0t.xyz/jar
2023-05-12 03:27:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.128:8443
2023-05-12 03:00:32	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	jcorrea@mottomortgage.com
2023-05-12 02:57:57	SSL Certificate - Raw Data	No	Certificate Transparency	7	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:89:7c:23:d8:89:20:d1:c5:b3:ae:30:91:44:3a:23:81:b8 Signature Algorithm: sha256Wi 26:b6:b9:a7:2f:e5:4c:52:ac:47:f6:61:c0:02:b0:ef:8e:c3: a6:d3:f1:ec:92:c0:a2:e1:7b:19:b2:3a:4e:87:84:15:a6:4c: 8a:85:bd:36:13:13:c4:da:

2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	WLAN (Net ID: 00:01:24:F0:8C:65)
2023-05-12 02:44:14	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	pics.battleb0t.xyz:443
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	default (Net ID: 00:01:24:F0:49:B4)
2023-05-12 03:10:24	Blacklisted IP Address	Yes	Threat Jammer	0	1	2	0	None	Threat Jammer - Risk score: 40 (MEDIUM) https://threatjammer.com/info/188.114.97.1
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Poshmark (Category: shopping) https://poshmark.com/closet/login
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MatrixEx Guest (Net ID: 00:01:21:26:54:B0)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	6dgs-guest (Net ID: 00:06:B1:28:66:5F)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wavelan network (Net ID: 00:02:2D:0E:29:C9)
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/ein_1.png
2023-05-12 03:00:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.11): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	XVIDEOS-profiles (Category: XXXPORNXXX) https://www.xvideos.com/profiles/login
2023-05-12 03:32:00	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.1:8443
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:0C:41:D7:22:4A)
2023-05-12 03:09:30	Co-Hosted Site - Domain Name	No	DNS Resolver	2	0	3	0	None	rathook.cc
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	default (Net ID: 00:00:94:CB:58:1E)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	dilara (Net ID: 00:12:BF:56:97:E9)
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Wikipedia (Category: news) https://en.wikipedia.org/wiki/User:Altpapier
2023-05-12 03:22:52	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.1:443
2023-05-12 03:41:52	BGP AS Membership	No	Censys	0	0	3	0	None	44486
2023-05-12 03:00:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.20): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:13:03	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0000magda0000.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:46:04	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'city': u'North Charleston', u'security': {u'is_vpn': False}, u'city_geoname_id': 4589387, u'region_geoname_id': 4597040, u'country'
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:07:40:61:40:4D)
2023-05-12 02:45:47	Physical Coordinates	No	AbstractAPI	0	0	2	0	None	37.751, -97.822
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Tenor (Category: images) https://tenor.com/users/ayhu

2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Hangar6 (Net ID: 00:02:6F:E9:36:AC)
2023-05-12 03:18:53	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image ExifOffset': (0x8769) Long=90 @ 66, 'EXIF ComponentsConfiguration': (0x9101) Undefined=YCbCr @ 112, 'Image YCbCrPositioning':
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	opensource (Category: tech) https://opensource.com/users/login
2023-05-12 03:03:59	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	james-gamboa.github.io
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	6565 7241 (Net ID: 00:00:C5:D7:5E:64)
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	3	0	None	Netlify\, Inc
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.156): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	ConnectionPoint (Net ID: 00:01:E3:05:13:41)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	^E^W^B^H^Y^B^I^L^G^R^_^W^H^S^^ (Net ID: 00:02:2D:6D:79:1B)
2023-05-12 02:47:44	Open TCP Port	No	Pulsedive	0	0	3	0	None	34.148.97.127:443
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom (Net ID: 00:0C:F6:43:34:F0)
2023-05-12 03:01:24	Raw Data from RIRs	No	Tool - WhatWeb	0	0	1	0	None	[{u'request_config': {u'headers': {u'User-Agent': u'Mozilla/5.0'}}, u'target': u'http://ayhu.xyz', u'http_status': 301, u'plugins': {u
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless (Net ID: 00:01:36:07:56:EF)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-F7C2 (Net ID: 00:1D:D2:C6:F7:C0)
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Blogspot (Category: blog) http://ayshoo.blogspot.com
2023-05-12 03:18:06	URL (Form)	No	Page Information	0	0	5	0	None	https://www.ayhu.xyz/?__cf_chl_f_tk=JtV8r0GkxGajl1GKjCT6mPEPAroD8NWzOwVMv5NMEkM-1683860062-0-gaNycGzNCiU
2023-05-12 02:45:34	Email Gateway (DNS MX Records)	No	DNS Raw Records	0	0	1	0	None	route3.mx.cloudflare.net
2023-05-12 03:24:49	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 02:54:00	Netblock Membership	No	Censys	0	0	2	0	None	104.21.0.0/20
2023-05-12 02:54:19	HTTP Headers	No	Web Spider	6	0	4	0	None	{"nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "alt-svc": "h3=\":443\"; ma=86400, h3-29=\":443\"; ma=
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_ipad (Net ID: 00:0C:E6:08:05:05)
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.219): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:48:43	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:9d:c5:27:de:ee:41:17:4e:89:34:e6:9d:87:79:d7:50:31 Signature Algorithm: sha256Wi fb:6d:d3:d4:7a:d8:73:24:57:b7:c5:32:e7:93:1d:78:bc:d7: ff:72:e3:d1:10:bf:79:59:e7:40:ad:5a:05:ec:c7:2b:28:99: c1:ed:47:65:dd:b0:d9:8c:
2023-05-12 03:00:57	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.95): Search Engine Last Activity: 0 days ago Threat Level: 29

2023-05-12 02:44:28	Affiliate - Internet Name	No	DNS Resolver	0	0	2	0	None	frabjous-lebkuchen-324004.netlify.app
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-embedder-policy: require-corp
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Beens Gast (Net ID: 00:01:21:1F:B1:A1)
2023-05-12 02:55:01	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:59:54	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	robert@broofa.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	L1NKSYS (Net ID: 00:0C:41:F6:2E:FE)
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:8080
2023-05-12 03:13:01	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-14n.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	APC (Net ID: 00:09:5B:4F:F1:CA)
2023-05-12 02:44:22	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CWhite-Aireconsole (Net ID: 00:02:0C:09:99:E0)
2023-05-12 03:03:16	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	webmail.ayhu.xyz
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Destructoid (Category: social) https://www.destructoid.com/?name=ayhu
2023-05-12 02:54:23	Web Content Type	No	Web Spider	0	0	4	0	None	text/html;charset=utf-8
2023-05-12 02:54:22	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://www.ayhu.xyz
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-1AA2 (Net ID: 00:1D:D2:1B:1A:A0)
2023-05-12 03:10:19	Malicious IP on Same Subnet	Yes	VoIPBL OpenPBX IPs	0	0	3	0	None	VOIPBL Publicly Accessible PBX List [188.114.96.0/24] http://www.voipbl.org/update
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	XVIDEOS-profiles (Category: XXXPORNXXX) https://www.xvideos.com/profiles/ayhu
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/kappi_1.png
2023-05-12 03:10:04	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	beatrixhaller.at
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	55 2nd PMO (Net ID: 00:01:21:10:61:00)
2023-05-12 02:44:53	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:36:85:4f:53:33:b4:86:64:2a:83:12:ed:95:43:fe:1e:22 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 02:C9: bc:05:a2:c1:63:10:a5:01:dc:4e:2b:3f:07:57:03:2b:c0:d6: 50:e4:e1:65:6d:4b:fd:e0:d9:56:40:77:bf:53:f8:f8:15:43: 95:2f:e5:cc:d5:7e:3a:08:
2023-05-12	WiFi Access	No	Wigle.net	0	0	4	0	None	logitec-99596f (Net ID: 00:01:8E:99:59:6E)

03:18:54	Point Nearby								
2023-05-12 02:50:26	Legal Entity Identifier	No	GLEIF	0	0	3	0	None	5493007DY18BGNLDWU14
2023-05-12 02:53:17	IP Address	No	Mnemonic PassiveDNS	117	0	1	0	None	87.248.157.102
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	My Wireless Network B (Net ID: 00:02:2D:2C:6D:7E)
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Cloud computing providers
2023-05-12 02:50:17	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-12 03:08:48	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.228
2023-05-12 03:03:51	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	rathook.cc
2023-05-12 02:44:14	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	1	1	2	0	None	netlify.app
2023-05-12 02:53:32	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-11T22:16:53.020Z", "ip": "185.199.111.153", "location_updated_at": "2023-05-05T15:17:56.721305Z", "autono 03-22T08:07:48.854244117Z"}, "emilyhem.com": {"record_type": "A", "resolved_at": "2023-03-10T13:30:54.344324871Z"}, "get.intersolar-nf 30T18:58:50.575231531Z"}, "okady.app": {"record_type": "A", "resolved_at": "2023-03-19T21:38:20.632143680Z"}, "t.iiwhy.cn": {"record_t {"record_type": "CNAME", "resolved_at": "2023-03-09T21:55:19.776247657Z"}, "www.bioverse.it": {"record_type": "CNAME", "resolved_at": 08T16:27:35.612127241Z"}, "www.openwaterlogger.org": {"record_type": "CNAME", "resolved_at": "2023-03-12T17:49:34.982246600Z"}, "www.m
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	fansly (Category: XXXPORNXXX) https://fansly.com/login/posts
2023-05-12 02:45:17	Raw Data from RIRs	No	ipapi.co	0	0	4	0	None	{u'region_code': u'ON', u'country_tld': u'.ca', u'ip': u'2606:4700:3037::6815:470e', u'currency_name': u'Dollar', u'currency': u'CAD',
2023-05-12 03:03:33	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:53:45	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:50c0:8002::/48
2023-05-12 03:00:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	chacha20-poly1305@openssh.com
2023-05-12 02:53:09	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'name': u'Contacts server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u' "query.prod.cms.msn.com"\n "teredo.ipv6.microsoft.com"\n "track.salesflare.com"\n "unbouncepages.com"'}, {u'category': u'General', u'o u'description': u'"4e220573-sharepoint_105d01m000000000000028_1_.png" has type "PNG image data 193 x 58 8-bit colormap non-interlaced" u'"urlblockindex_1_.bin" has type "data"- [targetUID: N/A]\n "TarE2C.tmp" has type "data"- Location: [%TEMP%\\TarE2C.tmp]- [targetUID:
2023-05-12 02:55:27	Linked URL - Internal	No	URLScan.io	0	0	1	0	None	http://kekw.battleb0t.xyz/
2023-05-12 02:54:17	Open TCP Port Banner	No	Censys	0	0	4	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.211): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:48:00	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis known community page', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevanc eligible-sites-pre-stable.json, Indicator: "ubs.com")\n ""cousinssubs.com"," (Source: wallet-checkout-eligible-sites-pre-stable.json, lines with no line terminators"- [targetUID: N/A]\n "Filtering Rules" has type "data"- Location: [%TEMP%\\6904_501582631\\Filtering Ru [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\ShaderCache\\data_1]- [targetUID: 00000000-00006904]\n "data_1" has type "data"- Location
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	My Passport (2.4 GHz) - 070B31 (Net ID: 00:00:C0:07:0B:31)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	linksys_SES_31322 (Net ID: 00:1C:10:8D:00:CA)

2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MobileInternet (Net ID: 00:02:B3:AE:AB:38)
2023-05-12 03:09:02	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.100
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:02:2D:9E:09:9A)
2023-05-12 02:45:04	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 02:44:12	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=DigiCert Inc,CN=DigiCert TLS RSA SHA256 2020 CA1
2023-05-12 03:15:35	Web Content Language	No	Language Detector	0	0	6	0	None	English
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Flipboard (Category: tech) https://flipboard.com/@ayhu
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:64:DA:1A)
2023-05-12 03:32:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.20:443
2023-05-12 03:00:57	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.94): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:53:45	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Boingo Colubris (Net ID: 00:02:2D:0B:A5:B3)
2023-05-12 02:53:20	IP Address	No	Mnemonic PassiveDNS	25	0	2	0	None	46.101.229.70
2023-05-12 03:11:19	Physical Coordinates	No	AbstractAPI	100	0	2	0	None	40.2024, 29.0398
2023-05-12 03:16:24	Physical Location	No	ipapi.co	0	0	2	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	logitec-a53131 (Net ID: 00:01:8E:A5:31:30)
2023-05-12 02:54:00	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:0C:41:D2:4D:0D)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Revolut (Category: finance) https://revolut.me/login
2023-05-12 02:53:52	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	OpenBSD OpenSSH 7.4
2023-05-12 03:09:28	SSL Certificate - Issued to	No	SSL Certificate Analyzer	0	0	2	0	None	CN=acilacikveteriner.com
2023-05-12 03:01:18	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.159): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:10:35	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.108.153:443
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	CableWiFi (Net ID: 00:0D:67:47:D4:F4)
2023-05-	WiFi	No	Wigle.net	0	0	4	0	None	

12 03:18:54	Access Point Nearby								MobileInternet (Net ID: 00:02:B3:AE:E4:40)
2023-05-12 02:55:00	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis "172.67.30.148:443"\n "65.8.158.55:443"'}, {u'category': u'General', u'origin': u'Binary File', u'identifier': u'binary-16', u'name': "52H103H9.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\52H103H9.txt]- [targetUID: 00000000-00001020] u'description': u'"cdnjs.cloudflare.com" seems to be random'}, {u'category': u'Network Related', u'origin': u'File/Memory', u'identifi :lrb^HXO3K9> Dn=VT\'TOd$IDLL7Y{a.R1a"q%\'A@uVh}n$AAM+/z5:RqaSR+?UFNaTQXNMl*?8`l3&!</i\'{.g^URVmquGy|hi1l4nc8[Sph]NV+-6v+yJ|BSC{t]u`mqu
2023-05-12 02:44:03	Internet Name	No	SpiderFoot UI	73	0	0	0	None	ayhu.xyz
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.190): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:03	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:08:49	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	35.229.48.109
2023-05-12 02:47:30	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:88:80:c3:9c:e1:f5:05:d4:ce:eb:a7:b8:8b:96:69:16:e7 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: EE:9A: 66:2a:ad:8c:e5:22:e0:2d:ff:f7:04:45:a4:bb:31:8c:99:a5: 16:da:1d:eb:c6:c4:fa:e4:70:84:9c:c6:93:f8:76:5a:3a:48: 95:d4:c6:4d:4c:36:eb:b7:
2023-05-12 02:55:15	Software Used	Yes	Censys	0	0	3	0	None	OpenBSD OpenSSH 8.9p1
2023-05-12 03:00:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.54): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	S-lan (Net ID: 00:01:24:F1:91:41)
2023-05-12 02:47:44	Open TCP Port	No	Pulsedive	0	0	3	0	None	34.148.97.127:80
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	cozyhome (Net ID: 00:06:25:B4:2A:03)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:03:2F:04:BB:BC)
2023-05-12 03:10:33	Blacklisted IP Address	Yes	Threat Jammer	0	1	3	0	None	Threat Jammer - Risk score: 50 (MEDIUM) https://threatjammer.com/info/46.101.229.70
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Microsoft subsidiaries
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	dvdbeyond (Net ID: 00:01:24:F2:B3:12)
2023-05-12 02:49:20	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 132B85B23C3A}"\n "UpdatingNewTabPageData"\n "IsoScope_b24_IESQMMUTEX_0_519"\n "Local\\!BrowserEmulation!SharedMemory!Mutex"'}, {u'cate u'Dropped files', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': "~DFC4D5F15611D45BBD.TMP" has type "data"- Location: [%TEMP%\\~DFC4D5F15611D45BBD.TMP]- [targetUID: 00000000-00002852]\n "nuFvD-vYSZvi "MUID14C9D52949456EC70EC6C7E648096F31msn.com/1025841935360310980906533360963101962 7*"\n Pattern match: "http://daneden.me/animate"\n H
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	1#########123x&&56########12X4& (Net ID: 00:02:2D:BC:46:55)
2023-05-12 02:54:23	Web Content	No	Web Spider	3	0	5	0	None	<!DOCTYPE html> <html lang="en-US"> <head> <title>Just a moment...</title> <meta http-equiv="Content-Type" content="text/html; charset JXEIWKB7DVUehYb7RiTKZ_trIoGgh7Q6yEfeLCDTtC1yC2iiOVhPkX_h4Qfaf7LfPKruh9cjrbe0r7qMb0h8bIRy1fsQXVXXjhWHUJzLPbbOWh7F_0GW3qFusmjdR_P6sJL-gX 'EHiPHm0Nl3GyThu9m1wbXjiHVtOqC3bOZB5NH6FZ4WpN/ont8bhxVwykMxIfoGSCjD8SpsL131biQUzVmplSkmz36+Rbm6LpKDPgFi1SZ6sdv468aKRPGhyFreJfGyRxilqUy
2023-05-12 03:25:40	Similar Domain - Whois	No	Whois	0	0	2	0	None	% Restricted rights. % % Terms and Conditions of Use % % The above data may only be used within the scope of technical or % administra
2023-05-12 03:23:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.8:80
2023-05-12 02:50:15	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	files.battleb0t.xyz
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	6	0	None	cross-origin-opener-policy: same-origin

2023-05-12 02:55:27	Web Server	No	URLScan.io	0	0	1	0	None	cloudflare
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	SoundCloud (Category: music) https://soundcloud.com/ayhu
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-cache-status: DYNAMIC
2023-05-12 02:44:42	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:91:08:65:b4:56:94:e3:89:37:6b:c8:ee:5a:fc:f4:80:52 Signature Algorithm: sha256Wi GMT Extensions: none Signature : ecdsa-with-SHA256 30:45:02:20:25:A0:69:FB:7F:3E:63:7D:A0:82:F0:BD: 99:FA:FF:84:20:AF:C5:86:81:24:4B:F
2023-05-12 03:23:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.8:443
2023-05-12 03:23:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.12:8080
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless (Net ID: 00:01:36:03:06:A5)
2023-05-12 02:49:49	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_FILEMAPSWITCH_MUTEX_3944"'}, {u'category': u'General', u'origin': u'Network Traffic' u'"urlblockindex_1_.bin" has type "data"- [targetUID: N/A]\n "combo_1_.js" has type "ASCII text with very long lines with no line term 00003944]\n "327730364_500683298907150_5975051271861994663_n_1_.jpg" has type "JPEG image data JFIF standard 1.01 aspect ratio density US\nAccept-Encoding: gzip, deflate\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nHost: www.facebook.com\
2023-05-12 02:54:27	Physical Location	No	Censys	0	0	4	0	None	Seattle, Washington, 98108, United States, North America
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.98): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:34	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	route3.mx.cloudflare.net
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 02:54:16	Web Content	No	Web Spider	0	0	4	0	None	/* MIT License Copyright (c) 2017 Pavel Dobryakov Permission is hereby granted, free of charge, to any person obtaining a copy of this paused/minimized. document.addEventListener("visibilitychange", function() { //alert(document.hidden+ " "+document.visibilityState); _ !!gl; if (!isWebGL2) gl = canvas.getContext('webgl', params) || canvas.getContext('experimental-webgl', params); let halfFloat; let su gl.COLOR_ATTACHMENT0, gl.TEXTURE_2D, texture, 0); const status = gl.checkFramebufferStatus(gl.FRAMEBUFFER); return status == gl.FRAMEB document.createElement('span'); github.domElement.parentElement.appendChild(githubIcon); githubIcon.className = 'icon github'; let twi
2023-05-12 02:45:54	Raw Data from RIRs	No	AbstractAPI	0	0	4	0	None	{u'city': u'Ashburn', u'security': {u'is_vpn': False}, u'city_geoname_id': 4744870, u'region_geoname_id': 6254928, u'country': u'Unite
2023-05-12 02:59:50	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	asdf1234@calendar.google.com
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	1	2	0	None	220-cp.keyubu.net ESMTP Exim 4.95 #2 Thu, 11 May 2023 06:41:45 +0300 220-We do not authorize the use of this system to transport unsol
2023-05-12 03:31:23	Malicious IP on Same Subnet	Yes	blocklist.de	0	0	4	0	None	blocklist.de List [207.154.224.0/20] http://lists.blocklist.de/lists/all.txt
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.211): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	SpiceWorks (Category: tech) https://community.spiceworks.com/people/ayhu
2023-05-12 03:00:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.7): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-origin-cache: HIT
2023-05-12 02:54:10	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-	Malicious IP	Yes	VolPBL	0	0	4	0	None	

12 03:10:14	on Same Subnet		OpenPBX IPs						VOIPBL Publicly Accessible PBX List [172.67.160.0/20] http://www.voipbl.org/update
2023-05-12 02:54:41	BGP AS Membership	No	Censys	0	0	3	0	None	396982
2023-05-12 02:45:43	Physical Location	No	AbstractAPI	1	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:09:26	Co-Hosted Site - Domain Whois	No	Whois	2	0	4	0	None	Domain Name: 001VIET.COM Registry Domain ID: 2685910837_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http: only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transm Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.48062425 otherwise support the dissemination or collection of this data, in part or in its entirety, for any purpose, such as transmission by e
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Pastebin (Category: tech) https://pastebin.com/u/login
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<hidden ssid> (Net ID: 00:01:E3:55:9A:D5)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	JIVE2.42025B0 (Net ID: 00:01:9F:20:25:B0)
2023-05-12 03:03:17	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	" (Cloaked) (Net ID: 00:01:36:59:CB:CF)
2023-05-12 02:59:55	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	robert.scheubeck@vitesco.com
2023-05-12 02:55:43	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	{u'count': 1, u'search_terms': [{u'id': u'host', u'value': u'64.226.81.43'}], u'result': [{u'environment_id': 160, u'job_id': u'6421d1
2023-05-12 02:55:15	HTTP Headers	No	Censys	0	0	3	0	None	{"Date": ["<REDACTED>"], "_encoding": {"Date": "DISPLAY_UTF8", "Connection": "DISPLAY_UTF8", "Content_Type": "DISPLAY_UTF8", "Server":
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	dmhs (Net ID: 00:02:2D:0B:16:21)
2023-05-12 03:01:28	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.16): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:35:13	Malicious Co-Hosted Site	Yes	Comodo	0	0	3	0	None	Blocked by Comodo DNS [rathook.cc]
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00jew.github.io
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	eLektriK (Net ID: 00:08:5C:7B:B9:3D)
2023-05-12 02:44:19	Internet Name	No	DNS Resolver	2	0	2	0	None	pics.battleb0t.xyz
2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	Bandlab (Category: music) https://www.bandlab.com/Altpapier
2023-05-12 02:53:39	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "Via": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary":
2023-05-12 02:54:17	HTTP Headers	No	Censys	0	0	4	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 02:48:56	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki {u'category': u'Unusual Characteristics', u'origin': u'Binary File', u'identifier': u'binary-5', u'name': u'Drops cabinet archive file

									has type "PNG image data 136 x 135 4-bit colormap non-interlaced"- [targetUID: N/A]\n "SSL-Certified-icons_1_.png" has type "PNG image Pattern match: "https://cct.google/taggy/agent.js"\n Heuristic match: "* Copyright: (c) 2018 David J. Bradshaw - dave@bradshaw.net"\n
2023-05-12 02:50:26	Physical Address	No	GLEIF	2	0	3	0	None	101 Townsend Street, San Francisco, US-CA, US, 94107
2023-05-12 02:54:17	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://nwapi.battleb0t.xyz
2023-05-12 03:00:25	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-128@openssh.com
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.235): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:17	Open TCP Port Banner	No	Censys	0	0	4	0	None	HTTP/1.1 400 Bad Request Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 253 Connection: close CF-RAY: -
2023-05-12 02:54:34	Physical Location	No	Censys	0	0	3	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:08:47	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.224
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	1	3	0	None	GitHub.com
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:9D:4C:90)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Blogspot (Category: blog) http://login.blogspot.com
2023-05-12 02:44:18	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	InnoPoint (Net ID: 00:02:2D:55:AD:1C)
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	4	0	None	Cloudflare, Inc.
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	MySpace (Category: social) https://myspace.com/Altpapier
2023-05-12 02:56:57	Internet Name	No	DNS Resolver	0	0	2	0	None	kekw.battleb0t.xyz
2023-05-12 02:53:25	IPv6 Address	No	Mnemonic PassiveDNS	0	0	2	0	None	2606:4700:3037::6815:470e
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cross-origin-embedder-policy: require-corp
2023-05-12 02:57:33	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'File/Memory', u'identifier': u'string-127', u'name': u'Found user-agent related strings', u'attck_id_wiki': u'https://attack.mitre.o number 1 6 datablocks 0x1 compression"\n "77EC63BDA74BD0D0E0426DC8F8008506" has type "Microsoft Cabinet archive data Windows 2000/XP s "~DF620C30C65B6B0A84.TMP" has type "data"- Location: [%TEMP%\\~DF620C30C65B6B0A84.TMP]- [targetUID: 00000000-00002272]\n "_4B81942E-80 [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 00000000-00002284]'}, {u'ca
2023-05-12 02:54:34	Raw Data from RIRs	No	Censys	0	0	3	0	None	{"last_updated_at": "2023-05-12T01:00:12.123Z", "ip": "104.21.71.14", "location_updated_at": "2023-04-28T19:19:18.236705Z", "autonomou "sgenundia.tk": {"record_type": "A", "resolved_at": "2023-03-24T07:24:26.513019486Z"}, "www.kjgenerationministries.com.cdn.cloudflare. "2023-05-07T21:13:44.303349330Z"}, "reistomam.ml": {"record_type": "A", "resolved_at": "2023-04-04T19:32:24.563529019Z"}, "brunittamod 30T22:44:30.853447549Z"}, "tizhoo.ir": {"record_type": "A", "resolved_at": "2022-12-14T15:27:25.652479467Z"}, "smartarena.vipe.us": {" "buvade.ml": {"record_type": "A", "resolved_at": "2023-04-27T19:50:04.921168507Z"}, "taapakspices.com": {"record_type": "A", "resolved
2023-05-12 03:08:45	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.213
2023-05-12 03:32:18	Malicious Affiliate	Yes	abuse.ch	0	1	4	0	None	abuse.ch URLhaus (Domain) [cdn-185-199-111-154.github.com] https://urlhaus.abuse.ch/downloads/csv_recent/

2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	101 (Net ID: 00:01:03:7B:E0:44)
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Project hosting websites
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	suddenlink.net-B882 (Net ID: 9C:34:26:46:B8:80)
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.245): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	NGMH (Net ID: 00:09:5B:B3:C8:70)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	USR9108 (Net ID: 00:14:C1:1A:3F:1C)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Freigut (Net ID: 00:01:21:21:C1:60)
2023-05-12 02:56:56	Internet Name	No	DNS Resolver	0	0	4	0	None	kekw.battleb0t.xyz
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Audiojungle (Category: music) https://audiojungle.net/user/ayhu
2023-05-12 02:46:50	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 02:55:18	BGP AS Membership	No	Censys	0	0	3	0	None	14061
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	no_ssid (Net ID: 00:00:0C:07:AC:29)
2023-05-12 02:51:20	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:57:f8:5f:6c:a4:d7:b1:d8:61:78:13:80:db:41:a4:54:3d Signature Algorithm: sha256Wi cc:a9:76:5f:0c:9a:14:80:51:ed:a7:e9:7f:f2:bd:57:5c:9b: 04:31:55:52:cc:d9:5d:ee:2c:9b:e4:bf:d8:d9:92:19:14:10: dd:51:d3:7f:4d:75:15:b6:
2023-05-12 03:10:09	Malicious IP on Same Subnet	Yes	VoIPBL OpenPBX IPs	0	0	3	0	None	VOIPBL Publicly Accessible PBX List [185.199.108.0/24] http://www.voipbl.org/update
2023-05-12 02:53:19	Internet Name	No	Mnemonic PassiveDNS	0	0	1	0	None	mail.ayhu.xyz
2023-05-12 03:33:10	Internet Name	No	DNS Resolver	0	0	3	0	None	vm.battleb0t.xyz
2023-05-12 03:10:01	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	expressdryclean.gr
2023-05-12 03:23:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.2:8080
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	ChicoWLAN (Net ID: 00:0C:F6:4A:CA:EE)
2023-05-12 02:44:03	Domain Name	No	SpiderFoot UI	72	0	0	0	None	battleb0t.xyz
2023-05-12 02:56:57	Internet Name	No	DNS Resolver	0	0	3	0	None	www.ayhu.xyz
2023-05-12 02:57:36	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	1	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.185): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:8880
2023-05-	Non-	No	Strange Header	0	0	5	0	None	

12 02:56:15	Standard HTTP Header		Identifier						nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 02:47:18	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:b9:dc:49:67:68:c5:fe:31:cf:92:a4:a3:f2:91:5a:dc:15 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: CF:FE:
2023-05-12 02:54:18	Linked URL - External	No	Web Spider	8	0	3	0	None	https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js
2023-05-12 03:33:14	Physical Location	No	ipstack	0	0	3	0	None	Germany
2023-05-12 03:32:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.7:8443
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ConnectionPoint (Net ID: 00:01:E3:4A:9F:48)
2023-05-12 02:54:56	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:d7:56:4b:39:cd:63:5b:72:07:1e:ba:15:c9:f7:2c:e7:33 Signature Algorithm: sha256Wi GMT Extensions: none Signature : ecdsa-with-SHA256 30:45:02:21:00:BE:39:54:A0:5F:1F:10:03:FA:09:8D: D3:C7:7F:B5:EC:4B:30:F5:03:1A:D7:1
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/random_6.PNG
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+74955801111
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Woonkamer extra (Net ID: 00:0C:F6:5C:D4:54)
2023-05-12 02:50:59	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://a u'threat_level': 0, u'type': 8, u'description': u'"urlblockindex_1_.bin" has type "data"- [targetUID: N/A]\n "1_2_.jpg" has type "JPEG "urlref_httpsasbrii.github.ioNetflixclone" has type "HTML document UTF-8 Unicode text"- [targetUID: N/A]\n "favicon_1_.ico" has type " "SUIDmicrosoft.com/9216277184358431032346166895971631032229MUID1037C11BAE9D67762C40D215AFD1661Bmicrosoft.com/10252904332800311107001660
2023-05-12 03:01:33	Raw Data from RIRs	No	Tool - WhatWeb	1	0	2	0	None	[{u'request_config': {u'headers': {u'User-Agent': u'Mozilla/5.0'}}, u'target': u'http://www.ayhu.xyz', u'http_status': 301, u'plugins'
2023-05-12 03:31:32	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	6	0	None	b7a6addeb33844c5b2bc9f82a64406e6.protect@withheldforprivacy.com
2023-05-12 02:51:56	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur domains', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u'threat_level_human': u'informative', u'capec_id': None, u' Call', u'identifier': u'api-242', u'name': u'Write files', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_le Location: [%TEMP%\\~DF4E28665F3A902F14.TMP]- [targetUID: 00000000-00003992]\n "~DF143E17619557CCD4.TMP" has type "data"- Location: [%T "ZN7JGHLC.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\ZN7JGHLC.txt]- [targetUID: 00000000-00003992]
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	#LG@Vo1P*Service& (Net ID: 00:01:36:26:BA:43)
2023-05-12 02:53:56	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 03:00:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	sntrup761x25519-sha512@openssh.com
2023-05-12 02:59:51	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	robert@broofa.com
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Open-source software hosting facilities
2023-05-12 02:48:07	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:a2:98:ee:7c:0f:82:53:85:c9:ed:86:47:94:a7:aa:74:64 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 1A:62:
2023-05-12 02:44:05	SSL Certificate Expiring	Yes	CertSpotter	0	0	1	0	None	2023-05-25 03:05:10
2023-05-12	WiFi Access	No	Wigle.net	0	0	3	0	None	UTAAPC (Net ID: 00:02:6F:35:38:63)

03:18:51	Point Nearby								
2023-05-12 02:44:27	Web Technology	No	Tool - Wappalyzer	0	0	2	0	None	Express
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Bookcrossing (Category: hobby) https://www.bookcrossing.com/mybookshelf/Altpapier
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	omniblock (Net ID: 00:09:5B:E9:6B:D6)
2023-05-12 03:01:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.254): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	WLAN_HS (Net ID: 00:01:E3:41:FA:3E)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	clownleo (Net ID: 00:02:CF:AF:25:7D)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX551552560 (Net ID: 00:01:E3:55:25:60)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	KEIL (Net ID: 00:01:38:A5:B3:D3)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	AIRTIES_RT-205 (Net ID: 00:1A:2A:02:E8:38)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-mitigated: challenge
2023-05-12 02:46:41	Physical Location	No	Fraudguard	0	0	3	0	None	United States, South Carolina, North Charleston
2023-05-12 02:49:19	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:b6:39:33:af:de:1e:32:f3:fc:2e:76:dc:bc:08:51:86:10 Signature Algorithm: sha256Wi 6d:1c:e7:15:10:f3:f5:51:a1:19:bc:c1:17:81:af:6e:00:02: 2c:2b:94:b9:a1:29:49:0c:d6:a8:59:00:4b:47:60:f7:bf:4d: a5:8e:dc:6c:e7:62:2f:6e:
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	101 (Net ID: 00:01:03:79:27:12)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Wikidot (Category: social) http://www.wikidot.com/user:info/login
2023-05-12 03:08:53	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.136
2023-05-12 02:44:14	Co-Hosted Site	No	SSL Certificate Analyzer	0	1	2	0	None	netlify.app
2023-05-12 03:13:09	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [010916hao.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:32:18	Malicious Affiliate	Yes	abuse.ch	0	1	4	0	None	abuse.ch URLhaus (Domain) [cdn-185-199-108-154.github.com] https://urlhaus.abuse.ch/downloads/csv_recent/
2023-05-12 02:44:18	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	185.199.110.153:443
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Chamsko (Category: images) https://www.chamsko.pl/profil/login
2023-05-12 03:00:55	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00indahouse.github.io
2023-05-12 02:44:30	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	jQuery
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:BB:17:A7)
2023-05-	Malicious IP	Yes	VoIPBL	0	0	3	0	None	VOIPBL Publicly Accessible PBX List [172.67.128.0/20] http://www.voipbl.org/update

12 03:10:12	on Same Subnet		OpenPBX IPs						
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:04:5A:F9:8E:4E)
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Monkeytown (Net ID: 00:02:2D:29:53:67)
2023-05-12 03:24:47	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 03:36:20	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.128:443
2023-05-12 02:54:22	HTTP Status Code	No	Web Spider	0	1	2	0	None	403
2023-05-12 02:54:22	Linked URL - External	No	Web Spider	2	0	4	0	None	https://github.com/login/oauth/authorize?client_id=42db428b279076117521&redirect_uri=https://qolhub.cloudflareaccess.com/cdn-cgi/acces
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=oldfluid.battleb0t.xyz
2023-05-12 03:31:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	abuse@web.com
2023-05-12 02:56:55	Internet Name	No	DNS Resolver	0	0	3	0	None	nuke.battleb0t.xyz
2023-05-12 03:09:43	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	120.97.148.34.bc.googleusercontent.com
2023-05-12 02:54:15	Linked URL - External	No	Web Spider	0	0	3	0	None	https://stackedit.io/style.css
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.72): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:24:22	HTTP Headers	No	Web Spider	10	0	4	0	None	{"content-encoding": "gzip", "nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "referrer-policy": "same-o
2023-05-12 02:45:35	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	pics.battleb0t.xyz. 300 IN CNAME frabjous-lebkuchen-324004.netlify.app.
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	1	3	0	None	Netlify
2023-05-12 02:53:56	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Room 204 (Net ID: 00:02:2D:1C:33:A5)
2023-05-12 03:09:42	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	119.97.148.34.bc.googleusercontent.com
2023-05-12 02:54:27	Netblock IPv6 Membership	No	Censys	0	0	4	0	None	2600:1f18:2000::/35
2023-05-12 02:44:12	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	2	0	2	0	None	cloudwaysapps.com
2023-05-12 02:46:54	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	teamcity.battleb0t.xyz
2023-05-12 02:56:56	Internet Name	No	DNS Resolver	0	0	4	0	None	panel.battleb0t.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:59:8F:D2)

2023-05-12 03:09:48	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	73.170.74.34.bc.googleusercontent.com
2023-05-12 03:12:54	Raw Data from RIRs	No	numverify	0	0	3	0	None	{u'international_format': u'+14806242599', u'local_format': u'4806242599', u'number': u'14806242599', u'valid': True, u'line_type': u'
2023-05-12 03:10:33	Malicious IP Address	Yes	Threat Jammer	0	1	3	0	None	Threat Jammer - Risk score: 50 (MEDIUM) https://threatjammer.com/info/46.101.229.70
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	ADVFN (Category: finance) https://uk.advfn.com/forum/profile/login
2023-05-12 02:58:36	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 8, u terminators with escape sequences"- Location: [%TEMP%\\7748_1128813663\\auto_open_controller.js]- [targetUID: 00000000-00007748]\n "Pa type "ASCII text with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\1e9e77c7-d679-4ce9-a725-3894fdca913 [%TEMP%\\7748_1128813663\\edge_tracking_page_validator.js]- [targetUID: 00000000-00007748]\n Dropped file: "shopping_iframe_driver.js"
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	bilikom (Net ID: 00:14:C1:0F:F1:FC)
2023-05-12 02:54:14	Web Content	No	Web Spider	1	0	2	0	None	<!DOCTYPE html> <html> <iframe src="https://cloudways-static-content.s3.us-east-1.amazonaws.com/error_page/maintenance-domain-mapping.
2023-05-12 02:44:16	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	www.github.com
2023-05-12 03:01:15	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.136): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:13	BGP AS Membership	No	Censys	0	0	4	0	None	13335
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cf-ray: 7c5f6051f8c478df-EWR
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Vienna (Net ID: 00:09:5B:B1:9F:16)
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	GitHub Category
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX55155989E (Net ID: 00:01:E3:55:98:9E)
2023-05-12 03:32:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.8:8443
2023-05-12 03:13:07	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00lt00.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:33:39	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	eKE>Q RQEA< QEQAE GrG Z?xV _2H- -EEO1AE e.coC ?wX3 QE_1< QEhO0QE QEAAE rGDpyt cv>myz kPIiG X?wV< \u2v5 Qc>ft1 TtV@I iY>eI OYIXf QPO0
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+14806242598
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-cache-status: MISS
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Officewirelessnew (Net ID: 00:13:10:7F:DA:06)
2023-05-12 03:03:51	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	james-gamboa.github.io
2023-05-12 02:44:31	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3037::6815:470e
2023-05-12 02:44:28	IP Address	No	DNS Resolver	74	0	2	0	None	35.229.48.116
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	2	0	3	0	None	https://funny.battleb0t.xyz/images/reveloder.jpg

2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	HOGWARTSSOWAW (Net ID: D4:B2:7A:F3:1A:42)
2023-05-12 02:55:15	Operating System	No	Censys	0	0	3	0	None	Ubuntu Linux
2023-05-12 02:55:21	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 404 Not Found Content-Length: 46 Content-Type: application/json; charset=UTF-8 Date: <REDACTED> Server: Caddy Vary: Origin X-
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:61:24:2C)
2023-05-12 02:54:20	HTTP Headers	No	Censys	0	0	4	0	None	{"Content_Length": ["0"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "
2023-05-12 03:23:11	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.1:443
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:88:80:c3:9c:e1:f5:05:d4:ce:eb:a7:b8:8b:96:69:16:e7 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: EE:9A: 66:2a:ad:8c:e5:22:e0:2d:ff:f7:04:45:a4:bb:31:8c:99:a5: 16:da:1d:eb:c6:c4:fa:e4:70:84:9c:c6:93:f8:76:5a:3a:48: 95:d4:c6:4d:4c:36:eb:b7:
2023-05-12 03:00:33	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	pelorriaga@insumetperu.com
2023-05-12 02:46:16	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 1, u'threat_level': 0, u'type': 7, u'description': u'"code.jquery.com"\n "maxcdn.bootstrapcdn.com"'}, {u'category': u'Installation/Per [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Crashpad\\settings.dat]- [targetUID: 00000000-00007100]\n "Last Browser" has type "data"- IP "3.0.0.8" found in string "\xef\xbb\xbf{ "description": "AutofillCore data component", "name": "AutofillCore", "version": "3.0.0.8" {applied_policy:block,domain:web.basemark.com},{applie"\n Pattern match: "kutumin.github.io/OSCP-notes/1.html"\n Heuristic match: "utu
2023-05-12 03:09:28	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:2b:20:f1:49:ce:17:59:bc:7b:39:e2:e2:fa:42:b1:cb:0c Signature Algorithm: sha256Wi Apr 15 17:29:54.589 2023 GMT Extensions: none Signature : ecdsa-with-SHA256 30:45:02:20:32:B4:07:60:D0:7B:AD:A1:AA:39:A0:33: 2C:4B:E1:
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	5	0	None	cloudflare
2023-05-12 02:53:52	Open TCP Port	No	Censys	0	0	2	0	None	2606:50c0:8003::153:80
2023-05-12 02:54:20	HTTP Status Code	No	Web Spider	0	0	2	0	None	200
2023-05-12 02:57:17	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level': 0, u'type': 7, u'description': u'"34.196.254.27:443"\n "23.62.46.138:80"'}, {u'category': u'General', u'origin': u'Bi 00000000-00001236]\n "RecoveryStore._C7A4F1AE-D920-11E7-B48D-080027D44A30_.dat" has type "Composite Document File V2 Document Cannot r [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63]- [targe positives: 13/88 scanned on 09/15/2022 16:06:16)\n URL: http://goldownloads.netlify.app/ (AV positives: 7/88 scanned on 09/15/2022 13:
2023-05-12 02:54:13	HTTP Headers	No	Web Spider	10	0	4	0	None	{"content-encoding": "gzip", "nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "referrer-policy": "same-o
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:9D:4C:90)
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.216): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:42	Internet Name	No	DNS Resolver	0	0	3	0	None	nwapi2.battleb0t.xyz
2023-05-12 03:01:19	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.173): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.239): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MotoJava (Net ID: 00:01:24:F2:AB:40)
2023-05-12 03:27:00	Web Server	No	Web Server Identifier	0	0	3	0	None	cloudflare
2023-05-12 03:18:57	WiFi Access	No	Wigle.net	0	0	5	0	None	SurfandSip (Net ID: 00:02:2D:03:7C:7A)

	Point Nearby								
2023-05-12 02:46:18	Affiliate Description - Category	No	DuckDuckGo	0	0	2	0	None	Technology companies based in the San Francisco Bay Area
2023-05-12 02:54:00	Open TCP Port	No	Censys	0	0	2	0	None	104.21.6.166:8080
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Sitecom94A3DC (Net ID: 00:0C:F6:94:A3:DC)
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00root.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetA41A (Net ID: 00:01:36:57:A4:18)
2023-05-12 02:50:23	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "dn.msmstatic.com"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-3', u'name': u'Tries to GET no u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 7, u'threat_level': ""99centsubs.com"," (Source: wallet-stable.json, Indicator: "ubs.com")\n ""allieandmickey.com"," (Source: wallet-stable.json, Indicato terminators"- Location: [%TEMP%\\7752_936046049\\edge_driver.js]- [targetUID: 00000000-00007752]\n "vendor.bundle.js" has type "ASCII
2023-05-12 02:56:16	Raw Data from RIRs	No	Tool - WAFW00F	1	0	2	0	None	[{"url": "https://www.ayhu.xyz", "firewall": "Cloudflare", "detected": true, "manufacturer": "Cloudflare Inc."}, {"url": "https://www.
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	www.hollywoodbowl.org (Net ID: 00:01:F4:ED:A0:89)
2023-05-12 03:18:06	URL (Purely Static)	No	Page Information	0	0	4	0	None	http://vscode.battleb0t.xyz
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet8682 (Net ID: 00:01:36:5B:86:80)
2023-05-12 03:09:54	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.108.133:80
2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	tumblr (Category: images) https://Altpapier.tumblr.com
2023-05-12 02:46:49	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 02:59:13	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'binary-16', u'name': u'Drops files marked as clean', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': Non "Local\\ZonesLockedCacheCounterMutex"\n "IsoScope_344_IESQMMUTEX_0_331"\n "IsoScope_344_IE_EarlyTabStart_0x404_Mutex"\n "Local\\URLBLO Cabinet archive data 61712 bytes 1 file"'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'bin Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\80237EE4964FC9C409AAF55BF996A292_D46D6FA25B74360E1349F9015B5CCE53
2023-05-12 02:50:37	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'ca checkout-eligible-sites-pre-stable.json, Indicator: "key.com")\n ""order.firehousesubs.com"," (Source: wallet-checkout-eligible-sites- text with no line terminators"- [targetUID: N/A]\n "data_2" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\De with very long lines"- Location: [%TEMP%\\4224_1061944327\\Mini-Wallet\\miniwallet.bundle.js]- [targetUID: 00000000-00004224]\n "notif
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Private (Net ID: 00:06:B1:20:D3:D2)
2023-05-12 02:54:13	Web Content	No	Web Spider	2	0	4	0	None	<!DOCTYPE html> <html lang="en-US"> <head> <title>Just a moment...</title> <meta http-equiv="Content-Type" content="text/html; charset vtP8UKYeQxLAnNdd4Vl3r7Sxgy5_U4ONoKkZLnzYO166hvNojFJrl5f4tJq3L8oaK1eV5U-xpdOk_jlFbI7ZzjrEUv9fZQsj5GaeDY02cHxOh7Nt2nNuGIpJ43yd7IG1NCu_ks 'TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgMTAuMDsgV2luNjQ7IHg2NDsgcnY6NjIuMCkgR2Vja28vMjAxMDAxMDEgRmlyZWZveC82Mi4w', rm: 'R0VU', d: 'HgohT/b1OM [0].appendChild(cpo); }()); </script> </body> </html>
2023-05-12 02:53:15	IPv6 Address	No	Mnemonic PassiveDNS	0	0	1	0	None	2606:50c0:8001::153
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:50:3C:2C)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	wireless (Net ID: 00:02:2D:26:4A:A6)
2023-05-12	Account on External Site	No	Account Finder	0	0	6	0	None	darudar (Category: misc) https://darudar.org/users/login/

03:19:09									
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	RyanLG (Net ID: 00:01:36:4F:9A:F0)
2023-05-12 02:56:54	Affiliate - Domain Name	No	DNS Resolver	2	0	3	0	None	keyubu.net
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	4	0	None	15169
2023-05-12 03:23:50	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.20:80
2023-05-12 03:00:56	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.92): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	5	0	2	0	None	+14806242598
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/ein_2.png
2023-05-12 02:44:34	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:23:36:1a:72:6e:fc:71:09:49:b1:35:f9:b5:e5:28:80:de Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: E6:0D:
2023-05-12 02:46:59	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur a3ae0000'}, {u'category': u'General', u'origin': u'API Call', u'identifier': u'api-8', u'name': u'Looks up procedures from modules (ex u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\8a37d1a7-21d3-4df9-8999-4552124a3857.tmp]- 36e2f1ffd71c.tmp" has type "UTF-8 Unicode text with very long lines with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\E
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SurfandSip Wavelan (Net ID: 00:02:2D:01:79:94)
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:53:04	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.111.153:80
2023-05-12 03:10:57	Raw Data from RIRs	No	Keybase	0	0	6	0	None	{u'status': {u'code': 0, u'name': u'OK'}, u'them': [{u'basics': {u'username': u'login', u'track_version': 0, u'ctime': 1437685663, u'l
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.158): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:24:29	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	Domains By Proxy, LLC
2023-05-12 02:54:18	Web Content Type	No	Web Spider	0	0	2	0	None	text/html;charset=utf-8
2023-05-12 03:01:18	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.160): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:03:33	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	logitec-a53131 (Net ID: 00:01:8E:A5:31:30)
2023-05-12 03:00:50	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00-evan.github.io
2023-05-12 03:13:05	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0065paula.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:44:07	Internet Name	No	CertSpotter	30	1	1	0	None	pics.battleb0t.xyz
2023-05-12 03:09:40	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	118.48.229.35.bc.googleusercontent.com
2023-05-12	Affiliate - Internet	No	DNS Resolver	0	0	4	0	None	112.48.229.35.bc.googleusercontent.com

03:09:39	Name								
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MobileInternet (Net ID: 00:02:B3:AE:65:D0)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	padt-1 (Net ID: 00:01:21:1F:7B:30)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	x-cache: HIT
2023-05-12 03:09:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	sni.cloudflaressl.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	TechAir (Net ID: 00:01:21:30:60:FD)
2023-05-12 02:54:19	Web Content	No	Web Spider	0	0	4	0	None	/** * dat-gui JavaScript Controller Library * http://code.google.com/p/dat-gui * * Copyright 2011 Data Arts Team, Google Creative Lab {e.style.background="",S.each(ee,function(i){e.style.cssText+="background: "+i+"linear-gradient("+t+", "+n+" 0%, "+o+" 100%); "})}func slider"),n.domElement.insertBefore(o.domElement,n.domElement.firstElementChild)}else if(n instanceof Q){var i=function(t){if(S.isNumbe X.addClass(l,"color"):X.addClass(l,H(i.getValue())),h(e,l,i),e.__controllers.push(i),i}function m(e,t){return document.location.href+" {return t.preventDefault(),e.width+=i-t.clientX,e.onResize(),i=t.clientX,!1}function n(){X.removeClass(e.__closeButton,he.CLASS_DRAG),
2023-05-12 02:45:43	Physical Coordinates	No	AbstractAPI	92	0	2	0	None	37.7642, -122.3993
2023-05-12 03:09:37	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	228.30.196.104.bc.googleusercontent.com
2023-05-12 02:54:20	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2023-05-12 02:54:00	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:46:42	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "104.26.6.190:49733"\n "142.250.191.42:49734"\n "104.18.11.207:49735"\n "104.17.24.14:49736"\n "69.16.175.42:49737"\n "185.199.111.153 Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Cache\\Cache_Data\\f_00023e]- [targetUID: 00000000-00004716]\n "Tabs_1 30d7-464d-9d7a-20dde7d02eca.tmp" has type "UTF-8 Unicode text with very long lines with no line terminators"- [targetUID: N/A]\n "Last "https://*excel.officeapps.live.com/*,https://*onenote.officeapps.live.com/*,https://*powerpoint.officeapps.live.com/*,https://*word-e
2023-05-12 02:44:49	Company Name	No	Company Name Extractor	0	0	2	0	None	Domain Names REG.RU, LLC
2023-05-12 03:12:53	Physical Location	No	numverify	0	0	3	0	None	Phoenix, US
2023-05-12 03:23:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.3:8443
2023-05-12 02:56:16	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	None None
2023-05-12 03:03:18	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	sntrup761x25519-sha512@openssh.com
2023-05-12 03:24:21	Web Content Type	No	Web Spider	0	0	4	0	None	text/html;charset=utf-8
2023-05-12 02:46:17	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Project hosting websites
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	3	0	None	Turkey
2023-05-12 03:11:10	Physical Coordinates	No	OpenStreetMap	98	0	4	0	None	33.336199,-111.89446440830702
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Wimbledon (Net ID: 00:02:CF:8C:8A:BF)

2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["1391"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "X_Powered_By": "DISPLAY_UTF8", "X_Content_Type_Options":
2023-05-12 03:31:29	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	abuse@nicproxy.com
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:2079
2023-05-12 02:54:44	Raw Data from RIRs	No	Censys	0	0	3	0	None	{"last_updated_at": "2023-05-11T23:52:27.325Z", "ip": "35.229.48.116", "location_updated_at": "2023-05-03T02:08:25.414245Z", "autonomo "akshaylilani.com": {"record_type": "A", "resolved_at": "2023-04-06T02:51:29.813870033Z"}, "blissfulspringark.com": {"record_type": "A 18T06:14:40.221938027Z"}, "damagestudio.dev": {"record_type": "A", "resolved_at": "2022-10-14T14:43:11.503470454Z"}, "matmicha.fr": {" {"record_type": "CNAME", "resolved_at": "2022-10-18T04:17:17.475596148Z"}, "dsa-play.altaracredit.com": {"record_type": "CNAME", "reso "www.guerraoffice.com": {"record_type": "CNAME", "resolved_at": "2022-10-18T06:23:06.306203975Z"}, "kind2-home.netlify.app": {"record_
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	referrer-policy: strict-origin-when-cross-origin
2023-05-12 02:44:16	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 03:23:38	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.14:80
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	keisharayne (Net ID: 00:1D:CE:8A:EF:D7)
2023-05-12 03:00:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.38): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:49	Physical Location	No	AbstractAPI	0	0	2	0	None	Chicago, Illinois, 60666, United States, North America
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	TATBIKAT MIMARLIK (Net ID: 00:14:C1:20:3F:E3)
2023-05-12 03:00:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	zlib@openssh.com
2023-05-12 03:03:47	Co-Hosted Site	No	ThreatMiner	1	0	2	0	None	ply.gg
2023-05-12 02:44:43	Internet Name	No	DNS Resolver	0	0	2	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.186): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<hidden ssid> (Net ID: 00:01:E3:54:FF:0B)
2023-05-12 03:01:36	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.129): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:09:45	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	134.97.148.34.bc.googleusercontent.com
2023-05-12 03:01:29	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.28): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	linksys (Net ID: 00:14:BF:A7:74:74)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:06:25:75:F1:53)
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	6	0	None	British Indian Ocean Territory

2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	warriorforum (Category: hobby) https://www.warriorforum.com/members/login.html
2023-05-12 03:01:24	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.227): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:13	HTTP Headers	No	Censys	0	0	4	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect
2023-05-12 03:03:27	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.192): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Speaker Deck (Category: social) https://speakerdeck.com/login/
2023-05-12 03:09:32	Affiliate - Internet Name	No	DNS Resolver	2	0	3	0	None	cdn-185-199-108-154.github.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	\022\026\024\001\027\004\013\017\005\014\022\032\0 (Net ID: 00:09:5B:2F:26:42)
2023-05-12 03:12:12	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2011-3389 https://nvd.nist.gov/vuln/detail/CVE-2011-3389 Score: 4.3 Description: The SSL protocol, as used in certain configuratio
2023-05-12 03:01:21	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.188): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	003marek.github.io
2023-05-12 02:53:52	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Connection: keep-alive Content-Length: 5142 Server: GitHub.com Content-Type: text/html; charset=utf-8 ETag: W/"
2023-05-12 03:00:50	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00-duino.github.io
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	4	0	3	0	None	http://nuke.battleb0t.xyz/cdn-cgi/styles/main.css
2023-05-12 03:24:52	Country	No	Country Name Extractor	0	0	3	0	None	United Kingdom
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	ru_123rf (Category: hobby) https://ru.123rf.com/profile_login
2023-05-12 02:48:54	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:37:68:7b:1f:26:29:cd:a4:cc:95:52:df:e2:0a:12:6f:13 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: D9:CF:
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	celikpalas (Net ID: 00:12:17:69:2A:A4)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Noisette (Net ID: 00:0D:93:87:BE:5F)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Mezzanine Airport (Net ID: 00:02:2D:0E:42:E3)
2023-05-12 02:48:31	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "172.67.75.130:80"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-0', u'name': u'Contacts domain solid-900_1_.eot" has type "Embedded OpenType (EOT) Font Awesome 5 Pro Solid family"- [targetUID: N/A]\n "AAAABVxdX2WnFSp49eXb1do0euaj "pxiEyp8kv8JHgFVrFJM_1_.woff" has type "Web Open Font Format TrueType length 66572 version 1.1"- [targetUID: N/A]'}, {u'category': u'N perspective_alpha_website_small.jpg"\n Pattern match: "https://assets.nflxext.com/ffe/siteui/acquisition/ourStory/fuji/desktop/tv.png"
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	BabyPips (Category: social) https://forums.babypips.com/u/login/summary
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	FIS (Net ID: 00:02:2D:2E:39:1C)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_ipad (Net ID: 00:0C:E6:08:09:05)
2023-05-12	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Fastly

02:44:19									
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX5515722CD (Net ID: 00:01:E3:57:22:CD)
2023-05-12 03:03:37	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:55:27	Web Server	No	URLScan.io	0	1	1	0	None	Werkzeug/2.2.2 Python/3.10.9
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_ipad (Net ID: 00:0C:E6:08:1D:05)
2023-05-12 03:15:37	Cookies	No	Cookie Extractor	0	0	4	0	None	CF_Session=nrj43fxpNUBlI2Utd; Path=/; Secure; Expires=Fri, 12 May 2023 06:54:22 GMT; HttpOnly; SameSite=none
2023-05-12 02:54:59	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur DATETIME-L1-1-1" at base b4ee0000\n "msedge.exe" loaded module "API-MS-WIN-CORE-LOCALIZATION-OBSOLETE-L1-2-0" at base b4ee0000\n "msed u'type': 7, u'description': u'"35.185.199.199:443"\n "185.199.109.153:443"\n "185.199.108.154:443"\n "35.247.66.204:443"\n "172.64.100 00000000-00008176]\n "manifest.json" has type "UTF-8 Unicode (with BOM) text with CRLF line terminators"- Location: [%LOCALAPPDATA%\\M [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Code Cache\\js\\index-dir\\temp-index]- [targetUID: 00000000-00008176]\n "edge_c
2023-05-12 03:00:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.0): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ASU (Net ID: 00:06:25:66:88:D8)
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:09:5B:6B:72:5C)
2023-05-12 02:48:30	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:10:8b:16:97:4c:80:e7:56:d7:06:74:1e:45:16:d2:cf:08 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: A8:1A:
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=fJBUelNZ98yfCYgTc7WNhjysoMluqrTDHq0SVIO%2F0YIAsdqyzhnqcX
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	ENHLG (Net ID: 00:01:36:5B:37:00)
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.75): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:14	Domain Name	No	DNS Resolver	0	0	1	0	None	ayhu.xyz
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.139): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:57	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2a06:98c1:3120::/48
2023-05-12 03:00:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-64-etm@openssh.com
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Poshmark (Category: shopping) https://poshmark.com/closet/ayhu
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	cable (Net ID: 00:02:2D:2F:C6:B5)
2023-05-12 03:13:06	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [007joshie.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:01:18	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.154): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:3a:9d:01:de:8f:db:a2:52:4a:02:0c:18:70:da:44:dd:bc Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 20:59: 29:67:65:9c:a3:5e:54:d7:42:a2:ca:57:e3:ed:40:b5:6b:e7: 20:ae:3b:11:70:76:c2:da:cf:31:f0:ab:ca:10:28:73:4e:36: 4a:79:71:99:ba:fe:41:29:
2023-05-	WiFi	No	Wigle.net	0	0	5	0	None	KKR Guest (Net ID: 00:01:21:70:65:31)

12 03:18:56	Access Point Nearby								
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	sohqwn1 (Net ID: 00:16:B6:F7:22:6E)
2023-05-12 02:55:05	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 151 Connection: keep-alive CF-RAY:
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	steemit (Category: social) https://steemit.com/@login
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	tla60e06 (Net ID: 00:25:F0:A6:0E:06)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MobileInternet (Net ID: 00:02:B3:AE:AB:1C)
2023-05-12 02:44:17	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.com
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/random_1.jpeg
2023-05-12 03:01:38	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.151): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:20	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://funny.battleb0t.xyz/images/withat_2.jpg
2023-05-12 02:54:07	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 400 Bad Request Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 253 Connection: close CF-RAY: -
2023-05-12 02:54:38	HTTP Headers	No	Censys	0	0	3	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:01:35	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.114): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	GitHub Category
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	1 375 East 2nd St Ch.11 (Net ID: 00:02:2D:8E:C5:7C)
2023-05-12 03:00:57	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	01-scripts.github.io
2023-05-12 02:53:30	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "65.8.158.24:443"\n "142.251.46.234:443"\n "142.251.46.195:443"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifi 00000000-00003428]'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dro [%TEMP%\\~DF11BB896A60D4C13F.TMP]- [targetUID: 00000000-00002684]\n "~DF5CCB270BF65728C8.TMP" has type "data"- Location: [%TEMP%\\~DF5 "SUIDMmicrosoft.com/92161081838464310294414282125642310293 23*MUID0AAB32D61E88645A137620291FC4652Cmicrosoft.com/10251214327680311077954
2023-05-12 03:31:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	abuse@name.com
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	NGMH (Net ID: 00:09:5B:B3:C8:73)
2023-05-12 03:01:40	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.186): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:51:13	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "13.227.74.49:443"\n "104.19.187.97:443"\n "129.148.158.16:443"\n "104.18.43.158:443"\n "142.251.46.227:443"\n "151.139.128.10:443"\n with (Indicator: "dir "; File: "3WL9D6RI.txt")\n file/memory contains long string with (Indicator: "dir "; File: "44XFFKPA.txt")\n Fou "Hellenic-Bank-HB_1_.png" has type "PNG image data 1501 x 626 8-bit/color RGB non-interlaced" and extension "png"\n "Together-with-Ser data 640 x 1452 8-bit colormap non-interlaced" and extension "png"\n "Home-Page-Newsroom-Investors-Careers-Desktop-Investors-1_1_.png"
2023-05-12 03:19:47	Account on External Site	No	Account Finder	0	0	2	0	None	Pinterest (Category: social) https://www.pinterest.com/patrickpogoda/
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:01:71:0A:07:07)
2023-05-	Co-Hosted	No	ThreatMiner	2	0	2	0	None	eliaspinheironeto.github.io

12 03:03:47	Site								
2023-05-12 03:09:49	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	77.170.74.34.bc.googleusercontent.com
2023-05-12 02:59:15	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'Created Mutant', u'identifier': u'mutant-0', u'name': u'Creates mutants', u'attck_id_wiki': None, u'threat_level_human': u'informati [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\E87CE99F124623F95572A696C80EFCAF_7F9CD1EAD79E5E81389FF041C7CC4C83]- [targe "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\BAD725C80F9E10846F35D039A996E4A8_88B6AE015495C1ECC395D19 CMS-SearchShardsFailed: 0\nX-CMS-SearchReturnedCount: 1\nX-CMS-DocumentStorageTier: Cache\nEdge-control: max-age=900s,downstream-ttl=9
2023-05-12 02:44:05	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	webmail.ayhu.xyz
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.198): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:59:54	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	astehnkuhl@generalatlantic.com
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	cHEEZburger (Category: hobby) https://profile.cheezburger.com/login
2023-05-12 03:24:22	HTTP Status Code	No	Web Spider	0	2	2	0	None	404
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	RPOWER3 (Net ID: 00:02:6F:B3:3B:AA)
2023-05-12 03:31:33	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	4f516d38c2f942669e9c1663e414ae75.protect@withheldforprivacy.com
2023-05-12 03:09:04	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	87.248.157.107
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SEC_LinkShare_693068 (Net ID: 00:12:FB:E0:05:F2)
2023-05-12 02:54:13	Open TCP Port Banner	No	Censys	0	0	4	0	None	HTTP/1.1 400 Bad Request Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 253 Connection: close CF-RAY: -
2023-05-12 02:52:48	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_huma href="https://twitter.com/OptiSignsInc" target="_blank" class="w-inline-block"> <svg width="32" height wallet-stable.json, Indicator: "ubs.com")\n ""annabelbleu.com"," (Source: wallet-stable.json, Indicator: "leu.com")\n ""aspirefashions mode\\0.0.0.10\\manifest.fingerprint"\n "msedge.exe" reads file "c:\\users\\%osuser%\\appdata\\local\\microsoft\\edge\\user data\\eadp
2023-05-12 03:01:44	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.233): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:01:F4:5B:7B:F7)
2023-05-12 02:48:26	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis "iexplore.exe" loaded module "%WINDIR%\\System32\\setupapi.dll" at 75CB0000\n "iexplore.exe" loaded module "%WINDIR%\\System32\\cfgmgr module "%WINDIR%\\System32\\advapi32.dll" at 75EE0000\n "iexplore.exe" loaded module "%WINDIR%\\System32\\sechost.dll" at 77020000\n " l1-1-0.dll" at 71E80000\n "iexplore.exe" loaded module "%WINDIR%\\System32\\shell32.dll" at 76230000\n "iexplore.exe" loaded module "% "%PROGRAMFILES%\\Internet Explorer\\ieproxy.dll" at 69220000\n "iexplore.exe" loaded module "%WINDIR%\\System32\\WSHTCPIP.DLL" at 741F
2023-05-12 02:45:39	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis "104.18.23.52:443"\n "142.250.191.74:443"\n "142.250.189.163:443"\n "45.57.91.1:443"\n "172.64.100.10:443"'}, {u'category': u'General' data JFIF standard 1.01 aspect ratio density 1x1 segment length 16 progressive precision 8 640x480 components 3" and extension "jpg"\n [%LOCALAPPDATA%\\Microsoft\\Internet Explorer\\DomainSuggestions\\en-US.4]- [targetUID: 00000000-00003540]\n "RecoveryStore._88B090C0- u'threat_level': 0, u'type': 2, u'description': u'Pattern match: "http://klliii.github.io/clone-netflix/"\n Pattern match: "http://kll
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BBHWIRELESS (Net ID: 00:00:C5:D7:5E:5C)
2023-05-12 03:09:39	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	109.48.229.35.bc.googleusercontent.com

2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00theway.github.io
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CHILDERS (Net ID: 00:09:5B:70:17:F2)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	PDI (Net ID: 00:06:25:FE:34:4D)
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	venia1101 5 (Net ID: 00:01:9F:34:7C:24)
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:443
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.203): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:54	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	cloudflare.net
2023-05-12 03:09:28	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	acilacikveteriner.com
2023-05-12 02:54:54	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Snapchat Stories (Category: social) https://story.snapchat.com/s/ayshoo
2023-05-12 02:44:24	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Cloudflare
2023-05-12 02:44:14	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	2	0	None	C=US,ST=California,L=San Francisco,O=Netlify\, Inc,CN=*.netlify.app
2023-05-12 02:55:05	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2096
2023-05-12 02:46:12	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://a compressed data from FAT filesystem (MS-DOS OS/2 NT) original size modulo 2^32 480998"- Location: [%TEMP%\\59f9f8c0-2fcb-48a3-9c43-382 None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 2, u 10, u'threat_level': 0, u'type': 12, u'description': u'0/90 Antivirus vendors marked sample as malicious (0% detection rate)'}, {u'cat
2023-05-12 02:49:42	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id': u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"ovolve.github.io"\n "ovolve.github.io." 00003076]\n "favicon_3_.ico" has type "MS Windows icon resource - 1 icon 32x32 32 bits/pixel"- [targetUID: N/A]\n "~DFA990EBDE4D7AD6EC u'SUCCESS', u'entrypoint': None, u'mitre_attcks': [{u'parent': None, u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071', u u'190362034693d3992c7a6e770f7f7b1f', u'network_mode': u'default', u'processes': [], u'sha1': u'a14c41f95cb25b4fba550658bd8036aa7eb9616
2023-05-12 03:03:20	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:54:48	BGP AS Membership	No	Censys	0	0	3	0	None	396982
2023-05-12 02:54:23	Web Content Type	No	Web Spider	0	0	4	0	None	text/css
2023-05-12 02:55:05	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:28:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.144:80
2023-05-12 02:54:38	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 400 Bad Request Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 253 Connection: close CF-RAY: -
2023-05-12 02:44:32	Affiliate - Internet Name	No	DNS Resolver	2	0	2	0	None	cdn-185-199-110-153.github.com
2023-05-12 02:44:39	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	portainer.battleb0t.xyz
2023-05-12	WiFi Access	No	Wigle.net	0	0	4	0	None	myLGNet (Net ID: 00:01:36:26:A1:14)

03:18:54	Point Nearby								
2023-05-12 03:00:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.3): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	logitec-a53c1d (Net ID: 00:01:8E:A5:3C:1C)
2023-05-12 02:55:56	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur 1', u'name': u'Contacts server', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, lor.instructure.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "user-agent: ")\n "GET /standard.94ce4fbb3fdb7e2758a9e018cc35e9c14e00 "mozilla/5.0 (")\n "GET /api/feature-flags HTTP/1.1\nAccept: */*\nContent-Type: application/json\nx-session-id: undefined\nReferer: ht Gecko\nHost: lor.instructure.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GET /api/licenses HTTP/1.1\nAccept:
2023-05-12 02:44:05	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:91:08:65:b4:56:94:e3:89:37:6b:c8:ee:5a:fc:f4:80:52 Signature Algorithm: sha256Wi GMT Extensions: none Signature : ecdsa-with-SHA256 30:45:02:20:25:A0:69:FB:7F:3E:63:7D:A0:82:F0:BD: 99:FA:FF:84:20:AF:C5:86:81:24:4B:F
2023-05-12 02:53:56	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Serve
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Wile (Net ID: 00:06:25:C6:1D:77)
2023-05-12 02:58:06	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'name': u'Creates mutants', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u're "Web Open Font Format TrueType length 20712 version 1.1"- [targetUID: N/A]\n "6BADA8974A10C4BD62CC921D13E43B18_28DEA62A0AE77228DD387E1 00000000-00003832]\n "analytics_3_.js" has type "ASCII text with very long lines"- [targetUID: N/A]\n "QWUH7FY2.txt" has type "ASCII t Explorer\\RPCRTREMOTE.DLL"\n "iexplore.exe" trying to touch file "C:\\Program Files\\Internet Explorer\\DNSAPI.DLL"\n "iexplore.exe" t
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.79): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:20	Web Content	No	Web Spider	7	0	2	0	None	<!DOCTYPE html> <html> <head> <title>Funny Forehead Gallery</title> <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/boots src="/images/carti_1.jpg"> <img src="/images/carti_2.PNG"> < "thumbnail"> <img src="/images/random_2.jpeg"> <img src="/im
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:2086
2023-05-12 02:53:00	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	Cloudflare Inc. Cloudflare
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+14806242598
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	\012\034\030\003\031\003\007\024\022\001\035\027\0 (Net ID: 00:05:4E:45:3B:FE)
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-resource-policy: same-origin
2023-05-12 02:54:30	Software Used	Yes	Censys	0	0	3	0	None	linux
2023-05-12 03:08:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.81
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	BLINK-6985 (Net ID: 00:03:7F:A1:AE:79)
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-001-0.github.io
2023-05-12 03:03:47	Co-Hosted Site	No	ThreatMiner	2	0	2	0	None	james-gamboa.github.io
2023-05-12 02:54:16	Web Content	No	Web Spider	0	0	4	0	None	/** * dat-gui JavaScript Controller Library * http://code.google.com/p/dat-gui * * Copyright 2011 Data Arts Team, Google Creative Lab {e.style.background="",S.each(ee,function(i){e.style.cssText+="background: "+i+"linear-gradient("+t+", "+n+" 0%, "+o+" 100%); "})}func slider"),n.domElement.insertBefore(o.domElement,n.domElement.firstElementChild)}else if(n instanceof Q){var i=function(t){if(S.isNumbe X.addClass(l,"color"):X.addClass(l,H(i.getValue())),h(e,l,i),e.__controllers.push(i),i}function m(e,t){return document.location.href+" {return t.preventDefault(),e.width+=i-t.clientX,e.onResize(),i=t.clientX,!1}function n(){X.removeClass(e.__closeButton,he.CLASS_DRAG),
2023-05-12 02:44:47	Software Used	Yes	Tool - Wappalyzer	0	0	3	0	None	HSTS

2023-05-12 03:13:01	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0-001-0.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:54:20	HTTP Headers	No	Web Spider	2	0	4	0	None	{"x-content-type-options": "nosniff", "content-encoding": "gzip", "transfer-encoding": "chunked", "expires": "Fri, 12 May 2023 04:54:2
2023-05-12 03:00:25	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.1): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:26	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	zlib@openssh.com
2023-05-12 02:44:21	Physical Location	No	ipstack	0	0	2	0	None	United States
2023-05-12 02:46:16	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	DevOps - DevOps is a methodology in the software development and IT industry. Used as a set of practices and tools, DevOps integrates
2023-05-12 02:54:51	HTTP Headers	No	Censys	0	0	3	0	None	{"Date": ["<REDACTED>"], "_encoding": {"Date": "DISPLAY_UTF8", "Content_Length": "DISPLAY_UTF8", "X_Nf_Request_Id": "DISPLAY_UTF8", "S
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom1330 (Net ID: 00:01:38:92:E5:07)
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date":
2023-05-12 03:01:24	Web Server	No	Tool - WhatWeb	0	0	1	0	None	cloudflare
2023-05-12 03:01:13	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.128): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:11	Raw Data from RIRs	No	Venmo	0	0	6	0	None	{u'username': u'login', u'first_name': u'baptiste', u'last_name': u'vauthey', u'display_name': u'baptiste vauthey', u'identity_type':
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	figma (Category: tech) https://www.figma.com/@login
2023-05-12 03:01:33	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.92): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys-a (Net ID: 00:0C:41:0B:AB:D7)
2023-05-12 03:01:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.201): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:24:33	Malicious Affiliate	Yes	VXVault.net	0	1	4	0	None	VXVault Malicious URL List [cdn-185-199-109-154.github.com] http://vxvault.net/URL_List.php
2023-05-12 03:32:19	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.10:8080
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	speedstream (Net ID: 00:01:24:F1:A9:A3)
2023-05-12 02:44:16	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 02:56:52	Internet Name	No	DNS Resolver	0	0	3	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:32:52	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 03:24:22	Web Content Type	No	Web Spider	0	0	2	0	None	text/html
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ASI (Net ID: 00:02:6F:51:19:D9)
2023-05-12 02:53:57	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7,

									bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCa [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 00000000-00002812]\n "sandes "https://wasimreja.me/assets/img/opengraph.png"\n Pattern match: "https://fonts.googleapis.com"\n Pattern match: "https://fonts.gstati
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	myLGNet (Net ID: 00:02:A8:C2:91:21)
2023-05-12 03:09:45	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	132.97.148.34.bc.googleusercontent.com
2023-05-12 03:01:41	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.200): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.249): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:57	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SX551D17A4D (Net ID: 00:01:E3:D1:7A:4D)
2023-05-12 03:00:56	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	00root.github.io
2023-05-12 02:54:34	HTTP Headers	No	Censys	0	0	3	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conne
2023-05-12 03:23:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.2:8443
2023-05-12 02:44:40	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	116.48.229.35.bc.googleusercontent.com
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	My Passport (2.4 GHz) - 0778A5 (Net ID: 00:00:C0:07:78:A5)
2023-05-12 02:50:56	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:62:27:a6:dc:16:28:de:ae:a0:a4:7d:7e:a0:02:81:25:0e Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 1A:29: 1e:cb:c5:98:bf:4b:bf:03:59:91:6e:75:8b:e9:11:d9:3b:3a: e6:90:a3:02:49:4e:21:28:66:07:46:87:31:86:8a:ff:ea:59: d0:c3:7e:c2:6d:3c:37:07:
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/nomnom.jpg
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 03:09:26	Co-Hosted Site - Domain Whois	No	Whois	3	0	4	0	None	Domain Name: 007316.XYZ Registry Domain ID: D339018444-CNIC Registrar WHOIS Server: whois.name.com Registrar URL: http://www.name.com/ names, (2) not to store or reproduce this data in any way, (3) not to use any high-volume, automated, electronic processes to obtain d Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2023-05-12T03:09:26Z <<< For more informa
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.101): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:33:45	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	http://ns.adobe.com/xap/1.0/ XPhotoshop 3.0 Photo Booth ICC_PROFILE mntrRGB XYZ acspAPPL -appl bdscm vcgt 0ndin >chad 8bTRC aagg desc
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Pillowfort (Category: social) https://www.pillowfort.social/login
2023-05-12 02:45:32	Malicious IP Address	Yes	PhishStats	0	1	2	0	None	Phishstats [185.199.108.153]
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Pornhub Users (Category: XXXPORNXXX) https://www.pornhub.com/users/Altpapier
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BriteMedia (Net ID: 00:00:72:20:59:DD)
2023-05-12 02:44:09	Co-Hosted Site	No	SSL Certificate Analyzer	4	1	1	0	None	www.github.com
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	FruityWifi-001 (Net ID: 00:02:72:8E:62:D1)
2023-05-12 03:01:26	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.248): Search Engine Last Activity: 0 days ago Threat Level: 29

2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MatrixEx BYOD (Net ID: 00:01:21:26:42:51)
2023-05-12 02:46:50	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	3	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 02:5a:61:0f:58:eb:84:f1:ad:53:ae:03:dc:a9:84:7a Signature Algorithm: ecdsa-with-SHA 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: 1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73 Timestamp : Dec 21 09:03:52.857 2022
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:8443
2023-05-12 02:50:11	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 8, u'description': u'Antivirus vendors marked dro Encoding: gzip, deflate\nDNT: 1\nHost: rotaryragusa.it\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GET / HTTP/1.1\nAccept Gecko\nAccept-Encoding: gzip, deflate\nHost: rotaryragusa.it\nDNT: 1\nConnection: Keep-Alive\nCookie: pll_language=it" (Indicator: "mo https://rotaryragusa.it/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-En
2023-05-12 02:54:13	Linked URL - Internal	No	Web Spider	0	0	1	0	None	http://ayhu.xyz
2023-05-12 03:00:36	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abusecomplaints@markmonitor.com
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	cross-origin-embedder-policy: require-corp
2023-05-12 02:55:11	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Content_Type": "DISPLAY_UTF8", "Set_Cookie": "DISPLAY_UTF8", "X_Content_Type_Options": "DISPLAY_UTF8", "Connection": "
2023-05-12 02:44:09	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	1	0	None	C=US,ST=California,L=San Francisco,O=GitHub\, Inc.,CN=*.github.io
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	denis (Net ID: 00:01:46:02:C4:4C)
2023-05-12 02:45:35	Internet Name	No	DNSDumpster	0	0	1	0	None	nwapi.battleb0t.xyz
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cf-ray: 7c5f6036feab195d-EWR
2023-05-12 03:07:25	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 03:08:53	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.74.170.64
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:2087
2023-05-12 03:13:05	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [003marek.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:33:51	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	PLTE$ kyhNlC2D kShPAJ esyS_S@? txkST`ANdNO rXYuPYXHR XajGc dzvRt IDATx :7MV- '@crrX QK>@W vWP`Z tmv1q XEFi" 4@1hb a'c:3 2FRB> LHiiB YF
2023-05-12 03:18:52	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Horizontal (normal) @ 18}
2023-05-12 03:01:32	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.77): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:16	IPv6 Address	No	DNS Resolver	0	0	3	0	None	2606:4700:3030::ac43:a8fc
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.55): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:15:35	Web Content Language	No	Language Detector	0	0	3	0	None	English
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	scratch (Category: coding) https://scratch.mit.edu/users/Altpapier/
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Hakim Evi (Net ID: 00:14:C1:2E:AE:67)
2023-05-12	Physical Location	No	ipapi.co	1	0	2	0	None	Toronto, Ontario, ON, Canada, CA

02:45:09									
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 3 of 50 allowed. 220-Local time is now 15:16. Se
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	oatscream (Net ID: 00:0C:E6:39:59:E1)
2023-05-12 02:56:25	BGP AS Membership	No	RIPE	0	0	4	0	None	14061
2023-05-12 02:44:24	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	githubusercontent.com
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 401 Unauthorized Date: <REDACTED> Server: cPanel Persistent-Auth: false Host: 87.248.157.102:2078 Cache-Control: no-cache, no
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	laethof_ipad (Net ID: 00:0C:E6:08:1C:05)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	RPOWER3 (Net ID: 00:02:6F:B3:3B:AA)
2023-05-12 02:44:19	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	MatrixEx Guest (Net ID: 00:01:21:26:54:30)
2023-05-12 03:19:00	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SX55154C9AA (Net ID: 00:01:E3:54:C9:AA)
2023-05-12 02:44:15	IPv6 Address	No	DNS Resolver	16	0	3	0	None	2606:4700:3037::6815:470e
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	NBNCorp (Net ID: 00:09:5B:A3:EA:31)
2023-05-12 03:24:51	Country	No	Country Name Extractor	0	0	6	0	None	Iceland
2023-05-12 02:57:26	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	teamcity.battleb0t.xyz
2023-05-12 02:54:34	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 400 Bad Request Server: cloudflare Date: <REDACTED> Content-Type: text/html Content-Length: 253 Connection: close CF-RAY: -
2023-05-12 02:55:22	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 3, u'threat_level': u'attck_id': u'T1105', u'relevance': 3, u'threat_level': 0, u'type': 8, u'description': u'"urlblockindex_1_.bin" has type "data"- [tar Exif standard: [TIFF image data little-endian direntries=0] baseline precision 8 1514x813 components 3"- [targetUID: N/A]\n "cropped-i [], u'attck_id': u'T1071.004', u'malicious_identifiers': [], u'malicious_identifiers_count': 0, u'technique': u'DNS', u'informative_id
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/nwp.PNG
2023-05-12 03:32:00	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.1:80
2023-05-12 03:01:26	Web Server	No	Tool - WhatWeb	0	0	2	0	None	cloudflare
2023-05-12 02:54:34	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Ashburn Square WiFi (Net ID: 00:0C:66:13:0B:72)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	x-nf-request-id: 01H06Y2YH7X6V06YSWWEW2NH9C
2023-05-12 03:32:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.13:443

2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	NotABug (Category: coding) https://notabug.org/login
2023-05-12 02:53:52	BGP AS Membership	No	Censys	0	0	2	0	None	54113
2023-05-12 03:23:50	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.20:8443
2023-05-12 02:54:19	HTTP Headers	No	Web Spider	6	0	2	0	None	{"nel": "{\"success_fraction\":0,\"report_to\":\"cf-nel\",\"max_age\":604800}", "alt-svc": "h3=\":443\"; ma=86400, h3-29=\":443\"; ma=
2023-05-12 02:44:24	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	github.io
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-cache-status: REVALIDATED
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://pics.battleb0t.xyz/images/master058_3.PNG
2023-05-12 03:01:45	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.241): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:58:15	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"34.148.97.127:80"\n "34.148.97.127:443"'}, {u'category': u'General 00000000-00003956]\n "~DF8145DA2F49859598.TMP" has type "data"- Location: [%TEMP%\\~DF8145DA2F49859598.TMP]- [targetUID: 00000000-0000 [%APPDATA%\\Microsoft\\Windows\\Cookies\\YU3Y19RW.txt]- [targetUID: 00000000-00002648]\n "_0571D1C5-1D1B-11ED-A31E-080027B82EA8_.dat" None, u'relevance': 10, u'threat_level': 0, u'type': 12, u'description': u'0/93 Antivirus vendors marked sample as malicious (0% detec
2023-05-12 02:44:39	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	tiktok.battleb0t.xyz
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Rick (Net ID: 00:0F:B5:14:80:C2)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Clementine (Net ID: 00:02:2D:39:EC:00)
2023-05-12 03:32:08	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.5:443
2023-05-12 02:54:49	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': None, [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\d632ab85-22c5-4d58-aa3b-6f1d5e994f5f.tmp]- [targetUID: 00000000-00003948]\n "7ae [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\EdgePushStorageWithConnectTokens\\LOG]- [targetUID: 00000000-00003948]'}, {u'cat Heuristic match: "PATHEXT=.COM;.EXE;.BAT;.CM"\n Heuristic match: "ishcouncil.org%2Fmonmon.myat%40mm.britishcouncil.org"\n Pattern matc
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	1	2	0	None	220-cp.keyubu.net ESMTP Exim 4.95 #2 Thu, 11 May 2023 00:03:02 +0300 220-We do not authorize the use of this system to transport unsol
2023-05-12 03:09:35	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	216.30.196.104.bc.googleusercontent.com
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	sflan47b (Net ID: 00:02:6F:08:22:03)
2023-05-12 02:45:56	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/ {d=a.document.getElementsByTagName("script");e=a.navigator&&a.navigator.userAgent||"";e=RegExp("appbankapppuzdradb|daumapps|fban|fbios "f_2_.txt" has type "ASCII text with very long lines"- [targetUID: N/A]\n "TarB03F.tmp" has type "data"- Location: [%TEMP%\\TarB03F.tm u'identifier': u'binary-39', u'name': u'Drops XML files', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'threat_lev
2023-05-12 02:54:38	Open TCP Port	No	Censys	0	0	3	0	None	172.67.168.252:2052
2023-05-12 02:44:04	Web Technology	No	Tool - WAFW00F	0	0	1	0	None	Fastly CDN Fastly
2023-05-12 03:01:46	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.254): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:03	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray
2023-05-12 02:54:10	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connect

2023-05-12 03:09:27	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	0	0	3	0	None	https://pics.battleb0t.xyz/images/master058_2.PNG
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:06:25:AC:5B:3E)
2023-05-12 02:46:50	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	PumaLANd Airport 1 (Net ID: 00:02:2D:39:EC:A6)
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Enis_Home (Net ID: 00:02:CF:DB:CE:E7)
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	suddenlink.net-9796 (Net ID: 5C:8F:E0:22:97:94)
2023-05-12 02:48:36	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'ca ID3 version 2.4.0 contains:MPEG ADTS layer III v1 64 kbps 44.1 kHz Stereo"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Def Tokens" has type "SQLite 3.x database last written using SQLite version 3039003"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Dat "Microsoft.Windows.Shell.rundll32,processorArchitecture="amd64",type="win32",version="5.1.0.0"C:\\WINDOWS\\system32\\RunDll32.exe"\n P
2023-05-12 02:50:13	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/ u'"widevinecdm.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%TEMP%\\5828_1392880218_platform_s "7de06ccc-e1f1-446e-9777-eeec16b06646.tmp" has type "ASCII text with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\ Location: [%TEMP%\\5828_1392880218_metadata\\verified_contents.json]- [targetUID: 00000000-00005828]\n "shopping_iframe_driver.js" h
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SWKIDNEY1 (Net ID: 00:02:6F:ED:54:F6)
2023-05-12 02:54:16	Web Content Type	No	Web Spider	0	0	4	0	None	application/javascript
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2052
2023-05-12 03:08:50	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	34.148.97.118
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:8880
2023-05-12 03:09:27	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 09:6b:82:e9:73:99:94:ba:fd:55:b0:21:db:c7:c8:bf Signature Algorithm: ecdsa-with-SHA : 35:CF:19:1B:BF:B1:6C:57:BF:0F:AD:4C:6D:42:CB:BB: B6:27:20:26:51:EA:3F:E1:2A:EF:A8:03:C3:3B:D6:4C Timestamp : Aug 3 19:12:00.017 2022
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00why00.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:00:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.26): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:18	HTTP Headers	No	Web Spider	2	0	2	0	None	{"content-length": "1200", "content-encoding": "gzip", "accept-ranges": "bytes", "strict-transport-security": "max-age=31536000", "var
2023-05-12 02:54:41	Open TCP Port	No	Censys	0	0	3	0	None	104.196.30.220:443
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet2EE2 (Net ID: 00:01:36:5B:2E:E0)
2023-05-12 03:23:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.3:80
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Burfas10 (Net ID: 00:15:6D:A0:BD:ED)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Brown?s Living Room (Net ID: 00:19:9D:FF:D0:E3)
2023-05-	SSL	Yes	CertSpotter	0	0	1	0	None	

12 02:44:09	Certificate Expiring								2023-05-12 05:22:09
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	5	0	2	0	None	+14806242599
2023-05-12 02:55:05	Physical Location	No	Censys	0	0	2	0	None	San Francisco, California, 94107, United States, North America
2023-05-12 02:54:03	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:03:39	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:58:22	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:18:ae:06:7e:fc:0b:78:46:5c:8b:fe:1a:31:bf:5b:16:b8 Signature Algorithm: sha256Wi 0d:d4:24:6a:dc:a8:66:3f:6f:01:46:76:6d:ab:41:86:f7:8a: 9f:a9:30:88:c8:3c:39:d0:93:9d:c0:84:21:71:d0:ed:5b:fd: 37:f1:e5:b1:17:44:f1:5d:
2023-05-12 03:01:37	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.137): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:44:12	SSL Certificate - Issued to	No	SSL Certificate Analyzer	1	0	2	0	None	C=US,ST=California,L=San Francisco,O=GitHub\, Inc.,CN=*.github.io
2023-05-12 02:53:25	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis u'type': 7, u'description': u'"154.82.100.186:80"\n "154.82.100.186:443"\n "172.217.12.106:443"\n "47.253.50.2:443"\n "142.250.191.42: content="https://uploads-ssl.webflow.com/5b479ea1731aa13135a70342/5e6010110671f79d5c96adf9_open%20graph.png" property="twitter:image"> "webflow_1_.css")\n Found string ".w-widget-twitter-count-shim:not(.w--vertical).w--large:before {" (Indicator: "dir "; File: "webflow 8 450x450 components 3" and extension "jpg"\n "dapp-aave_1_.png" has type "PNG image data 560 x 560 8-bit/color RGBA non-interlaced" a
2023-05-12 03:11:22	Physical Coordinates	No	AbstractAPI	0	0	3	0	None	50.1188, 8.6843
2023-05-12 03:24:48	Country	No	Country Name Extractor	0	0	4	0	None	United States
2023-05-12 03:12:12	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	2	2	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	Villakakelbond2 (Net ID: 00:14:5C:8C:72:80)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cross-origin-embedder-policy: require-corp
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.169): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:00:37	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	registrar-abuse@cloudflare.com
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	REL (Net ID: 00:02:2D:02:35:63)
2023-05-12 03:03:40	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	totamay (Net ID: 00:02:2D:29:D3:71)
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	MPR1 (Net ID: 00:02:6F:BD:4E:18)
2023-05-12 02:45:53	Physical Location	No	AbstractAPI	0	0	4	0	None	Montreal, Quebec, H4X, United States, North America
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F0:17:4A)
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	Instagram (Category: social) https://instagram.com/ayhu
2023-05-12	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	cloudwaysapps.com

2023-05-12 02:46:49									
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 401 Unauthorized Date: <REDACTED> Server: cPanel Persistent-Auth: false Host: 87.248.157.102:2091 Connection: close WWW-Authe
2023-05-12 03:12:10	Affiliate Description - Category	No	DuckDuckGo	0	0	5	0	None	Companies based in Bath, Somerset
2023-05-12 03:01:39	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.165): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:47	Account on External Site	No	Account Finder	0	0	2	0	None	Snapchat Stories (Category: social) https://story.snapchat.com/s/patrickpogoda
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	cpanel.ayhu.xyz
2023-05-12 02:54:34	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:09:40	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	115.48.229.35.bc.googleusercontent.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Wireless (Net ID: 00:09:5B:31:8E:D4)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
2023-05-12 02:58:35	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+14806242599
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	HOME-4F32 (Net ID: 00:1D:D4:64:4F:30)
2023-05-12 02:45:35	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	www.battleb0t.xyz. 300 IN CNAME battleb0t.github.io.
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	imgur (Category: images) https://imgur.com/user/login/about
2023-05-12 03:31:27	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	abuse@ascio.com
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Ashton7346 (Net ID: 00:06:25:61:05:DC)
2023-05-12 03:13:09	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0101.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	snoopyine (Net ID: 00:01:E3:4A:B1:79)
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	vapor (Net ID: 00:02:2D:09:FC:69)
2023-05-12 03:03:17	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	cpcontacts.ayhu.xyz
2023-05-12 03:00:49	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0-fog.github.io
2023-05-12 02:50:19	Physical Location	No	ipstack	0	0	3	0	None	United States
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	myLGNet_411 (Net ID: 00:01:36:45:14:AA)
2023-05-12 02:50:19	Physical Location	No	ipstack	0	0	3	0	None	United States
2023-05-12 02:44:49	Raw Data from RIRs	No	CRXcavator	0	0	1	0	None	[{"platform": "Chrome", "version": "1.6.1", "data": {"webstore": {"website": "https://github.com/jawil/GayHub", "rating": 4.6923075, " "https://lh3.googleusercontent.com/GQWBPNAC8Q7LdRt-cnVK4JrImzSNY2HVSNWgsZlup1YaXFLx5VVr7fa34WEvV0cPv-zalCCQ5_3ck7IHBxrhgsGuKA=w128-h12

									9YPGOHIyPleEphEcxtYZ7P41-tokT9f0iOferGYTOLdI4flseKdEsHZjy8g=w128-h128-e365-rj-sc0x00ffffff", "rating_users": 39, "name": "Darker Backg "short_description": "A customizable web browser extension that enhances productivity and efficiency through the use of mouse.", "icon "https://lh3.googleusercontent.com/wVtUFY8eOOwpsblTcFWpOmQt4yB2BF3aVumaIgMZMf_L6i9ynhcGdXdI7f256COTYOzhxvWGJLcelzBm_5-jq3Y8=w128-h128-
2023-05-12 03:31:58	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.0:443
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pancakes (Net ID: 00:00:48:67:6D:D1)
2023-05-12 03:33:47	Raw File Meta Data	No	Binary String Extractor	0	0	4	0	None	IDATx m_p Y 0a6-X h5Zh5b 4L8uS >m7xY YGhP5 10IMLR bc<p0 :"CGlZ k>04D A nL/ "KBt:-t h\dHkQU 2<qC jg>v\i AW$@C V3\/g :>2'F WF93l IDATV S
2023-05-12 03:01:07	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.117): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	Bitchute (Category: political) https://www.bitchute.com/channel/login/
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ProCare-Guest (Net ID: 00:01:21:1C:30:F0)
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	002evapey.github.io
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	2WIRE119 (Net ID: 00:02:2D:68:85:12)
2023-05-12 02:55:11	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 401 Unauthorized Date: <REDACTED> Server: cPanel Persistent-Auth: false Host: 87.248.157.102:2080 Cache-Control: no-cache, no
2023-05-12 02:46:04	Physical Location	No	MetaDefender	0	0	3	0	None	Jacksonville, United States
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	cross-origin-embedder-policy: require-corp
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	5	0	None	Australia
2023-05-12 03:08:46	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.215
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	infinity2 (Net ID: 00:06:25:DA:3E:86)
2023-05-12 02:51:22	Malicious Co-Hosted Site	Yes	VirusTotal	0	1	3	0	None	VirusTotal [netlify.app] https://www.virustotal.com/en/domain/netlify.app/information/
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ToddNet (Net ID: 00:01:24:F2:5E:43)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	MobileInternet (Net ID: 00:02:B3:AE:FA:18)
2023-05-12 02:48:14	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informative', u'capec_id': N u'https://attack.mitre.org/techniques/T1105', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1105', u'relev no line terminators"- [targetUID: N/A]\n "en-US.4" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Internet Explorer\\DomainSug "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\T4W3H708.txt]- [targetUID: 00000000-00003008]\n "urlref_httpsllink.to
2023-05-12 02:45:30	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:99:a3:5c:44:13:8f:1f:f4:9f:74:e5:4f:ad:57:81:83:24 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 98:BA:
2023-05-12 03:19:01	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Beyza (Net ID: 00:13:49:45:9F:FA)
2023-05-12 03:03:16	Internet Name	No	DNS Resolver	0	0	2	0	None	ayhu.xyz
2023-05-12	Blacklisted IP on Same	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.188): Search Engine Last Activity: 0 days ago Threat Level: 29

03:01:40	Subnet								
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	iMGSRC.RU (Category: images) https://imgsrc.ru/main/user.php?lang=ru&user=login
2023-05-12 02:45:22	Raw Data from RIRs	No	ipapi.co	0	0	4	0	None	{u'region_code': u'VA', u'country_tld': u'.us', u'ip': u'2600:1f18:2489:8202::c8', u'currency_name': u'Dollar', u'currency': u'USD', u
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.10): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:15:05	Account on External Site	No	Account Finder	0	0	1	0	None	Twitter (Category: social) https://twitter.com/Battleb0t
2023-05-12 02:49:28	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur user32.dll, gdi32.dll, ole32.dll, comctl32.dll, uxtheme.dll, oleaut32.dll, version.dll, msctfime.ime)', u'attck_id_wiki': None, u'thre u'relevance': 1, u'threat_level': 0, u'type': 2, u'description': u'Observed API string:"OpenThread" [Source: 00000000-00004176.0000000 [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 00000000-00004664]\n "deny_ [targetUID: 00000000-00004664]\n "temp-index" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Code Ca
2023-05-12 02:57:04	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\InternetShortcutMutex"\n "{5312EE61-79E3-4A24-BFE1-132B85B23C3A}"\n "UpdatingNewTabPageData"\n "Local\\URLBLOCK_FILEMAPSWITCH_ u'threat_level': 0, u'type': 8, u'description': u'"urlblockindex_1_.bin" has type "data"- [targetUID: N/A]\n "6BADA8974A10C4BD62CC921D "57C8EDB95DF3F0AD4EE2DC2B8CFD4157" has type "Microsoft Cabinet archive data 4817 bytes 1 file"- Location: [%LOCALAPPDATA%\\ow\\Microso None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 12, u'description': u'0/89 Antivirus vendors marked sample as
2023-05-12 02:58:39	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur Antivirus vendors marked dropped file "Tar3EB2.tmp" as clean (type is "data")'}, {u'category': u'General', u'origin': u'Created Mutant Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\W1QY00XB.txt]- [targetUID: 00000000-00003688]\n Dropped file: "ZT5CWOJ1.txt" - Loca File', u'identifier': u'binary-5', u'name': u'Drops cabinet archive files', u'attck_id_wiki': None, u'threat_level_human': u'informati "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\ZT5CWOJ1.txt]- [targetUID: 00000000-00003688]\n "mwgt_4.1_1_.js" has
2023-05-12 03:16:17	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	aahu.xyz
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	padt-1 (Net ID: 00:01:21:1F:75:30)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	logitec-a028e9 (Net ID: 00:01:8E:A0:28:E8)
2023-05-12 03:02:26	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Cloudflare Turnstile
2023-05-12 02:46:42	Physical Location	No	Fraudguard	0	0	3	0	None	United States, South Carolina, North Charleston
2023-05-12 03:13:09	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0101kvmt.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:01:06	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.116): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:31:34	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	proxy@whoisprotectservice.com
2023-05-12 03:23:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.10:8080
2023-05-12 02:44:21	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	www.github.com
2023-05-12 02:59:21	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:88:a7:3c:db:48:4e:7a:5b:30:55:60:8f:23:20:34:8b:3f Signature Algorithm: sha256Wi Extensions: none Signature : ecdsa-with-SHA256 30:46:02:21:00:C8:55:7C:0B:F2:4A:D4:C9:EE:94:0C: EF:F0:9C:B6:19:B4:91:58:D6:05:71:7A:F5
2023-05-12 02:44:09	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Google Trust Services LLC,CN=GTS CA 1P5
2023-05-12 02:54:03	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 02:46:49	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	netlify.app
2023-05-12 02:58:55	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\UpdatingNewTabPageData"'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'i Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE8126868377

									Explorer\\IEXPLORE.EXE.LOCAL"\n "iexplore.exe" trying to touch file "C:\\Program Files\\Internet Explorer\\SSPICLI.DLL"\n "iexplore.ex 2/88 scanned on 09/07/2022 18:55:54)\n URL: http://nintransfer.netlify.app/ (AV positives: 4/88 scanned on 09/07/2022 18:34:11)\n URL:
2023-05-12 02:57:38	Vulnerability - CVE Low	Yes	Tool - testssl.sh	0	2	1	0	None	CVE-2013-0169 https://nvd.nist.gov/vuln/detail/CVE-2013-0169 Score: 2.6 Description: The TLS protocol 1.1 and 1.2 and the DTLS protoco
2023-05-12 02:59:44	Co-Hosted Site - Domain Whois	No	Whois	2	0	3	0	None	Domain Name: netlify.app Registry Domain ID: 2CB5C0CD0-APP Registrar WHOIS Server: whois.nic.google Registrar URL: http://www.name.com REDACTED FOR PRIVACY Billing Organization: REDACTED FOR PRIVACY Billing Street: REDACTED FOR PRIVACY Billing City: REDACTED FOR PRIVAC ID: 2CB5C0CD0-APP Registrar WHOIS Server: whois.nic.google Registrar URL: http://www.name.com Updated Date: 2023-04-11T15:58:16Z Creat REDACTED FOR PRIVACY Billing Street: REDACTED FOR PRIVACY Billing City: REDACTED FOR PRIVACY Billing State/Province: REDACTED FOR PRIV
2023-05-12 02:46:49	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	3	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 9d:49:08:08:d4:e9:44:f0:ed:d2:82:b7:e0:6b:90:98 Signature Algorithm: sha256WithRSAE 76:FF:88:3F:0A:B6:FB:95:51:C2:61:CC:F5:87:BA:34: B4:A4:CD:BB:29:DC:68:42:0A:9F:E6:67:4C:5A:3A:74 Timestamp : Apr 27 08:49:21.510 2023 74:0e:15:b3:cc:fb:a8:3c:e6:07:2b:89:aa:f9:0a:70:0d:02: b5:99:9c:87
2023-05-12 03:01:34	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.105): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:08:46	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	104.196.30.216
2023-05-12 02:53:11	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis "209.94.90.1:443"\n "185.199.109.153:443"\n "69.16.175.10:443"\n "52.155.62.95:443"'}, {u'category': u'General', u'origin': u'Network files', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1083', u'threat_level_human': u'informative', u'capec_id': None, u'at "sharepoint_2_.htm" has type "HTML document ASCII text with very long lines with CRLF line terminators"- [targetUID: N/A]\n "jquery-1. "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\UK2REO93.txt]- [targetUID: 00000000-00003560]\n "7NLF2DJG.txt" has ty
2023-05-12 03:12:10	Affiliate Description - Category	No	DuckDuckGo	0	0	5	0	None	WOT Services , community of volunteer users ranking website reputation.
2023-05-12 02:54:44	Open TCP Port	No	Censys	0	0	3	0	None	35.229.48.116:443
2023-05-12 03:09:43	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	122.97.148.34.bc.googleusercontent.com
2023-05-12 02:44:06	Internet Name	No	CertSpotter	28	0	1	0	None	nwapi2.battleb0t.xyz
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	5	0	None	cf-ray: 7c5f60721cb70f8d-EWR
2023-05-12 02:45:24	Physical Location	No	ipapi.co	1	0	3	0	None	Frankfurt am Main, Hesse, HE, Germany, DE
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.56): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:42	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:04:02:53:52:8b:ff:fb:8a:0a:11:44:e7:ab:f5:69:c5:9e Signature Algorithm: sha256Wi 3d:db:2e:3d:c8:b1:34:d0:37:5f:80:1d:38:7f:1c:95:f3:da: c4:21:7d:17
2023-05-12 02:59:49	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	carymolinaro12@gmail.com
2023-05-12 03:10:05	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	4	0	None	ecash-pay.com
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CableWiFi (Net ID: 00:0D:67:8C:21:AB)
2023-05-12 03:16:31	Physical Location	No	ipapi.co	0	0	3	0	None	Frankfurt am Main, Hesse, HE, Germany, DE
2023-05-12 03:24:19	Account on External Site	No	Account Finder	0	0	8	0	None	Gravatar (Category: images) http://en.gravatar.com/profiles/baptistevauthey
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	xfinitywifi (Net ID: 00:0D:67:65:A6:FB)
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:2053
2023-05-12 03:03:23	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io

2023-05-12 02:55:21	Open TCP Port	No	Censys	0	0	3	0	None	207.154.228.169:80
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/carti_3.JPG
2023-05-12 03:03:16	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	cpcalendars.ayhu.xyz
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	SF Library (Net ID: 00:02:2D:01:53:3D)
2023-05-12 03:01:31	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.60): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	<no ssid> (Net ID: 00:02:2D:03:B5:CA)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	NSA (Net ID: 00:02:6F:24:1C:7D)
2023-05-12 03:18:06	URL (Uses Javascript)	No	Page Information	0	0	3	0	None	http://pics.battleb0t.xyz
2023-05-12 02:54:13	Linked URL - Internal	No	Web Spider	4	0	2	0	None	https://battleb0t.xyz/./src/style.css?4
2023-05-12 02:50:07	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:53:52:1f:22:68:d4:e4:bd:04:c1:ea:37:ae:da:35:a4:38 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: C8:7D:
2023-05-12 03:06:53	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2013-3587 https://nvd.nist.gov/vuln/detail/CVE-2013-3587 Score: 5.9 Description: The HTTPS protocol, as used in unspecified web ap
2023-05-12 03:00:25	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	aes128-gcm@openssh.com
2023-05-12 03:18:25	Account on External Site	No	Account Finder	0	0	5	0	None	Linktree (Category: social) https://linktr.ee/Altpapier
2023-05-12 02:44:45	Similar Domain	Yes	Similar Domain Finder	1	0	1	0	None	battlebot.xyz
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ProCare-Staff (Net ID: 00:01:21:1C:31:01)
2023-05-12 02:48:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur deflate\nAccept-Language: en-US,en;q=0.9"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u' "key.com")\n ""order.firehousesubs.com"," (Source: wallet-checkout-eligible-sites-pre-stable.json, Indicator: "ubs.com")\n ""cousinssu u'name': u'Read files', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1083', u'threat_level_human': u'informative', u'capec with CRLF line terminators"- Location: [%TEMP%\\2988_1083578063\\edge_driver.js]- [targetUID: 00000000-00002988]\n "wallet.bundle.js"
2023-05-12 03:08:42	Affiliate - IP Address	No	DNS Look-aside	0	0	3	0	None	64.226.81.33
2023-05-12 02:45:46	Physical Coordinates	No	AbstractAPI	0	0	2	0	None	37.751, -97.822
2023-05-12 02:53:45	Open TCP Port	No	Censys	0	0	2	0	None	2606:50c0:8002::153:443
2023-05-12 03:12:15	Affiliate - Domain Whois	No	Whois	6	0	6	0	None	Domain Name: ONDIGITALOCEAN.COM Registry Domain ID: 2280019987_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.networksolutions.com Regi or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compila Registry Tech ID: Tech Name: PERFECT PRIVACY, LLC Tech Organization: Tech Street: 5335 Gate Parkway care of Network Solutions PO Box 4 terms. For more information on Whois status codes, please visit https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en.
2023-05-12 03:23:02	Account on External Site	No	Account Finder	0	0	2	0	None	ask.fm (Category: social) https://ask.fm/ayhu
2023-05-12 02:59:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "Local\\ZonesLockedCacheCounterMutex"\n "UpdatingNewTabPageData"\n "Local\\ZonesCacheCounterMutex"\n "Local\\VERMGMTBlockListFileMutex u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 9, u'description': u'Spawned proce

									[%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776]- [target 00001292]\n "TarCDC7.tmp" has type "data"- Location: [%TEMP%\\TarCDC7.tmp]- [targetUID: 00000000-00002388]'}, {u'category': u'Network
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	xfinitywifi (Net ID: 00:0D:67:33:68:60)
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	BudgetScottsdale (Net ID: 00:09:5B:29:02:37)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SSR (Net ID: 00:01:E3:51:27:11)
2023-05-12 03:18:49	Raw File Meta Data	No	File Metadata Extractor	0	0	4	0	None	{'Image Orientation': (0x0112) Short=Rotated 90 CW @ 18}
2023-05-12 03:10:06	Malicious IP Address	Yes	VoIPBL OpenPBX IPs	0	1	2	0	None	VOIPBL Publicly Accessible PBX List [185.199.109.153] http://www.voipbl.org/update
2023-05-12 02:44:27	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Express
2023-05-12 02:59:53	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	david@14islands.com
2023-05-12 02:46:06	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:3a:9d:01:de:8f:db:a2:52:4a:02:0c:18:70:da:44:dd:bc Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 20:59:
2023-05-12 02:44:03	Username	No	SpiderFoot UI	0	0	0	0	None	Kekwltd
2023-05-12 03:24:50	Country	No	Country Name Extractor	0	0	4	0	None	Cocos Islands
2023-05-12 03:18:58	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	HPN (Net ID: 00:0C:41:76:71:40)
2023-05-12 02:56:15	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	x-fastly-request-id: 81f392d6f8601ba9f7017cc835b0845172eec1e9
2023-05-12 02:54:19	Web Content	No	Web Spider	0	0	4	0	None	/* MIT License Copyright (c) 2017 Pavel Dobryakov Permission is hereby granted, free of charge, to any person obtaining a copy of this 0.2, PRESSURE: 0.8, PRESSURE_ITERATIONS: 20, CURL: 30, SPLAT_RADIUS: 0.25, SPLAT_FORCE: 6000, SHADING: true, COLORFUL: true, COLOR_UPD halfFloatTexType); formatR = getSupportedFormat(gl, gl.RGBA, gl.RGBA, halfFloatTexType); } ga('send', 'event', isWebGL2 ? 'webgl2' : ' 'SHADING').name('shading').onFinishChange(updateKeywords); gui.add(config, 'COLORFUL').name('colorful'); gui.add(config, 'PAUSED').nam document.createElement('span'); discord.domElement.parentElement.appendChild(discordIcon); discordIcon.className = 'icon discord'; let
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ThomasWirelessNetwork (Net ID: 00:0D:3A:2C:F8:2D)
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	SitecomD86B30 (Net ID: 00:0C:F6:D8:6B:30)
2023-05-12 02:56:07	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis /index_files/style_v2_optimized.css HTTP/1.1\nAccept: text/css, */*\nReferer: https://wm50098748930309454ft456.netlify.app/index.htm\n Encoding: gzip, deflate\nHost: wm50098748930309454ft456.netlify.app\nDNT: 1\nConnection: Keep-Alive" (Indicator: "user-agent: ")\n "GE wm50098748930309454ft456.netlify.app\nDNT: 1\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GET /cPanel_magic_revision_13861 /cPanel_magic_revision_1386192031/unprotected/cpanel/fonts/open_sans/OpenSans-BoldItalic-webfont.eot? HTTP/1.1\nAccept: */*\nReferer:
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0000cap.github.io
2023-05-12 03:17:44	Account on External Site	No	Account Finder	0	0	1	0	None	Pronouns.Page (Category: social) https://pronouns.page/api/profile/get/ BattleB0t ?version=2
2023-05-12 02:44:15	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Patreon
2023-05-12 03:13:02	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [0.github.io] https://www.openphish.com/feed.txt
2023-05-12 02:56:50	Internet Name	No	DNS Resolver	0	0	2	0	None	fluid.battleb0t.xyz
2023-05-	Affiliate -	No	DNS Resolver	0	0	3	0	None	127.97.148.34.bc.googleusercontent.com

12 02:44:41	Internet Name								
2023-05-12 03:22:23	Account on External Site	No	Account Finder	0	0	2	0	None	Spotify (Category: music) https://open.spotify.com/user/battleb0t
2023-05-12 03:18:59	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Allstate 5G (Net ID: 00:02:6F:F8:0A:41)
2023-05-12 02:56:16	Raw Data from RIRs	No	Hybrid Analysis	1	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'identifier': u'mutant-0', u'name': u'Creates mutants', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': N u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 5, u'threat_level': [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\BAD725C80F9E10846F35D039A996E4A8_88B6AE015495C1ECC395D19C1DD02894]- [targe N/A]\n "7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\
2023-05-12 02:44:21	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	185.199.108.153:443
2023-05-12 03:18:51	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	NH-NEW (Net ID: 00:01:21:30:F0:D3)
2023-05-12 03:42:54	Affiliate - Domain Whois	No	Whois	3	0	6	0	None	Domain Name: INFLANY.COM Registry Domain ID: 2688698192_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.world4you.com Registrar URL: htt commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processe PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Coun systems). # World4You reserves the right to modify these terms at any time. # By submitting this query, you agree to abide by this pol
2023-05-12 02:54:13	HTTP Status Code	No	Web Spider	0	0	3	0	None	403
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	BBHWIRELESS_24 (Net ID: 00:00:C5:D7:60:DC)
2023-05-12 03:17:35	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: AYU.XYZ Registry Domain ID: D9607467-CNIC Registrar WHOIS Server: whois.west.cn Registrar URL: http://www.west.cn Updated presented here for any purpose other than determining ownership of domain names, (2) not to store or reproduce this data in any way, (REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVA
2023-05-12 02:44:15	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Patreon
2023-05-12 02:56:25	Netblock Membership	No	RIPE	0	0	3	0	None	207.154.224.0/20
2023-05-12 03:23:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.7:80
2023-05-12 02:54:34	Open TCP Port	No	Censys	0	0	3	0	None	104.21.71.14:2082
2023-05-12 03:13:08	Malicious Co-Hosted Site	Yes	OpenPhish	0	0	3	0	None	OpenPhish [00p513-dev.github.io] https://www.openphish.com/feed.txt
2023-05-12 03:32:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.4:80
2023-05-12 03:32:08	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.5:80
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	eminent992 (Net ID: 00:14:5C:86:B3:9A)
2023-05-12 02:45:34	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'SC', u'country_tld': u'.us', u'ip': u'34.74.170.74', u'currency_name': u'Dollar', u'currency': u'USD', u'country_po
2023-05-12 02:52:10	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur u'origin': u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre. (type is "data")\n Antivirus vendors marked dropped file "TarA135.tmp" as clean (type is "data")\n Antivirus vendors marked dropped fi u'description': u'"iexplore.exe" reads file "c:\\windows\\fonts\\staticcache.dat"\n "iexplore.exe" reads file "c:\\users\\%osuser%\\ap "urlref_httpsgateway.pinata.cloudipfsbafybeifn47jywvhgzpcpcoitg5ftfimcmq6667ul2quva46dfyz3t6u3qqsharepoint.html" has type "HTML docume
2023-05-12 02:50:16	Internet Name	No	DNS Resolver	0	0	2	0	None	nwapi2.battleb0t.xyz
2023-05-12 03:32:02	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.2:8443
2023-05-12 02:55:28	Web Server	No	URLScan.io	0	1	2	0	None	Werkzeug/2.2.2 Python/3.10.9
2023-05-	WiFi	No	Wigle.net	0	0	4	0	None	

12 03:42:18	Access Point Nearby								WLAN (Net ID: 00:14:5C:86:B9:32)
2023-05-12 02:44:28	IP Address	No	DNS Resolver	0	0	2	0	None	185.199.111.153
2023-05-12 02:55:01	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:8080
2023-05-12 03:24:52	Country	No	Country Name Extractor	0	0	3	0	None	Netherlands
2023-05-12 02:52:24	Open TCP Port	No	Pulsedive	0	0	3	0	None	185.199.111.133:80
2023-05-12 03:23:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.11:8443
2023-05-12 02:55:11	Open TCP Port	No	Censys	0	0	2	0	None	87.248.157.102:2087
2023-05-12 03:18:26	Account on External Site	No	Account Finder	0	0	5	0	None	FatSecret (Category: health) https://www.fatsecret.com/member/Altpapier
2023-05-12 03:12:51	Raw Data from RIRs	No	numverify	0	0	3	0	None	{u'international_format': u'+74955801111', u'local_format': u'84955801111', u'number': u'74955801111', u'valid': True, u'line_type': u
2023-05-12 02:44:51	Raw Data from RIRs	No	CRXcavator	1	0	1	0	None	[{"platform": "Chrome", "version": "1.0", "data": {"dangerousfunctions": {".insertBefore(": {"/tmp/agjliddikiapkkpacaacecphgdoplfop_1. "https://lh3.googleusercontent.com/wpEAZCTc19k3y0XQ7kjngo0zY2gDblkGn4E-sp41P9QZJyERCUErowcPq7IYEJDop6Nxk-Mnn5lJDVHm5TTOWMBpRw=w128-h12 golf game packed with challenging courses, custom hats, and a powerful level builder.", "icon": "https://lh3.googleusercontent.com/CJl developers of Boxel Rebound.", "icon": "https://lh3.googleusercontent.com/wJh9K6xTW1upb8nCKtceJ62mE4BWbS7o4RiQpNnxoATQ8sn5w6RIYK9e5B6v "https://lh3.googleusercontent.com/Wafwq7jbZDxfLNCG587_eBMy91NkmSP2JFA3b4hWobkUAplS41SaW08gHYd8vcamJ1EPG5gQMPoQ_VDoVTNT9wH-KQ=w128-h12
2023-05-12 02:59:45	Affiliate - Domain Whois	No	Whois	2	0	5	0	None	Domain Name: GOOGLEUSERCONTENT.COM Registry Domain ID: 1528918319_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.markmonitor.com Regist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By s
2023-05-12 03:18:57	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	55 2nd PMO (Net ID: 00:01:21:10:61:00)
2023-05-12 03:19:09	Account on External Site	No	Account Finder	0	0	6	0	None	BodyBuilding.com (Category: health) http://bodyspace.bodybuilding.com/login/
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:2095
2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0000rgb124.github.io
2023-05-12 02:54:34	Open TCP Port Banner	No	Censys	0	0	3	0	None	HTTP/1.1 403 Forbidden Date: <REDACTED> Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Frame-Op
2023-05-12 03:18:56	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:01:24:F2:E0:26)
2023-05-12 03:10:06	Malicious IP Address	Yes	VoIPBL OpenPBX IPs	0	1	2	0	None	VOIPBL Publicly Accessible PBX List [185.199.110.153] http://www.voipbl.org/update
2023-05-12 03:03:30	Co-Hosted Site - Domain Name	No	DNS Resolver	0	0	3	0	None	github.io
2023-05-12 02:53:49	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2023-05-11T17:57:31.398Z", "ip": "2606:50c0:8000::153", "location_updated_at": "2023-05-08T16:34:05.180048Z", "au 23T09:37:19.694810939Z"}, "mst.biuxbiu.design": {"record_type": "CNAME", "resolved_at": "2023-04-28T17:39:08.436586135Z"}, "kbau.dev": "resolved_at": "2023-03-21T00:19:55.315272389Z"}, "www.shaneporter.dev": {"record_type": "CNAME", "resolved_at": "2023-03-21T00:20:35. {"record_type": "CNAME", "resolved_at": "2023-01-04T12:37:43.534076338Z"}, "www.mtconnectcore.dev": {"record_type": "CNAME", "resolved "CNAME", "resolved_at": "2023-03-05T15:53:20.930987816Z"}, "www.jasonscotto.dev": {"record_type": "CNAME", "resolved_at": "2023-03-16T
2023-05-12 03:01:23	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.218): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:46:38	BGP AS Membership	No	RIPE	0	0	3	0	None	36459
2023-05-12 03:03:16	Internet Name	No	DNS Resolver	0	0	2	0	None	panel.battleb0t.xyz
2023-05-12 02:44:39	Internet Name	No	DNS Resolver	0	0	2	0	None	battleb0t.xyz
2023-05-	IPv6	No	Mnemonic	0	0	1	0	None	

12 02:53:15	Address		PassiveDNS						2606:50c0:8003::153
2023-05-12 02:54:14	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://kekw.battleb0t.xyz/
2023-05-12 02:53:38	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': {u'executable_process_memory_analysis': [], u'analysis_related_ur "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_FILEMAPSWITCH_MUTEX_2880"'}, {u'category': u'General', u'origin': u'Network Traffic' u'capec_id': None, u'attck_id': None, u'relevance': 7, u'threat_level': 0, u'type': 2, u'description': u'"src="https://www.facebook.co b}xy.N="internal.enableAutoEventOnScroll";var cc=ea(["data-gtm-yt-inspected-"])\nyy=["www.youtube.com"\n"www.youtube-nocookie.com"]\nz "data")\n Antivirus vendors marked dropped file "TarFB80.tmp" as clean (type is "data")'}, {u'category': u'Installation/Persistence',
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	ELSA1 (Net ID: 00:02:2D:21:83:7A)
2023-05-12 03:18:54	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	XFBSECA7HE6H (Net ID: 00:0D:67:66:08:15)
2023-05-12 03:10:05	Co-Hosted Site - Domain Name	No	DNS Resolver	2	0	4	0	None	ecash-pay.com
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	J-Snijders (Net ID: 00:0C:F6:25:03:E8)
2023-05-12 02:46:33	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:a2:98:ee:7c:0f:82:53:85:c9:ed:86:47:94:a7:aa:74:64 Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: 1A:62: 11:42:e6:c6:c6:df:61:d7:1c:e4:ca:7f:bc:9e:71:30:82:fe: d4:6f:58:81:ab:0e:55:97:bb:c1:5d:e3:30:ef:17:60:9b:37: 2f:f7:be:34:13:0e:a6:78:
2023-05-12 03:16:17	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	ayiu.xyz
2023-05-12 02:54:18	Linked URL - Internal	No	Web Spider	1	0	3	0	None	https://pics.battleb0t.xyz/images/withat_2.jpg
2023-05-12 03:18:53	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	vulcan (Net ID: 00:02:8A:AD:D0:F3)
2023-05-12 03:25:06	Internet Name	No	DNS Brute-forcer	0	0	1	0	None	panel.battleb0t.xyz
2023-05-12 03:42:18	WiFi Access Point Nearby	No	Wigle.net	0	0	4	0	None	EAP6005G (Net ID: 00:02:6F:EB:3F:8B)
2023-05-12 03:09:28	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	3	0	None	C=US,O=Let's Encrypt,CN=R3
2023-05-12 03:00:31	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	umac-64@openssh.com
2023-05-12 02:44:37	Internet Name	No	DNS Resolver	0	0	2	0	None	oldfluid.battleb0t.xyz
2023-05-12 03:00:42	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.53): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:45:42	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:50:55:6d:e5:64:92:a0:7f:d0:de:03:2b:af:77:c2:fc:fe Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: CB:34: 01:1a:ea:aa:63:1c:40:bd:2f:59:0a:34:b7:be:8a:f1:7e:27: 85:d0:0e:96:7f:f0:0b:eb:18:35:77:95:6b:27:bf:9c:18:72: 58:89:63:0e:ed:84:1b:cb:
2023-05-12 02:55:11	Software Used	Yes	Censys	0	0	2	0	None	cPanel cPanel
2023-05-12 03:01:19	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.166): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:53:32	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"X_Cache": "DISPLAY_UTF8", "X_Github_Request_Id": "DISPLAY_UTF8", "Age": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "X_Ser
2023-05-12 03:17:57	Malicious IP on Same Subnet	Yes	CINS Army List	0	0	4	0	None	cinsscore.com [34.148.96.0/20] http://cinsscore.com/list/ci-badguys.txt
2023-05-12 02:44:05	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=*.battleb0t.xyz

2023-05-12 03:00:53	Co-Hosted Site	No	HackerTarget	2	0	2	0	None	0031.github.io
2023-05-12 03:01:27	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.12): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:03	Open TCP Port	No	Censys	0	0	2	0	None	172.67.135.9:8080
2023-05-12 03:27:00	Web Technology	No	Web Server Identifier	0	0	3	0	None	Express
2023-05-12 03:17:05	Account on External Site	No	Account Finder	0	0	1	0	None	Chess.com (Category: gaming) https://www.chess.com/member/ayshoo
2023-05-12 02:45:59	Raw Data from RIRs	No	AbstractAPI	0	0	3	0	None	{u'city': u'Chicago', u'security': {u'is_vpn': False}, u'city_geoname_id': 4887398, u'region_geoname_id': 4896861, u'country': u'Unite
2023-05-12 02:45:04	Country	No	Country Name Extractor	0	0	3	0	None	United States
2023-05-12 02:54:51	Netblock Membership	No	Censys	0	0	3	0	None	34.74.160.0/20
2023-05-12 02:45:51	Physical Location	No	AbstractAPI	0	0	2	0	None	Montreal, Quebec, H4X, United States, North America
2023-05-12 03:18:49	WiFi Access Point Nearby	No	Wigle.net	0	0	3	0	None	Special Litigation (Net ID: 00:02:2D:2E:93:90)
2023-05-12 02:44:26	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:03:e6:77:f0:fb:1d:de:0e:93:d2:d9:e5:40:98:fb:b1:42 Signature Algorithm: ecdsa-wi 6D:D4:73:9D:63:2C:14:38:C7:1C:15:38:7A:3E:1C:B5: 3A:C9:C0:A8:02:21:00:C8:7B:89:3A:AC:D8:F0:69:E9: DE:74:9E:7E:74:A9:4E:43:C7:89:2C:62:
2023-05-12 02:53:44	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:15:41:ea:93:cd:8d:62:0f:07:0f:be:37:47:74:c1:ad:1b Signature Algorithm: sha256Wi Server Authentication, TLS Web Client Authentication X509v3 Basic Constraints: critical CA:FALSE X509v3 Subject Key Identifier: CE:03: c1:45:7a:6f:01:d6:e5:6b:4c:b1:72:55:a1:cc:c8:79:92:38: 80:4e:bb:ab:bb:48:59:61:91:04:3d:4f:6a:29:7c:c3:ea:6b: 3b:30:22:90:a8:7e:7e:06:
2023-05-12 02:54:20	Open TCP Port Banner	No	Censys	0	0	4	0	None	HTTP/1.1 404 Not Found Server: Netlify X-Nf-Request-Id: 01H04BK0BS0X0MXB72Y8AY7JTF Date: <REDACTED> Content-Length: 0
2023-05-12 03:00:48	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.96.66): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 03:01:43	Blacklisted IP on Same Subnet	Yes	Honeypot Checker	0	0	3	0	None	Honeypotproject (188.114.97.222): Search Engine Last Activity: 0 days ago Threat Level: 29
2023-05-12 02:54:00	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray