Date Found	Type	Risky Data Type	Module	Children	Correlations	Distance	Starred	Annotation	
2022-12-18 00:12:06	Physical Location	No	ipapi.co	1	0	2	0	None	Toronto, Ontario, ON, Canada, CA
2022-12-18 00:27:43	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.sk
2022-12-18 00:05:39	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	hook.plague.fun
2022-12-18 00:17:00	Web Content Type	No	Web Spider	0	0	4	0	None	application/javascript
2022-12-18 00:04:10	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-SH X509v3 Basic Constraints: critical CA:FALSE CT Precertificate SCTs: Signed Certificate Timestamp: Version : v1 (0x0) Log ID : E8:3E:D 30:45:02:21:00:d8:35:e0:5c:fe:c9:39:b4:06:5a:95:36:1c: 73:f4:85:1c:c5:6e:6b:ef:48:76:d6:7f:a3:fe:55:ed:82:7f: c5:02:20:7f:8c:86:3a:6f
2022-12-18 00:06:33	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.0:80
2022-12-18 00:06:44	Open TCP Port	No	Pulsedive	0	0	2	0	None	104.21.19.243:443
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	fanpop (Category: social) https://www.fanpop.com/fans/rasputain
2022-12-18 00:16:59	HTTP Headers	No	Web Spider	0	0	4	0	None	{"content-length": "26711", "accept-ranges": "bytes", "last-modified": "Fri, 12 Feb 2021 14:43:40 GMT", "connection": "keep-alive", "
2022-12-18 00:40:45	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namespro.ca
2022-12-18 00:08:36	Raw Data from RIRs	No	LeakIX	0	0	1	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'137.117.157.128', u'vendor': u'', u'port': u'80', u'transpo u'lon': 4.8975}, u'country_name': u'Netherlands', u'continent_name': u'Europe', u'region_name': u'North Holland'}, u'host': u'137.117
2022-12-18 00:07:06	Web Content	No	Web Spider	2	0	2	0	None	<!doctype html> <html lang=en> <title>403 Forbidden</title> <h1>Forbidden</h1> <p>You don't have the permission to access the rec
2022-12-18 00:06:42	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.190.129:8080
2022-12-18 00:09:54	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	brns.xyz
2022-12-18 00:11:56	Physical Location	No	ipapi.co	0	0	1	0	None	Campinas, Sao Paulo, SP, Brazil, BR
2022-12-18 00:09:34	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	formivankie.tk
2022-12-18 00:03:16	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-102.w90-116.abo.wanadoo.fr
2022-12-18 00:18:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.8:8443
2022-12-18 00:04:04	Web Technology	No	Tool - WhatWeb	0	0	1	0	None	Werkzeug
2022-12-18 00:18:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.12:8080
2022-12-18 00:16:26	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:12:31	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'compromised_ "IsoScope_c84_IE_EarlyTabStart_0xe68_Mutex"\n "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\Zon u'description': u'"urlblockindex_1_.bin" has type "data"- [targetUID: N/A]\n "RecoveryStore._5FC32A7B-771D-11ED-B8BD-0800278A77A4_.da "data"- Location: [%TEMP%\\~DFABD3E3197957479F.TMP]- [targetUID: 00000000-00003204]\n "EWM02H3X.txt" has type "ASCII text"- Location: u'threat_level': 1, u'type': 2, u'description': u'Potential IP "188.114.97.3" found in string "https://188.114.97.3/"\n Potential IP

									u'https://188.114.97.3/', u'submission_id': u'63922bb58f5d337c6c22e8a0', u'created_at': u'2022-12-08T18:23:49+00:00', u'filename': N u'Network Traffic', u'identifier': u'network-1', u'name': u'Contacts server', u'attck_id_wiki': None, u'threat_level_human': u'inform
2022-12-18 00:08:41	Physical Location	No	LeakIX	0	0	1	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:31:03	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@dynadot.com
2022-12-18 00:25:13	Malicious IP Address	Yes	MetaDefender	0	0	1	0	None	webroot.com [20.224.2.213]
2022-12-18 00:04:49	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.biz
2022-12-18 00:24:07	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse-contact@publicdomainregistry.com
2022-12-18 00:04:30	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	ns1.amenworld.com
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	denis (Net ID: 00:01:46:02:C4:4C)
2022-12-18 00:25:41	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-189.w90-116.abo.wanadoo.fr
2022-12-18 00:22:28	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.128:443
2022-12-18 00:09:38	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	1sygo.com.cdn.cloudflare.net
2022-12-18 00:32:59	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.225] https://www.virustotal.com/en/ip-address/81.88.52.225/information/
2022-12-18 00:21:02	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-
2022-12-18 00:04:04	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://rasputain.fr', u'http_status': 301, u'plugins
2022-12-18 00:13:35	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	noc@cloudflare.com
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	charmingsinfulbusinesses.distingindouser.repl.co
2022-12-18 00:09:43	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	alejandrocastillero.com.pa
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Conne
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:25:19	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [104.21.28.240]
2022-12-18 00:34:23	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.dynv6.net
2022-12-18 00:03:05	IPv6 Address	No	DNS Resolver	2	0	1	0	None	2606:4700:3035::6815:1bf2
2022-12-18 00:13:56	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:06:31	Company Name	No	Company Name Extractor	0	0	2	0	None	ENOM, INC.
2022-12-18	WiFi Access	No	Wigle.net	0	0	5	0	None	fse2 (Net ID: 00:01:38:A0:A1:09)

00:21:11	Point Nearby								
2022-12-18 00:15:47	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	keep-alive: timeout=5
2022-12-18 00:24:56	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.176
2022-12-18 00:03:09	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.226
2022-12-18 00:03:03	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.105
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	#LG@Vo1P*Service& (Net ID: 00:01:36:57:A4:17)
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:13:38	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	info@indiantypefoundry.com
2022-12-18 00:21:02	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:04:47	Raw Data from RIRs	No	Maltiverse	3	0	2	0	None	{u'asn_registry': u'arin', u'country_code': u'US', u'classification': u'whitelist', u'asn_country_code': u'US', u'is_open_proxy': Fal
2022-12-18 00:20:36	Raw Data from RIRs	No	Censys	0	0	1	0	None	{"last_updated_at": "2022-11-17T13:21:29.012Z", "ip": "137.117.157.128", "location_updated_at": "2022-12-18T00:20:33.438254Z", "autor
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	tradingview (Category: finance) https://www.tradingview.com/u/rasputain/
2022-12-18 00:09:53	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	brilliantposts.com
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:8880
2022-12-18 00:05:38	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	www.plague.fun
2022-12-18 00:25:45	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	dominiando.us
2022-12-18 00:21:23	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:4700:3032::/48
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:21:37	Open TCP Port	No	Censys	0	0	2	0	None	20.226.83.185:80
2022-12-18 00:34:26	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.230] https://www.virustotal.com/en/ip-address/81.88.52.230/information/
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:80
2022-12-18 00:02:54	Domain Whois	No	Whois	8	0	1	0	None	Domain Name: ZEROTWO-BEST-WAIFU.ONLINE Registry Domain ID: D266274377-CNIC Registrar WHOIS Server: whois.enom.com Registrar URL: http 2022-12-18T00:02:53.0Z <<< For more information on Whois status codes, please visit https://icann.org/epp >>> IMPORTANT INFORMATION A FOR PRIVACY Registrant State/Province: Paris Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: FR Registrant Phone: RE only, that is, to assist you in obtaining information about or related to a domain name registration record. We make this informatior
2022-12-18 00:24:59	Malicious IP Address	Yes	VirusTotal	0	0	2	0	None	VirusTotal [172.67.169.215] https://www.virustotal.com/en/ip-address/172.67.169.215/information/
2022-12-18 00:31:45	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.online
2022-12-18	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'

00:21:44									
2022-12-18 00:04:28	Raw DNS Records	No	DNS Raw Records	0	0	1	0	None	zerotwo-best-waifu.online. 900 IN NS ns2.amenworld.com. zerotwo-best-waifu.online. 900 IN NS ns1.amenworld.com.
2022-12-18 00:21:34	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-(
2022-12-18 00:22:11	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-07-16T13:05:15.855Z", "ip": "81.88.52.232", "location_updated_at": "2022-12-18T00:22:08.060556Z", "autonomo
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	InterSolar (Net ID: 00:00:00:00:83:B5)
2022-12-18 00:25:06	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	81.88.48.111
2022-12-18 00:03:33	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3236.webapps.net
2022-12-18 00:02:50	IP Address	No	Mnemonic PassiveDNS	13	0	1	0	None	20.226.56.97
2022-12-18 00:12:19	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'172.67.190.129', u'currency_name': u'Dollar', u'currency': u'CAD', u'country
2022-12-18 00:02:48	IP Address	No	Mnemonic PassiveDNS	77	0	1	0	None	188.114.96.1
2022-12-18 00:27:23	Physical Location	No	MetaDefender	0	0	2	0	None	Medellin, Colombia
2022-12-18 00:03:10	SSL Certificate Host Mismatch	Yes	SSL Certificate Analyzer	0	0	1	0	None	*.webapps.net, webapps.net
2022-12-18 00:21:20	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:13:04	Search Engines Web Content	No	DuckDuckGo	0	0	3	0	None	{ "Abstract" : "Wanadoo was the Internet service provider division of Orange S.A. It operated in France, Spain, the United Kingdom, E first appeared in an internal project at France T\u00e9l\u00e9com, much in line with a number of other such projects such as France A Website", "value" : "http://www.orange.fr", "wiki_order" : "208" }], "meta" : [{ "data_type" : "string", "label" : "article_title", { "FirstURL" : "http://www.orange.fr", "Icon" : { "Height" : 16, "URL" : "/i/orange.fr.ico", "Width" : 16 }, "Result" : "<a href=\"ht
2022-12-18 00:12:49	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'188.114.97.9', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2022-12-18 00:09:21	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.7.179:80
2022-12-18 00:22:07	Malicious Internet Name	Yes	Cleanbrowsing.org	0	1	2	0	None	Blocked by Cleanbrowsing.org [autoconfig.zerotwo-best-waifu.online]
2022-12-18 00:04:00	Physical Location	No	ipstack	0	0	1	0	None	Brazil
2022-12-18 00:18:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.1:8080
2022-12-18 00:02:39	IP Address	No	SpiderFoot UI	14	0	0	0	None	40.113.112.131
2022-12-18 00:04:24	Raw Data from RIRs	No	Hybrid Analysis	0	0	1	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 15, u'threat_score': None, u'compromis "Local\\SM0:4324:304:WilStaging_02"\n "Local\\ChromeProcessSingletonStartup!"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\ChromeProces Data\\Default\\Network\\90765a85-28a0-4fa7-b3ad-27a06095474a.tmp]- [targetUID: 00000000-00002116]\n "load_statistics.db-wal" has type "Last Browser" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Last Browser]- [targetUID: 00000000-00004324]\ "http://20.224.2.213/"\n Pattern match: "http://20.224.2.213"'}, {u'category': u'External Systems', u'origin': u'External System', u' [%TEMP%\\4324_1765292486\\auto_open_controller.js]- [targetUID: 00000000-00004324]\n Dropped file: "edge_tracking_page_validator.js" 1152268696\n "C:\\Users\\HAPUBWS\\AppData\\Local\\Microsoft\\Edge\\User Data\\Crashpad\\reports" (Indicator: "microsoft\\edge\\user c
2022-12-18 00:12:23	Physical Location	No	ipapi.co	0	0	2	0	None	Campinas, Sao Paulo, SP, Brazil, BR
2022-12-18 00:09:22	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.6:8443
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F0:97:C1)
2022-12-18	Affiliate Description	No	DuckDuckGo	0	0	3	0	None	Orange S.A.

00:13:04	- Category								
2022-12-18 00:23:19	Country	No	Country Name Extractor	0	1	2	0	None	Switzerland
2022-12-18 00:19:20	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [u'mydoom', u'upx'], u'crowdstrike_ai': None, u'total_processes': 2, u'threat_score': 1 "193.175.80.161:25"\n "17.171.2.72:25"\n "17.171.2.68:25"\n "17.172.224.47:25"\n "217.12.15.96:80"\n "209.202.251.1:80"\n "162.209.10 "\\Sessions\\1\\BaseNamedObjects\\Local\\WininetConnectionMutex"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\WininetProxyRegistryMutex .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)\nHost: search.lycos.com\nConnection: Keep-Alive"\n "GET /?fr=altavista H PHPSESSID=nk5rco1pvk06lvada52c9f0op3"\n "GET /default.asp?lpv=1&loc=searchhp&tab=web&query=reply+unicode.org HTTP/1.1\nAccept: */*\nA .NET4.0C; .NET4.0E)\nHost: search.lycos.com\nConnection: Keep-Alive\nCookie: PHPSESSID=nk5rco1pvk06lvada52c9f0op3"\n "GET /default.as Media Center PC 6.0; .NET4.0C; .NET4.0E)\nHost: search.yahoo.com\nConnection: Keep-Alive\nCookie: B=dbc2c8lcc2fkn&b=3&s=um; sSN=K6M9X
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conn
2022-12-18 00:06:51	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.137.37:443
2022-12-18 00:21:37	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 200 OK X-Powered-By: Express Access-Control-Allow-Origin: * Accept-Ranges: bytes Cache-Control: public, max-age=0 Last-Modif
2022-12-18 00:03:39	Malicious Internet Name	Yes	CloudFlare Malware DNS	0	1	1	0	None	Blocked by CloudFlare DNS [misogyny.wtf]
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:8880
2022-12-18 00:20:59	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T20:29:44.410Z", "ip": "2606:4700:3033::6815:1cf0", "location_updated_at": "2022-12-03T13:27:53.341659 {"record_type": "AAAA", "resolved_at": "2022-10-28T15:43:22.731629900Z"}, "unafinen.cf": {"record_type": "AAAA", "resolved_at": "2022 "www.eshutter.com.cdn.cloudflare.net": {"record_type": "AAAA", "resolved_at": "2022-12-04T15:53:55.557031240Z"}, "makecoloradohome.co 08T14:50:03.504145435Z"}, "garageshedcarportbuilder.com": {"record_type": "AAAA", "resolved_at": "2022-12-13T13:26:04.059048706Z"}, " "2022-12-15T13:57:52.400597943Z"}, "naresdiapormasit.ga": {"record_type": "AAAA", "resolved_at": "2022-12-07T15:07:35.636246521Z"}, " "resolved_at": "2022-11-30T16:55:45.682027528Z"}, "webdisk.nensi.eu": {"record_type": "AAAA", "resolved_at": "2022-11-13T14:26:06.988 "resolved_at": "2022-12-09T16:41:18.225114327Z"}, "www.thedollhousemuseum.com.cdn.cloudflare.net": {"record_type": "AAAA", "resolved_
2022-12-18 00:23:19	Country	No	Country Name Extractor	0	0	5	0	None	Italy
2022-12-18 00:04:01	Country	No	Country Name Extractor	0	0	4	0	None	United States
2022-12-18 00:12:22	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 6, u'search_terms': [{u'id': u'host', u'value': u'188.114.97.3'}], u'result': [{u'environment_id': 120, u'job_id': u'63922 u'environment_description': u'Windows 7 32 bit', u'threat_score': 2, u'verdict': u'suspicious', u'submit_name': u'sample.url', u'sha2
2022-12-18 00:21:37	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 200 OK Server: Werkzeug/2.2.2 Python/3.9.11 Date: <REDACTED> Content-Type: text/html; charset=utf-8 Content-Length: 29 Conne
2022-12-18 00:02:50	Domain Registrar	No	Whois	0	0	1	0	None	ENOM, INC.
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	LF-X1U.00014A10EF0C (Net ID: 00:01:4A:10:EF:0C)
2022-12-18 00:06:35	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.0:443
2022-12-18 00:11:19	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	wasp.plague.fun
2022-12-18 00:03:08	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.196
2022-12-18 00:14:47	Internet Name - Unresolved	No	VirusTotal	0	0	1	0	None	api.plague.fun
2022-12-18 00:12:26	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'NJ', u'country_tld': u'.us', u'ip': u'2606:4700:3031::6815:7b3', u'currency_name': u'Dollar', u'currency': u'USD',
2022-12-18 00:23:30	URL (Uses Javascript)	No	Page Information	0	0	3	0	None	http://webmail.zerotwo-best-waifu.online
2022-12-18	Raw Data from RIRs	No	LeakIX	0	0	1	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'51.103.210.236', u'vendor': u'', u'port': u'80', u'transpor

00:08:42									{u'region_iso_code': u'CH-ZH', u'country_iso_code': u'CH', u'city_name': u'Zurich', u'location': {u'lat': 47.3682, u'lon': 8.5671}, u {u'content-length': u'94', u'server': u'Werkzeug/2.2.2 Python/3.10.6'}, u'length': 0, u'favicon_hash': u'', u'root': u''}, u'tags': [u'key': u''}, u'software': {u'modules': [{u'version': u'3.10.6', u'name': u'Python', u'fingerprint': u''}], u'version': u'2.2.2', u'c Length: 94\r\nConnection: close\r\n\n\nRoses are red\n \nViolets are blue\n \nWasp is happy\n \nBecause he grabb
2022-12-18 00:09:46	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.17:8443
2022-12-18 00:21:02	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date"
2022-12-18 00:03:13	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-97.w90-116.abo.wanadoo.fr
2022-12-18 00:08:30	Physical Location	No	LeakIX	0	0	1	0	None	United States
2022-12-18 00:12:19	Physical Location	No	ipapi.co	0	0	2	0	None	Toronto, Ontario, ON, Canada, CA
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	CATYLN (Net ID: 00:01:38:86:06:1F)
2022-12-18 00:12:41	Physical Location	No	ipapi.co	0	0	2	0	None	Toronto, Ontario, ON, Canada, CA
2022-12-18 00:08:42	Internet Name	No	DNS Resolver	0	0	2	0	None	www.zerotwo-best-waifu.online
2022-12-18 00:03:24	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-114.w90-116.abo.wanadoo.fr
2022-12-18 00:14:47	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.160:80
2022-12-18 00:02:50	IPv6 Address	No	Mnemonic PassiveDNS	13	0	1	0	None	2a06:98c1:3120::1
2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:06:52	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': u'Windows Gui', u'classification_tags': [u'evasive'], u'crowdstrike_ai': None, u'total_processes': 7, u'threat_score' "HKLM\\SOFTWARE\\POLICIES\\MICROSOFT\\SYSTEMCERTIFICATES\\DISALLOWED\\CTLS"; Key: "")\n "google.exe" (Path: "HKLM\\SOFTWARE\\POLICIES u'description': u'"CorExitProcess" (Indicator: "ExitProcess")\n "FlsSetValue" (Indicator: "FlsSetValue")\n "FlsGetValue" (Indicator: u'identifier': u'binary-26', u'name': u'The input sample possibly contains the RDTSCP instruction', u'attck_id_wiki': u'https://attac u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 0, u'description': u'"8ae28c30669d3cffca54e317362 [eax], al,addbyte ptr [eax], al,addbyte ptr [eax], al,addbyte ptr [eax], al,addbyte ptr [eax], al,addbyte ptr [eax], al,addbyte ptr [u'description': u'Spawned process "ASYNCCLIENT.EXE" (UID: 00000000-00002976)\n Spawned process "cmd.exe" with commandline "/c schtask
2022-12-18 00:08:44	Open TCP Port	No	LeakIX	0	0	1	0	None	20.224.2.213:80
2022-12-18 00:12:18	Physical Location	No	ipapi.co	0	0	2	0	None	Newark, New Jersey, NJ, United States, US
2022-12-18 00:03:06	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	api.plague.fun
2022-12-18 00:25:43	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-193.w90-116.abo.wanadoo.fr
2022-12-18 00:59:50	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	misogyny.org
2022-12-18 00:03:09	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:2f:49:07:90:93:a8:06:e6:05:0c:26:40:50:ef:77:d7:82 Signature Algorithm: sha256W Identifier: keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6 Authority Information Access: OCSP - URI:http://r3.o.le
2022-12-18 00:03:36	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom2888 (Net ID: 00:01:38:85:BD:9E)
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:37:29	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.242] https://www.virustotal.com/en/ip-address/81.88.52.242/information/
2022-12-	Raw Data	No	ipapi.co	0	0	2	0	None	

18 00:12:36	from RIRs								{u'region_code': u'PAC', u'country_tld': u'.fr', u'ip': u'90.116.166.104', u'currency_name': u'Euro', u'currency': u'EUR', u'country_
2022-12-18 00:03:05	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	hook.plague.fun
2022-12-18 00:09:39	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.9:443
2022-12-18 00:09:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.8:443
2022-12-18 00:03:11	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.238
2022-12-18 00:09:45	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.9:80
2022-12-18 00:02:58	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:b5:ee:aa:9f:a9:bb:86:86:d8:5d:7e:c7:71:cb:57:b5:27 Signature Algorithm: sha256W ac:91:71:d6:e0:98:69:40:a1:f7:fc:ef:bd:5e:7b:66:85:7a: ed:35:a3:82:d2:9e:37:a2:ca:bc:c1:cf:6e:5b:d9:04:ae:28: e8:a2:05:a4:f8:e3:e6:35
2022-12-18 00:20:56	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:09:21	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'https', u'event_type': u'service', u'ip': u'104.21.7.179', u'vendor': u'', u'port': u'443', u'transpor u'detected': False, u'version': u'TLSv1.3'}, u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'banner': u'', u'fingerprint': u''}, u'os': u'', u'name': u'cloudflare', u'fingerprint': u''}}, u'event_fingerprint': u'6d1f2e7c9ee98731fedbc44a39cb147fd61faf139899b932cc s=w35ltoLfxmzU%2BLV0Iye9ADkcnmaLFoVg14AsLDdaYVQbu7Qcj9ZVhQ%2BUkPijYfYXTatno9IkxZkM2oOlyTVpqqS%2F5h%2BXEfPuLVAux5gwez0%2FN5SFcQ%2Frxo u'0000000000000000000000000000000000000000000000000000000000000000', u'certificate': {u'domain': [u'*.marcz.com.mx', u'marcz.com.mx'], nel","max_age":604800}\r\nServer: cloudflare\r\nCF-RAY: 7642c4fe2921dd71-LHR\r\nalt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400\ 04T23:59:59Z', u'key_size': 256, u'issuer_name': u'Cloudflare Inc ECC CA-3', u'fingerprint': u'1b4fde192766931f3a23145b88a1f9838dfdc8
2022-12-18 00:14:36	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 protoc
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	d68f9904-2e3d-4090-854b-ff8a0a1bfcdf.id.repl.co
2022-12-18 00:07:04	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 4, u'search_terms': [{u'id': u'host', u'value': u'81.88.52.232'}], u'result': [{u'environment_id': 100, u'job_id': u'62da6 7 64 bit', u'threat_score': 77, u'verdict': u'suspicious', u'submit_name': u'sample.url', u'sha256': u'56a636800d3684f91fbe334333b8bf
2022-12-18 00:12:19	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 15, u'threat_score': 35, u'compromised "Local\\SM0:7844:120:WilError_01"\n "Local\\ChromeProcessSingletonStartup!"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:7844:120:W Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Network\\1a8f52a0-4099-4402-b391-421fc08473ee.tmp]- [targetUID: 00000 7175f0cedd28.tmp]- [targetUID: 00000000-00007844]\n "870b1947-b37b-41dc-a12d-92436625da90.tmp" has type "UTF-8 Unicode text with very u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 2, u'description': u'Pattern mat [%TEMP%\\7844_1603751462\\product_page.js]- [targetUID: 00000000-00007844]\n Dropped file: "edge_driver.js" - Location: [%TEMP%\\7844 "C:\\Users\\HAPUBWS\\AppData\\Local\\Microsoft\\Edge\\User Data\\Default\\EdgePushStorageWithConnectTokens" (Indicator: "microsoft\\e
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	new.friendsquito.repl.co
2022-12-18 00:08:38	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2022-12-18 00:16:27	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-SH X509v3 Basic Constraints: critical CA:FALSE CT Precertificate SCTs: Signed Certificate Timestamp: Version : v1 (0x0) Log ID : E8:3E:D 30:45:02:21:00:d8:35:e0:5c:fe:c9:39:b4:06:5a:95:36:1c: 73:f4:85:1c:c5:6e:6b:ef:48:76:d6:7f:a3:fe:55:ed:82:7f: c5:02:20:7f:8c:86:3a:6f
2022-12-18 00:19:16	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 0, u'threat_score': None, u'compromise u'malicious', u'minor_os_version': None, u'domains': [], u'extracted_files': [], u'type_short': [u'peexe', u'executable']}, {u'subsys "Local\\ZonesLockedCacheCounterMutex"\n "Local\\ZonesCacheCounterMutex"\n "\\Sessions\\1\\BaseNamedObjects\\RasPbFile"\n "\\Sessions\ process "auwtnjty.exe" with commandline "/d"C:\\4623e1ce31a8671e59640e83fc545a5f19e167c31cfc6e8d097864c7a4 ..." (UID: 00021867-000037 "Network" (Path: "HKCU\\WOW6432NODE\\CLSID\\{208D2C60-3AEA-1069-A2D7-08002B30309D}\\SHELLFOLDER")\n "<Input Sample>.exe" touched "Rec 4B2D810D956B}\\SHELLFOLDER")\n "<Input Sample>.exe" touched "Other Users Folder" (Path: "HKCU\\WOW6432NODE\\CLSID\\{B4FB3F98-C1EA-428 "72.167.238.29:25"\n "170.146.221.13:25"\n "74.208.5.20:25"\n "184.171.128.11:25"\n "69.168.106.33:25"\n "185.37.226.254:25"\n "68.87
2022-12-18 00:31:50	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.133:443
2022-12-18 00:04:11	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com

2022-12-18 00:21:09	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:
2022-12-18 00:19:08	Physical Location	No	ipapi.co	0	0	3	0	None	Florence, Tuscany, 52, Italy, IT
2022-12-18 00:16:53	Affiliate - Company Name	No	Company Name Extractor	0	0	4	0	None	CloudFlare, Inc.
2022-12-18 00:14:47	Internet Name - Unresolved	No	VirusTotal	0	0	1	0	None	hook.plague.fun
2022-12-18 00:06:15	Linked URL - Internal	No	Web Spider	0	0	1	0	None	http://misogyny.wtf
2022-12-18 00:07:06	Web Content	No	Web Spider	1	0	2	0	None	<script> window.location = `https://discord.gg/wasp` </script>
2022-12-18 00:16:27	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-SH X509v3 Basic Constraints: critical CA:FALSE CT Precertificate SCTs: Signed Certificate Timestamp: Version : v1 (0x0) Log ID : E8:3E:D 30:45:02:21:00:d8:35:e0:5c:fe:c9:39:b4:06:5a:95:36:1c: 73:f4:85:1c:c5:6e:6b:ef:48:76:d6:7f:a3:fe:55:ed:82:7f: c5:02:20:7f:8c:86:3a:6f
2022-12-18 00:03:08	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.224
2022-12-18 00:14:35	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 5.0 Description: The DES and Triple DES ciphers, as used in the T
2022-12-18 00:04:45	Malicious IP Address	Yes	Maltiverse	0	1	2	0	None	Maltiverse [172.67.190.129]
2022-12-18 00:09:53	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	braseciscaditbest.cf
2022-12-18 00:03:32	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3233.webapps.net
2022-12-18 00:08:26	Physical Location	No	Fraudguard	0	0	2	0	None	United States, Missouri, Kansas City
2022-12-18 00:04:30	Raw DNS Records	No	DNS Raw Records	0	0	1	0	None	zerotwo-best-waifu.online. 900 IN TXT "v=spf1 include:spf.webapps.net ~all"
2022-12-18 00:13:46	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	domain.operations@web.com
2022-12-18 00:24:57	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.184
2022-12-18 00:09:51	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	bestlifeindividualsupportservices.com
2022-12-18 00:21:02	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-O
2022-12-18 00:25:16	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [104.21.27.242] https://www.virustotal.com/en/ip-address/104.21.27.242/information/
2022-12-18 00:22:28	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.128:8443
2022-12-18 00:27:23	Malicious IP Address	Yes	MetaDefender	0	0	2	0	None	webroot.com [188.114.97.9]
2022-12-18 00:09:42	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	ahedeyay.work
2022-12-18 00:21:02	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-O
2022-12-18 00:13:04	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 protoc
2022-12-	Company	No	Company Name	4	0	2	0	None	Identity Digital Inc.

18 00:06:31	Name		Extractor						
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:09:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.9:8080
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pancakes (Net ID: 00:00:48:67:6D:D1)
2022-12-18 00:03:06	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.183
2022-12-18 00:13:47	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	info@sonexo.nl
2022-12-18 00:03:06	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.181
2022-12-18 00:09:53	Malicious IP on Same Subnet	Yes	abuse.ch	0	0	3	0	None	abuse.ch Feodo Tracker (IP) [90.116.0.0/16] https://feodotracker.abuse.ch/downloads/ipblocklist.txt
2022-12-18 00:39:26	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.6] https://www.virustotal.com/en/ip-address/188.114.96.6/information/
2022-12-18 00:18:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.11:443
2022-12-18 00:25:10	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	81.88.58.201
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	FriendFinder-X (Category: dating) https://www.friendfinder-x.com/profile/rasputain
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	php-web-server-1.0635412.repl.co
2022-12-18 00:08:24	Netblock Membership	No	RIPE	0	0	2	0	None	188.114.97.0/24
2022-12-18 00:22:07	Open TCP Port	No	Censys	0	1	2	0	None	34.149.204.188:9000
2022-12-18 00:08:56	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.0:443
2022-12-18 00:03:02	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.100
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:03:B5:60)
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	onlinepichinchabankingecuinfor--ecuador1.repl.co
2022-12-18 00:09:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.9:443
2022-12-18 00:03:26	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	192.204.149.34.bc.googleusercontent.com
2022-12-18 00:03:11	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:09:40	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	a-prime-sp-health.fyi
2022-12-18 00:06:15	HTTP Status Code	No	Web Spider	0	0	1	0	None	200
2022-12-18 00:03:04	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.108

2022-12-18 00:25:57	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.org
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:00:21:01)
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:01:24:F2:E2:35)
2022-12-18 00:03:11	Affiliate - Internet Name	No	DNS Resolver	1	0	2	0	None	lhcp3232.webapps.net
2022-12-18 00:21:58	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2a06:98c1:3120::/48
2022-12-18 00:13:34	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	noc@cloudflare.com
2022-12-18 00:21:20	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-(
2022-12-18 00:09:52	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.20:8443
2022-12-18 00:17:00	Web Content	No	Web Spider	1	0	4	0	None	/*! * Bootstrap v3.4.1 (https://getbootstrap.com/) * Copyright 2011-2019 Twitter, Inc. * Licensed under the MIT license */ if("undefi {o.detach().trigger("closed.bs.alert").remove()}t&&t.preventDefault(),o.length||(o=e.closest(".alert")),o.trigger(t=s.Event("close.bs i=this.$element.find("input");"radio"==i.prop("type")?(i.prop("checked")&&(t=!1),e.find(".active").removeClass("active"),this.$elemer document.documentElement)&&this.$element.on("mouseenter.bs.carousel",p.proxy(this.pause,this)).on("mouseleave.bs.carousel",p.proxy(th this.pause().cycle():this.slide(i<t?"next":"prev",this.$items.eq(t))},c.prototype.pause=function(t){return t||(this.paused=!0),this.$ t=p.fn.carousel;p.fn.carousel=r,p.fn.carousel.Constructor=c,p.fn.carousel.noConflict=function(){return p.fn.carousel=t,this};var e=fu {return this.$element.hasClass("width")?"width":"height"},r.prototype.show=function(){if(!this.transitioning&&!this.$element.hasClass
2022-12-18 00:22:07	Open TCP Port	No	Censys	0	0	2	0	None	34.149.204.188:80
2022-12-18 00:08:30	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.52.223:21
2022-12-18 00:13:04	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 5.0 Description: The DES and Triple DES ciphers, as used in the T
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:443
2022-12-18 00:21:37	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["29"], "_encoding": {"Date": "DISPLAY_UTF8", "Content_Length": "DISPLAY_UTF8", "Connection": "DISPLAY_UTF8", "Cor
2022-12-18 00:16:53	Company Name	No	Company Name Extractor	0	0	3	0	None	Cloudflare\, Inc.
2022-12-18 00:24:47	Physical Location	No	MetaDefender	0	0	1	0	None	Campinas, Brazil
2022-12-18 00:20:49	Physical Location	No	Censys	1	0	1	0	None	Zurich, Zurich, 8000, Switzerland, Europe
2022-12-18 00:02:56	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: e5:46:5a:b1:fb:47:13:cc:0e:4e:81:45:49:c8:68:c3 Signature Algorithm: sha256WithRSA keyid:D5:FC:9E:0D:DF:1E:CA:DD:08:97:97:6E:2B:C5:5F:C5:2B:F5:EC:B8 Authority Information Access: OCSP - URI:http://ocsp.pki.goog/s/gts
2022-12-18 00:40:43	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: misogyny.ca Registry Domain ID: 95142585-CIRA Registrar WHOIS Server: whois.ca.fury.ca Registrar URL: http://www.namespr REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please ask the Registrar of Rec slns1.namespro.ca Name Server: slns2.namespro.ca DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icanr Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Other contacts of the queri REDACTED FOR PRIVACY Billing State/Province: REDACTED FOR PRIVACY Billing Postal Code: REDACTED FOR PRIVACY Billing Country: REDACTED
2022-12-18 00:13:56	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2086
2022-12-18 00:12:09	Physical Location	No	ipapi.co	0	0	2	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	07:55:46 (Net ID: 00:02:2D:05:BB:87)
2022-12-18	Web Content	No	Web Spider	0	0	3	0	None	body { background-color: #3c4359; background: linear-gradient(140deg, #3c4359, #000); background-size: 400% 400%; -webkit-animation:

00:07:18									
2022-12-18 00:08:30	IP Address	No	LeakIX	24	0	1	0	None	188.114.96.9
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	089070 (Net ID: 00:02:2D:08:90:70)
2022-12-18 00:05:57	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	www.plague.fun
2022-12-18 00:10:05	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	https://zerotwo-best-waifu.online/778112985743251/wap/enner/injector
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpeedStream (Net ID: 00:01:24:F0:82:16)
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	onlinebankingpichinchaaccount--ecuador0.repl.co
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:2052
2022-12-18 00:02:43	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:f8:40:07:a9:2a:29:fa:95:e2:5f:ea:f2:e9:75:79:57:8e Signature Algorithm: sha256W with-SHA256 30:44:02:20:61:29:22:AC:4F:7C:30:86:DB:CB:A5:62: 1A:74:E6:F0:17:04:90:2B:D9:04:A5:D2:DA:A2:8A:F3: A8:7C:6C:79:02:20:6F:4(
2022-12-18 00:14:26	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:27:43	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: plague.pro Registry Domain ID: 63d81ab88f224721bf7defd24d12c687-DONUTS Registrar WHOIS Server: whois.reg.com Registrar U Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record i under no circumstances may this data be used to: a) allow, enable, or otherwise support the transmission by e-mail, telephone, or fac upon request, where it can be reasonably confirmed that the requester holds a specific legitimate interest and a proper legal basis f Postal Code: 123007 Admin Country: RU Admin Phone: +7.4955801111 Admin Phone Ext: Admin Fax: +7.4955801111 Admin Fax Ext: Admin Email
2022-12-18 00:12:31	Physical Location	No	ipapi.co	0	0	2	0	None	Toronto, Ontario, ON, Canada, CA
2022-12-18 00:12:13	Physical Location	No	ipapi.co	0	0	2	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2022-12-18 00:03:32	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3234.webapps.net
2022-12-18 00:09:52	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.20:443
2022-12-18 00:06:24	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_HASHFILESWITCH_MUTEX"'}, {u'category': u'General', u'origin': u'Network Traffic', u u'"GET /main/https:/pixiv.karakuri.ai/api/chats/popup.js HTTP/1.1\nAccept: text/html, application/xhtml+xml, */*\nAccept-Language: en Characteristics', u'origin': u'Binary File', u'identifier': u'binary-37', u'name': u'Drops files inside appdata directory', u'attck_i archive data Windows 2000/XP setup 62919 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%7 Cabinet archive data Windows 2000/XP setup 62919 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"- Locat sentry_key=615192fd532445bfbbbe966cd7131791"\nReplit-Cluster: global\nServer: nginx/1.20.1\nStrict-Transport-Security: max-age=748816
2022-12-18 00:27:45	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	plague.pro@regprivate.ru
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:2086
2022-12-18 00:21:20	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:16:40	Blacklisted Affiliate Internet Name	Yes	DNS for Family	0	0	2	0	None	DNS for Family [dns2.registrar-servers.com]
2022-12-18 00:31:07	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.dog
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SurfandSip (Net ID: 00:02:2D:03:7C:7A)
2022-12-18 00:21:10	WiFi Access	No	Wigle.net	0	0	5	0	None	myLGNet8682 (Net ID: 00:01:36:5B:86:80)

	Point Nearby								
2022-12-18 00:02:47	Raw Data from RIRs	No	grep.app	0	0	1	0	None	{u'repo': {u'raw': u'stamparm/maltrail'}, u'total_matches': {u'raw': u'1'}, u'content': {u'snippet': u'<table class="highlight-table'
2022-12-18 00:03:26	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	191.204.149.34.bc.googleusercontent.com
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:03:B5:60)
2022-12-18 00:21:06	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: -
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet8FBA (Net ID: 00:01:36:5C:8F:B8)
2022-12-18 00:14:32	Country	No	Country Name Extractor	0	1	3	0	None	Germany
2022-12-18 00:20:36	BGP AS Membership	No	Censys	0	0	1	0	None	8075
2022-12-18 00:28:47	Physical Location	No	MetaDefender	0	0	3	0	None	Firenze, Italy
2022-12-18 00:09:45	Physical Location	No	LeakIX	0	0	2	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:09:51	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	billing.cross.network
2022-12-18 00:06:04	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	cloudflare.com
2022-12-18 00:25:13	Affiliate - IP Address	No	DNS Look-aside	0	0	3	0	None	81.88.48.101
2022-12-18 00:12:19	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+3544212434
2022-12-18 00:23:09	Raw Data from RIRs	No	CRXcavator	1	0	1	0	None	[{"platform": "Chrome", "version": "0.3", "data": {"webstore": {"website": "", "rating": 5, "privacy_policy": "http://newtabwallpaper "http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/", "https://nvd.nist.gov/vuln/detail/CVE-2015-9251", "http://research "/tmp/mlbijjeimhmdbdomoalcpnelmlfjjclj_0.3/start/js/libs/jquery.min.js"}], "related": {"fnenbhacmjcbgjpldpmmpdkggbnnpdpg": {"rating": Fortnite Game Custom page, with bookmarks, apps, games and Fortnite pride wallpaper.", "icon": "https://lh3.googleusercontent.com/Cti e365-rj-sc0x00ffffff", "rating_users": 1338, "name": "Infinite Dashboard - New Tab like no other"}, "onjloafnnfndgpkdojhbhcebkpilfehi website.", "icon": "https://lh3.googleusercontent.com/O037nyE7ukNJ5iZXYe2qY1twLrqm05QgShmBWd65JWJ1NRGaMwj9cCwZ7gEHfSFEDuFMp7TCFoWcvq\ "ghabmoobnekiapiffifjdhgccbfbdgek": {"rating": 3.48, "users": 2000, "platform": "", "short_description": "The game features a map. We
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2082
2022-12-18 00:05:39	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "Local\\URLBLOCK_HASHFILESWITCH_MUTEX"\n "\\Sessions\\1\\BaseNamedObjects\\UpdatingNewTabPageData"\n "\\Sessions\\1\\BaseNamedObjects u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 8, u'description': u'"CabCBF2.tmp" has type "Mic N/A]\n "llave_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUID: N/A]\n "gradient_1_.svg" has type "SVG Scalable Vect "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "search_1_.json" has type "JSON data"- [targetUID: u'f75edeec390f27707f95a0f28f71601e872894a104a9e846ff0277e3cf7918c42487c8ad8cd207aef81237e2e9c6a96abb4e42ec89ce3908f54bf357bdb6451e',
2022-12-18 00:09:47	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	auto-cash.xyz
2022-12-18 00:16:27	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3
2022-12-18 00:33:51	Similar Domain - Whois	No	Whois	0	0	2	0	None	Malformed request. >>> Last update of WHOIS database: 2022-12-18T00:33:51Z <<< Terms of Use: Access to Public Interest Registry WHOIS
2022-12-18 00:24:58	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.186
2022-12-18 00:03:10	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.234
2022-12-18 00:21:10	WiFi Access	No	Wigle.net	0	0	5	0	None	00:02:2D:05:7E:8A (Net ID: 00:02:2D:05:7E:8A)

	Point Nearby								
2022-12-18 00:16:57	HTTP Headers	No	Web Spider	0	0	2	0	None	{"content-length": "664", "content-encoding": "gzip", "accept-ranges": "bytes", "vary": "Accept-Encoding", "connection": "keep-alive"
2022-12-18 00:02:53	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:a4:99:c7:6c:cb:8c:60:87:12:4d:ac:6d:aa:bc:48:46:46 Signature Algorithm: ecdsa-w 00:b6:70:a5:8a:80:f9:65:63:f5:4e:8a:9f:00:55:5b:1c:61: af:79:57:92:51:0e:76:a7:d1:43:e6:9b:64:5c:22:3d:99:f7: f9:9b:ac:52:3e:73:11:67
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Rock Chalk (Net ID: 00:01:95:08:D8:04)
2022-12-18 00:03:18	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:32:13	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.top
2022-12-18 00:09:45	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	anininfio.ml
2022-12-18 00:04:30	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'banker', u'emotet', u'macros-on-open'], u'crowdstrike_ai': None, u'total_processes': u'capec_id': None, u'attck_id': None, u'relevance': 0, u'threat_level': 0, u'type': 9, u'description': u'Process "cmd.exe" with comma 72', u'name': u'Overview of unique CLSIDs touched in registry', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'cape "HKLM\\SOFTWARE\\CLASSES\\CLSID\\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\\TREATAS")\n "WINWORD.EXE" touched "Microsoft Word-Vorlage mi u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1204', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id' Function\n\nFunction qkdluw()\nOn Error Resume Next\nSet zdcpwns = juvqz\n If jjllf <= 288438056 Then\n bdcmw = jnsjsui * Sin(mido Then\n ijftw = paawbub * Sin(zulzjp) - qiwru - CInt(jsvcjuw + Rnd(637606491) + 646801169 + CDbl(928496469))\n nwlfcni = 69285864\nEnd
2022-12-18 00:21:17	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:
2022-12-18 00:21:20	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T16:59:24.849Z", "ip": "188.114.97.1", "location_updated_at": "2022-12-14T09:57:27.738993Z", "autonomo 01T13:38:25.278618273Z"}, "www.alvandcenter.com": {"record_type": "A", "resolved_at": "2022-11-07T12:46:16.283141371Z"}, "www.les1000 {"record_type": "A", "resolved_at": "2022-10-07T10:43:58.475530009Z"}, "les1000volets.com": {"record_type": "A", "resolved_at": "2022 28T15:05:14.014491568Z"}, "www.wolny.poker": {"record_type": "A", "resolved_at": "2022-10-16T17:06:44.448663582Z"}, "ritta.app": {"re "User_Agent": ["Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)"], "Accept": ["*/*"]}, "method": "GET", "uri": Key\",\"c771f0e4b54944bebf4261d44bd79a1e\");\nb.send(JSON.stringify(a));c.classList.add(\"feedback-hidden\");d.classList.remove(\"fee class=\"w-240 lg:w-full mx-auto mb-8 lg:px-8\">\n <div id=\"what-happened-section\" class=\"w-1/2 md:w-full\">\n <h2 class=\"text-3xl
2022-12-18 00:26:50	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [81.88.52.232]
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	MySpace (Category: social) https://myspace.com/rasputain
2022-12-18 00:22:08	Malicious Internet Name	Yes	Cleanbrowsing.org	0	1	2	0	None	Blocked by Cleanbrowsing.org [smtp.zerotwo-best-waifu.online]
2022-12-18 00:21:34	Netblock Membership	No	Censys	0	0	2	0	None	104.21.16.0/20
2022-12-18 00:07:21	Linked URL - Internal	No	Google	0	0	1	0	None	http://misogyny.wtf/
2022-12-18 00:04:12	Linked URL - Internal	No	Hybrid Analysis	1	0	1	0	None	http://misogyny.wtf:8080/
2022-12-18 00:06:31	Company Name	No	Company Name Extractor	1	0	2	0	None	(c) CentralNic Ltd
2022-12-18 00:18:03	Web Technology	No	Tool - WhatWeb	0	0	2	0	None	JQuery
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:2082
2022-12-18 00:12:42	Physical Location	No	ipapi.co	0	0	2	0	None	Toronto, Ontario, ON, Canada, CA
2022-12-18 00:06:06	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	raspu.tain.fr
2022-12-18 00:09:32	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	cogigang.com
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	turbofeistyintelligence.provhvfvqqho.repl.co

2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:23:32	Affiliate - Internet Name	No	DNS Raw Records	1	0	2	0	None	smtp-fr.securemail.pro
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:32:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namecheap.com
2022-12-18 00:20:42	Physical Location	No	Censys	0	0	1	0	None	Campinas, Sao Paulo, Brazil, South America
2022-12-18 00:18:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.10:80
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:8443
2022-12-18 00:24:58	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.188
2022-12-18 00:02:45	SSL Certificate Expiring	Yes	CertSpotter	0	0	1	0	None	2022-12-19 21:18:05
2022-12-18 00:08:52	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.28.240:443
2022-12-18 00:06:40	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.1:8443
2022-12-18 00:06:19	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.cx
2022-12-18 00:09:53	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	brasfaberk.ga
2022-12-18 00:22:04	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Te": "DISPLAY_UTF8", "Content_Type": "DISPLAY_UTF8"}, "Te": ["chunked"], "Content_Type": ["text/html"]}
2022-12-18 00:06:06	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	amenworld.com
2022-12-18 00:09:46	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	assets.auroramediagroup.xyz
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	grasshopper2 (Net ID: 00:01:38:5A:88:28)
2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:09:48	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 5.0 Description: The DES and Triple DES ciphers, as used in the T
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	onlinenewbankbcp.viiabcp.repl.co
2022-12-18 00:21:37	Software Used	Yes	Censys	0	0	2	0	None	PalletsProjects Werkzeug 2.2.2
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:44	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3031::6815:7b3:80
2022-12-18 00:03:03	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:5f:2b:c4:e2:52:ac:ba:5b:55:25:2b:3c:57:78:0c:6b:4f Signature Algorithm: sha256W Identifier: keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6 Authority Information Access: OCSP - URI:http://r3.o.le
2022-12-18 00:27:03	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [104.21.27.242]
2022-12-18 00:21:20	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-O

2022-12-18 00:21:47	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:4700:3032::/48
2022-12-18 00:08:30	Open TCP Port	No	LeakIX	0	0	1	0	None	plague.fun:80
2022-12-18 00:37:11	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.241] https://www.virustotal.com/en/ip-address/81.88.52.241/information/
2022-12-18 00:02:58	Raw Data from RIRs	No	Tool - WAFW00F	0	0	1	0	None	[{"url": "https://zerotwo-best-waifu.online", "firewall": "Generic", "detected": true, "manufacturer": "Unknown"}]
2022-12-18 00:03:02	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.99
2022-12-18 00:09:36	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	stadverket.ru.com
2022-12-18 00:08:40	BGP AS Membership	No	RIPE	0	0	3	0	None	39729
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2053
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:2053
2022-12-18 00:21:02	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-(
2022-12-18 00:03:15	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-100.w90-116.abo.wanadoo.fr
2022-12-18 00:23:31	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	smtp.zerotwo-best-waifu.online. 900 IN CNAME smtp-fr.securemail.pro.
2022-12-18 00:10:20	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 5.0 Description: The DES and Triple DES ciphers, as used in the T
2022-12-18 00:21:06	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetFBC6 (Net ID: 00:01:36:5A:FB:C4)
2022-12-18 00:03:05	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	api.plague.fun
2022-12-18 00:22:28	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.128:8080
2022-12-18 00:03:07	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.191
2022-12-18 00:10:05	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	https://zerotwo-best-waifu.online/778112985743251/wap/shatlegay/stealer123365
2022-12-18 00:20:54	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [34.149.204.188] https://www.virustotal.com/en/ip-address/34.149.204.188/information/
2022-12-18 00:08:45	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	api.plague.fun
2022-12-18 00:31:50	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.133:21
2022-12-18 00:20:59	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:2087
2022-12-18 00:11:11	Similar Domain - Whois	No	Whois	0	0	2	0	None	Domain Name: plague.in Registry Domain ID: D1204034-IN Registrar WHOIS Server: Registrar URL: https://www.namesilo.com Updated Date: FOR PRIVACY Admin Email: Please contact the Registrar listed above Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRI solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic pr

2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://wasp.plague.fun/inject/Fu643XzaSbmCcnGN/
2022-12-18 00:16:27	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
2022-12-18 00:21:54	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-O
2022-12-18 00:20:46	Raw Data from RIRs	No	Censys	0	0	1	0	None	{"last_updated_at": "2022-11-23T01:34:36.916Z", "ip": "40.113.112.131", "location_updated_at": "2022-12-18T00:20:43.061599Z", "autono
2022-12-18 00:23:07	Raw Data from RIRs	No	CRXcavator	0	0	1	0	None	[{"platform": "Chrome", "extension_id": "bifklmkjcgfnoholohpcenkjpdmkjmgj", "name": "Plague Inc Virus Wallpaper New Tab Theme", "icor
2022-12-18 00:03:17	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-105.w90-116.abo.wanadoo.fr
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:8880
2022-12-18 00:16:37	Raw Data from RIRs	No	numverify	0	0	3	0	None	{u'international_format': u'+33892556677', u'local_format': u'0892556677', u'number': u'33892556677', u'valid': True, u'line_type': u
2022-12-18 00:27:44	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	domini@dominiando.it
2022-12-18 00:12:11	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'188.114.97.0', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2022-12-18 00:18:46	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.20:8080
2022-12-18 00:03:09	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.230
2022-12-18 00:02:50	IP Address	No	Mnemonic PassiveDNS	38	0	1	0	None	20.226.83.185
2022-12-18 00:18:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.1:443
2022-12-18 00:06:00	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\ZonesCacheCounterMutex"\ u'Antivirus vendors marked dropped file "urlblockindex_1_.bin" as clean (type is "data")'}, {u'category': u'Unusual Characteristics', Location: [%TEMP%\\~DFAA44616120A668AB.TMP]- [targetUID: 00000000-00003176]\n "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has text"- [targetUID: N/A]'}, {u'category': u'Network Related', u'origin': u'String', u'identifier': u'string-3', u'name': u'Found poter u'certificates': [], u'hosts': [u'34.149.204.188', u'23.56.194.53'], u'sha256': u'1a8504381e6e071e92540e8d7b63b9f627b793b3ae398a9f28e
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet4862 (Net ID: 00:01:36:5B:48:60)
2022-12-18 00:04:28	Email Gateway (DNS MX Records)	No	DNS Raw Records	0	0	1	0	None	eforward1.registrar-servers.com
2022-12-18 00:18:08	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.2:8080
2022-12-18 00:09:00	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.1:80
2022-12-18 00:09:16	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.3:8080
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	43215.345121.repl.co
2022-12-18 00:19:06	Physical Location	No	ipapi.co	0	0	3	0	None	Bergamo, Lombardy, 25, Italy, IT
2022-12-18 00:03:26	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	189.204.149.34.bc.googleusercontent.com
2022-12-18 00:16:53	Affiliate - Company Name	No	Company Name Extractor	0	0	4	0	None	Cloudflare, Inc.

2022-12-18 00:07:37	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:2c:cd:9b:50:65:02:e8:a9:66:93:11:97:33:8f:e3:ed:9b Signature Algorithm: sha256W 83:94:56:ac:25:05:62:89:5c:35:fc:32:04:91:ab:d9:a9:3e: 3e:82:d9:03:2a:25:e9:e1:c0:6e:9f:c2:5f:2b:eb:15:61:ed: ff:a3:97:ef:78:fb:69:ef
2022-12-18 00:09:39	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'https', u'event_type': u'service', u'ip': u'188.114.97.9', u'vendor': u'', u'port': u'8443', u'transpo u'detected': False, u'version': u'TLSv1.3'}, u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'banner': u'', u'fingerprint': u''}, u'', u'name': u'cloudflare', u'fingerprint': u''}}, u'event_fingerprint': u'6d1f2e7c9ee98731fedbc44a39cb147fd61faf13c54319aa7eb0c7d81 2022 13:55:48 GMT\r\nContent-Type: text/html; charset=UTF-8\r\nTransfer-Encoding: chunked\r\nConnection: close\r\nCache-Control: no-c 0}, u'type': u'', u'severity': u'', u'stage': u''}, u'event_pipeline': [u'CertStream', u'l9scan', u'tcpid', u'HttpPlugin'], u'http': [{"url":"https:\\/\\\/a.nel.cloudflare.com\\/report\\\/v3?s=gacXtCN5nhXvtXx%2BZaMTvJgSyJKyhNbIOzsB2qIa2uXIoWfXDgJuv%2Bq3T5xD2Mdk96ScN0C u'event_pipeline': [u'CertStream', u'l9scan', u'tcpid', u'HttpPlugin'], u'http': {u'status': 0, u'title': u'301 Moved Permanently', u
2022-12-18 00:21:02	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-C
2022-12-18 00:10:04	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	https://misogyny.wtf/api/v2/sendtk
2022-12-18 00:03:06	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.182
2022-12-18 00:21:34	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:31:01	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.chat Registry Domain ID: 7664ba56bd064bbf82bc4fb158862a02-DONUTS Registrar WHOIS Server: whois.dynadot.com Regist REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identi may this data be used to: a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolici can be reasonably confirmed that the requester holds a specific legitimate interest and a proper legal basis for accessing the withhe REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Phone: REDACTED FOR PRIVACY Admin Em
2022-12-18 00:09:47	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	attikosilios.gr
2022-12-18 00:11:53	Physical Location	No	ipapi.co	1	0	1	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2022-12-18 00:31:48	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.place
2022-12-18 00:19:33	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [20.226.83.185] https://www.virustotal.com/en/ip-address/20.226.83.185/information/
2022-12-18 00:22:07	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Connection": "DISPLAY_UTF8"}, "Connection": ["close"]}
2022-12-18 00:05:58	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:20:17	Netblock Membership	No	RIPE	16	0	3	0	None	195.110.124.0/24
2022-12-18 00:07:03	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u' u'identifier': u'network-1', u'name': u'Contacts server', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': [%APPDATA%\\Microsoft\\Windows\\Cookies\\W05YX9G3.txt]- [targetUID: 00000000-00003028]\n Dropped file: "H4T1U159.txt" - Location: [%A "L2LWFGYF.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\L2LWFGYF.txt]- [targetUID: 00000000-00003028]'}, {u'category': u' "large.lc-20220223-181547-lc.min.ACSHASH8f81358eebb18a1778ddd3319a401956_1_.css" has type "ASCII text with very long lines with no li woff_1_.woff" has type "Web Open Font Format TrueType length 68827 version 1.0"- [targetUID: N/A]\n "F4RUS99S.htm" has type "HTML doc blueCore.svg"\n Pattern match: "https://www.bbva.com.ar/fnetcore/assets/img/left-arrow.png"\n Pattern match: "https://www.bbva.com.ar
2022-12-18 00:04:00	Physical Location	No	ipstack	0	0	1	0	None	Netherlands
2022-12-18 00:10:20	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 4.3 Description: OpenVPN, when using a 64-bit block cipher, makes
2022-12-18 00:07:18	Web Content Type	No	Web Spider	0	0	3	0	None	text/html; charset=utf-8
2022-12-18 00:13:26	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	abuse@enom.com
2022-12-18 00:24:06	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	private@register.it
2022-12-18 00:04:35	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 2, u'search_terms': [{u'id': u'host', u'value': u'172.67.147.230'}], u'result': [{u'environment_id': 160, u'job_id': u'638

2022-12-18 00:16:27	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
2022-12-18 00:18:03	Web Technology	No	Tool - WhatWeb	0	0	2	0	None	HTML5
2022-12-18 00:19:03	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'52', u'country_tld': u'.it', u'ip': u'195.110.124.246', u'currency_name': u'Euro', u'currency': u'EUR', u'country_
2022-12-18 00:06:35	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.0:80
2022-12-18 00:12:58	Malicious IP on Same Subnet	Yes	blocklist.de	0	0	2	0	None	blocklist.de List [40.112.0.0/13] http://lists.blocklist.de/lists/all.txt
2022-12-18 00:28:20	Web Framework	No	Web Framework Identifier	0	0	5	0	None	jQuery
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetA41A (Net ID: 00:01:36:57:A4:18)
2022-12-18 00:08:38	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2022-12-18 00:37:20	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@joker.com
2022-12-18 00:20:56	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:03:11	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:08:aa:47:53:40:59:b8:a3:96:dc:96:87:a9:7a:35:d6:08 Signature Algorithm: ecdsa-w with-SHA256 30:46:02:21:00:EC:B7:61:12:A5:3D:86:54:42:E0:1C: 85:40:38:6B:1D:DC:BA:74:3E:FB:D2:C9:05:2E:1B:34: 1F:4B:CF:C0:3C:02:21:00
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	logitec-a53131 (Net ID: 00:01:8E:A5:31:30)
2022-12-18 00:04:38	Raw Data from RIRs	No	Maltiverse	0	0	2	0	None	{u'asn_registry': u'ripencc', u'country_code': u'US', u'classification': u'whitelist', u'asn_country_code': u'US', u'address': u'Vikt
2022-12-18 00:02:43	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Google Trust Services LLC,CN=GTS CA 1P5
2022-12-18 00:18:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.9:80
2022-12-18 00:21:51	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-O
2022-12-18 00:09:46	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.17:443
2022-12-18 00:02:50	Domain Whois	No	Whois	8	0	1	0	None	Domain Name: PLAGUE.FUN Registry Domain ID: D268611982-CNIC Registrar WHOIS Server: whois.enom.com Registrar URL: https://www.enom.co WHOIS database: 2022-12-18T00:02:49.0Z <<< For more information on Whois status codes, please visit https://icann.org/epp >>> IMPORTA Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Alpes-Maritimes Registrant Postal Code: REDACTED FOR PRIVACY Registr database is provided to you for information purposes only, that is, to assist you in obtaining information about or related to a doma
2022-12-18 00:12:21	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'104.21.19.243', u'currency_name': u'Dollar', u'currency': u'CAD', u'country_
2022-12-18 00:07:18	Web Content Type	No	Web Spider	0	0	3	0	None	text/css; charset=UTF-8
2022-12-18 00:03:06	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.180
2022-12-18 00:16:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:33:43	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.188:80
2022-12-	Open TCP	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-O

18 00:21:13	Port Banner								
2022-12-18 00:17:08	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	amen.fr
2022-12-18 00:20:56	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T20:29:44.251Z", "ip": "2606:4700:3031::ac43:93e6", "location_updated_at": "2022-12-15T11:12:39.98736 "2022-11-23T13:31:05.516293256Z"}, "www.innerreachescounselling.com.au.cdn.cloudflare.net": {"record_type": "AAAA", "resolved_at": "2 "makecoloradohome.com": {"record_type": "AAAA", "resolved_at": "2022-12-05T13:38:59.828798047Z"}, "wailacamatcoman.gq": {"record_type "garageshedcarportbuilder.com": {"record_type": "AAAA", "resolved_at": "2022-12-13T13:26:04.059048706Z"}, "cpanel.sectraexpress.com": 15T13:57:52.400597943Z"}, "greneflahiggewhi.gq": {"record_type": "AAAA", "resolved_at": "2022-12-01T14:51:12.241455327Z"}, "tticarot "warmodeon.com": {"record_type": "AAAA", "resolved_at": "2022-12-10T14:04:27.488932415Z"}, "gamewinwin.net": {"record_type": "AAAA", 09T16:41:18.225114327Z"}, "www.thedollhousemuseum.com.cdn.cloudflare.net": {"record_type": "AAAA", "resolved_at": "2022-10-31T16:19:
2022-12-18 00:21:09	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-
2022-12-18 00:21:17	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-
2022-12-18 00:03:08	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	api.plague.fun
2022-12-18 00:06:57	Open TCP Port	No	Pulsedive	0	0	2	0	None	34.149.204.188:80
2022-12-18 00:03:12	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.242
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	2WIRE623 (Net ID: 00:00:85:F5:03:9F)
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:03:02	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.101
2022-12-18 00:17:08	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	2	0	None	amen.fr
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	clumsydarkchords.88838.repl.co
2022-12-18 00:25:42	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-190.w90-116.abo.wanadoo.fr
2022-12-18 00:11:11	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.info Registry Domain ID: c6b55818519e49ffbd1c2a329f4bac56-DONUTS Registrar WHOIS Server: whois.godaddy.com/ Regis Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED Whois service for information purposes, and to assist persons in obtaining information about or related to a domain name registratior Public Data] tag indicates that such data is not made publicly available due to applicable data privacy laws or requirements. Should
2022-12-18 00:04:04	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://misogyny.wtf', u'http_status': 200, u'plugins
2022-12-18 00:09:02	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.1:8443
2022-12-18 00:12:35	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'compromised_ deflate\nHost: performance.radar.cloudflare.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "user-agent: ")'}, {u'category': u'Gener 0, u'type': 7, u'description': u'"188.114.97.3:80"\n "104.18.31.78:443"'}, {u'category': u'Unusual Characteristics', u'origin': u'Bir [%APPDATA%\\Microsoft\\Windows\\Cookies\\63CJVUP7.txt]- [targetUID: 00000000-00002832]\n "LM0USI2F.txt" has type "ASCII text"- Locati 32x32 32 bits/pixel"- [targetUID: N/A]\n "~DF6F835D267B734551.TMP" has type "data"- Location: [%TEMP%\\~DF6F835D267B734551.TMP]- [tar application/javascript, */*;q=0.8\nReferer: http://188.114.97.3/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Tr None, u'interesting': False, u'error_type': None, u'state': u'SUCCESS', u'entrypoint': None, u'mitre_attcks': [{u'parent': None, u'at
2022-12-18 00:27:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.48.101:80
2022-12-18 00:07:05	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:14:31	Physical Location	No	ipstack	0	0	2	0	None	Colombia

2022-12-18 00:14:32	Country	No	Country Name Extractor	0	0	3	0	None	United States
2022-12-18 00:13:27	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	abuse@namecheap.com
2022-12-18 00:22:37	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.nl
2022-12-18 00:03:05	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:12:16	Physical Location	No	ipapi.co	0	0	2	0	None	Newark, New Jersey, NJ, United States, US
2022-12-18 00:22:07	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.0 400 Bad Request
2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	https://obf.plague.fun/obf/
2022-12-18 00:04:41	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObjects\\IsoScope_eec_IESQMMUTEX_0_519"\n "Local\\Internet u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 8, u'descr [targetUID: 00000000-00003756]\n "0GRXRUKJ.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\0GRXRUKJ.tx u'Found potential URL in binary/memory', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id 5/88 scanned on 08/29/2022 07:42:04)\n URL: https://188.114.96.0/alternatiff/version-ax-w32.txt (AV positives: 5/88 scanned on 08/26/ Trident/7.0; rv:11.0) like Gecko'}, {u'category': u'Network Related', u'origin': u'String', u'identifier': u'string-14', u'name': u'F
2022-12-18 00:02:39	Domain Name	No	SpiderFoot UI	24	0	0	0	None	misogyny.wtf
2022-12-18 00:04:28	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	journey.ns.cloudflare.com
2022-12-18 00:09:24	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.7:80
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:8443
2022-12-18 00:12:46	Physical Location	No	ipapi.co	0	0	2	0	None	Newark, New Jersey, NJ, United States, US
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	Pornhub Users (Category: XXXPORNXXX) https://www.pornhub.com/users/rasputain
2022-12-18 00:02:47	Raw Data from RIRs	No	grep.app	0	0	1	0	None	{u'repo': {u'raw': u'aceeontop/wasp-stealer'}, u'total_matches': {u'raw': u'1'}, u'content': {u'snippet': u'<table class="highlight-t </td></tr></table>'}, u'branch': {u'raw': u'main'}, u'path': {u'raw': u'OldWaspsVersions/wasp-1.1.2.py'}, u'id': {u'raw': u'g/aceeont
2022-12-18 00:18:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.12:443
2022-12-18 00:02:43	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=E1
2022-12-18 00:09:19	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.137.37:80
2022-12-18 00:26:49	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: plague.org Registry Domain ID: 8bd26273e60b490495d081f7f0b8a64c-LROR Registrar WHOIS Server: whois.tucows.com Registrar REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identi guarantee its accuracy. This service is intended only for query-based access. You agree that you will use this data only for lawful p Registrant Street: 96 Mowat Ave Registrant City: Toronto Registrant State/Province: ON Registrant Postal Code: M6K 3M1 Registrant Cou obtaining information about or related to a domain name's registration record. Tucows makes this information available "as is," and c
2022-12-18 00:20:59	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3033::6815:1cf0:80

2022-12-18 00:12:47	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'188.114.96.3', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F2:6F:6D)
2022-12-18 00:04:11	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3
2022-12-18 00:18:35	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.15:8080
2022-12-18 00:02:43	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:43:a4:7d:29:1f:15:0e:6b:ac:86:e4:4b:c0:be:69:71:a9 Signature Algorithm: sha256W SHA256 30:46:02:21:00:B6:95:B7:C7:1C:80:2B:FD:7A:41:2D: D1:EE:2B:F0:0C:C7:D5:AD:4A:C9:E0:25:F1:61:3A:42: F4:C7:98:23:BC:02:21:00:B0:8
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:2096
2022-12-18 00:21:20	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:16:56	Malicious Internet Name	Yes	CloudFlare Malware DNS	0	1	2	0	None	Blocked by CloudFlare DNS [webmail.zerotwo-best-waifu.online]
2022-12-18 00:17:00	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2022-12-18 00:12:06	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'104.21.28.240', u'currency_name': u'Dollar', u'currency': u'CAD', u'country_
2022-12-18 00:05:49	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 16, u'threat_score': None, u'compromis u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:2268:120:WilError_01' type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%TEMP%\\2268_478418729_platform_specific\\win_x64\\widevi "77EC63BDA74BD0D0E0426DC8F8008506" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\77EC63BDA74 with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\e93703ec-1b1f-4cd8-ac7e-72ecaace237e.tmp]- [targetU u'suspicious', u'capec_id': None, u'attck_id': None, u'relevance': 5, u'threat_level': 1, u'type': 8, u'description': u'Dropped file: u'identifier': u'binary-1', u'name': u'Drops executable files', u'attck_id_wiki': None, u'threat_level_human': u'suspicious', u'capec
2022-12-18 00:31:52	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	westabuse@gmail.com
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpaceStation (Net ID: 00:02:2D:01:CF:F8)
2022-12-18 00:09:14	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.2:443
2022-12-18 00:09:45	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.9:443
2022-12-18 00:37:18	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: PRGMR.COM Registry Domain ID: 70002607_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.joker.com Registrar URL: http://www Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in whois.joker.com Registrar URL: https://joker.com Updated Date: 2022-05-22T20:37:35Z Creation Date: 2001-04-27T00:09:53Z Registrar Reg (or its computer systems). NOTE: The compilation, repackaging, dissemination or other use of this data NOTE: is expressly prohibited
2022-12-18 00:10:04	Web Server	No	URLScan.io	0	0	1	0	None	Werkzeug/2.2.2 Python/3.9.11
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:2052
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:20:59	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:09:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.0:8443
2022-12-18 00:27:16	Physical Location	No	MetaDefender	0	0	2	0	None	Medellin, Colombia
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	2cdc0387-f453-4585-abc6-b131de9f7b91.id.repl.co
2022-12-18	WiFi Access	No	Wigle.net	0	0	5	0	None	dvdbeyond (Net ID: 00:01:24:F2:B3:12)

00:21:11	Point Nearby								
2022-12-18 00:19:06	Physical Location	No	ipstack	0	0	3	0	None	Italy
2022-12-18 00:11:48	Malicious IP on Same Subnet	Yes	Greensnow	0	0	2	0	None	greensnow.co [20.192.0.0/10] https://blocklist.greensnow.co/greensnow.txt
2022-12-18 00:08:11	Netblock Membership	No	RIPE	6	0	1	0	None	20.192.0.0/10
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	ecuadopichi--ecuado30499f.repl.co
2022-12-18 00:03:16	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	stream.plague.fun
2022-12-18 00:20:56	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	infoworld (Net ID: 00:02:2D:04:D1:DB)
2022-12-18 00:22:01	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:21:41	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-11-20T15:07:59.768Z", "ip": "20.226.56.97", "location_updated_at": "2022-12-18T00:21:37.986540Z", "autonomo
2022-12-18 00:07:17	Linked URL - External	No	Web Spider	0	0	2	0	None	https://i.imgur.com/W2gQQnU.png
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:04:38	Malicious IP Address	Yes	Maltiverse	0	1	2	0	None	Maltiverse [188.114.97.0]
2022-12-18 00:12:24	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'SP', u'country_tld': u'.br', u'ip': u'20.226.56.97', u'currency_name': u'Real', u'currency': u'BRL', u'country_pop
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom (Net ID: 00:01:38:A4:44:3A)
2022-12-18 00:04:28	Name Server (DNS NS Records)	No	DNS Raw Records	0	0	1	0	None	journey.ns.cloudflare.com
2022-12-18 00:12:26	Physical Location	No	ipapi.co	0	0	2	0	None	Newark, New Jersey, NJ, United States, US
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet24CE (Net ID: 00:01:36:59:24:CC)
2022-12-18 00:22:14	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:21:34	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-(
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:16:54	Malicious Internet Name	Yes	CloudFlare Malware DNS	0	1	2	0	None	Blocked by CloudFlare DNS [ftp.zerotwo-best-waifu.online]
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	yahvehseencargaradebendecirmehoymismo.dios12xx.repl.co
2022-12-18 00:20:47	Web Content Language	No	Language Detector	0	0	3	0	None	English
2022-12-18 00:18:03	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://webmail.zerotwo-best-waifu.online', u'http_st
2022-12-18	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	baysicqua.ga

00:09:50									
2022-12-18 00:24:03	Similar Domain - Whois	No	Whois	0	0	2	0	None	Domain name: plague.nl Status: active Registrar: Sonexo B.V. Edeseweg 52 6721JX BENNEKOM Netherlands Abuse Contact: Creation Date: 20
2022-12-18 00:04:28	Raw DNS Records	No	DNS Raw Records	0	0	1	0	None	misogyny.wtf. 1800 IN TXT "v=spf1 include:spf.efwd.registrar-servers.com ~all"
2022-12-18 00:07:17	Linked URL - Internal	No	Web Spider	4	0	2	0	None	http://misogyny.wtf/parser
2022-12-18 00:26:31	Physical Location	No	MetaDefender	0	0	2	0	None	San Jose, United States
2022-12-18 00:10:04	Web Server	No	URLScan.io	0	1	1	0	None	Werkzeug/2.0.3 Python/3.9.0
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	hj92.gh67.repl.co
2022-12-18 00:11:07	Similar Domain - Whois	No	Whois	2	0	2	0	None	%% %% This is the AFNIC Whois server. %% %% complete date format: YYYY-MM-DDThh:mm:ssZ %% %% Rights restricted by copyright. %% See h contact@kifcorp.fr registrar: KIFCORP changed: 2022-12-16T10:49:00.573083Z anonymous: NO obsoleted: NO eppstatus: associated eppstatu
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:8080
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:09:31	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'172.67.169.215', u'vendor': u'', u'port': u'80', u'transpor u'country_iso_code': u'US', u'city_name': u'', u'location': {u'lat': 37.751, u'lon': -97.822}, u'country_name': u'United States', u'c u'6d1f2e7c9ee987319317d86e2d588a2b7f31fc7718ad4491369cb730d3a794a6', u'leak': {u'dataset': {u'files': 0, u'rows': 0, u'ransom_notes': modified: Sun, 19 Jun 2022 19:35:41 GMT\r\nvary: Accept-Encoding\r\nCF-Cache-Status: DYNAMIC\r\nReport-To: {"endpoints":[{"url":"http u'172.67.169.215', u'vendor': u'', u'port': u'443', u'transport': [u'tcp', u'tls', u'http'], u'event_source': u'HttpPlugin', u'networ True, u'detected': False, u'version': u'TLSv1.3'}, u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'banner': u'', u'fingerprint': u'CLOUDFLARENET', u'asn': 13335, u'network': u'172.67.0.0/16'}, u'service': {u'credentials': {u'username': u'', u'raw': None, u'passw
2022-12-18 00:32:16	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: PLAGUE.TECH Registry Domain ID: D183124424-CNIC Registrar WHOIS Server: whois.west.cn Registrar URL: http://www.west.cn WHOIS database: 2022-12-18T00:32:15.0Z <<< For more information on Whois status codes, please visit https://icann.org/epp >>> IMPORTA REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Jiang S of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2022-12-18T00:32:15.0
2022-12-18 00:21:13	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:
2022-12-18 00:09:35	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	onlimapotexttac.tk
2022-12-18 00:08:38	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:54	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: -
2022-12-18 00:21:58	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	s4bskcnr4ocn.m7yke.repl.co
2022-12-18 00:25:39	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-184.w90-116.abo.wanadoo.fr
2022-12-18 00:04:11	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-SH X509v3 Basic Constraints: critical CA:FALSE CT Precertificate SCTs: Signed Certificate Timestamp: Version : v1 (0x0) Log ID : E8:3E:D 30:45:02:21:00:d8:35:e0:5c:fe:c9:39:b4:06:5a:95:36:1c: 73:f4:85:1c:c5:6e:6b:ef:48:76:d6:7f:a3:fe:55:ed:82:7f: c5:02:20:7f:8c:86:3a:6f
2022-12-18 00:05:57	Account on External Site	No	Account Finder	0	0	2	0	None	Reddit (Category: social) https://www.reddit.com/user/zerotwo-best-waifu
2022-12-18 00:02:48	IP Address	No	Mnemonic PassiveDNS	75	0	1	0	None	188.114.97.1
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:13:38	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	familiar@familiar.com.py

2022-12-18 00:08:38	BGP AS Membership	No	RIPE	0	0	2	0	None	8075
2022-12-18 00:04:02	Physical Location	No	ipstack	0	0	2	0	None	United States
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2053
2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:13:48	Web Content Language	No	Language Detector	0	0	3	0	None	English
2022-12-18 00:19:05	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'52', u'country_tld': u'.it', u'ip': u'81.88.48.101', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2022-12-18 00:21:44	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-(
2022-12-18 00:56:42	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@godaddy.com
2022-12-18 00:09:36	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.12:80
2022-12-18 00:03:09	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.229
2022-12-18 00:27:14	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.48.102:80
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	kingj73664liv.hbinging.repl.co
2022-12-18 00:04:00	Physical Location	No	ipstack	0	0	1	0	None	Netherlands
2022-12-18 00:09:54	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:12:28	Physical Location	No	ipapi.co	0	0	2	0	None	Newark, New Jersey, NJ, United States, US
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	infoworld (Net ID: 00:02:2D:01:DD:9B)
2022-12-18 00:14:14	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.144:8443
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WestEd (Net ID: 00:02:2D:05:7E:85)
2022-12-18 00:27:44	Similar Domain - Whois	No	Whois	0	0	2	0	None	% TCI Whois Service. Terms of use: % https://tcinet.ru/documents/whois_ru_rf.pdf (in Russian) % https://tcinet.ru/documents/whois_su.
2022-12-18 00:13:48	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	registryinfo@eurodns.com
2022-12-18 00:14:47	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.160:8443
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18	Physical Location	No	MetaDefender	0	0	1	0	None	Campinas, Brazil

00:24:54									
2022-12-18 00:04:10	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	sni.cloudflaressl.com
2022-12-18 00:04:54	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 6, u'search_terms': [{u'id': u'host', u'value': u'172.67.190.129'}], u'result': [{u'environment_id': 100, u'job_id': u'623 7 32 bit', u'threat_score': 69, u'verdict': u'malicious', u'submit_name': u'sample.url', u'sha256': u'8720302e50a9a4ae897b8f151d004c7
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	galiciaenlinea-1.larescomco.repl.co
2022-12-18 00:21:27	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:08:42	Internet Name	No	DNS Resolver	0	0	2	0	None	rasputain.fr
2022-12-18 00:16:33	Physical Location	No	numverify	0	0	3	0	None	Bellevue, US
2022-12-18 00:11:58	Raw Data from RIRs	No	ipapi.co	0	0	1	0	None	{u'region_code': u'NH', u'country_tld': u'.nl', u'ip': u'40.113.112.131', u'currency_name': u'Euro', u'currency': u'EUR', u'country_p
2022-12-18 00:10:04	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	https://misogyny.wtf/
2022-12-18 00:31:32	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.link Registry Domain ID: DO_00981b8bafad29479f36ae1c8b278bf9-UR Registrar WHOIS Server: whois.tucows.com Registra REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information of WHOIS database: 2022-12-18T00:31:32.521Z <<< For more information on domain status codes, please visit https://icann.org/epp The W PLAGUE.LINK Registry Domain ID: DO_00981b8bafad29479f36ae1c8b278bf9-UR Registrar WHOIS Server: whois.tucows.com Registrar URL: http:/ City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FO necessary to register domain names or modify existing registrations. The compilation, repackaging, dissemination or other use of this
2022-12-18 00:21:54	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-O
2022-12-18 00:12:37	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'MO', u'country_tld': u'.us', u'ip': u'34.149.204.188', u'currency_name': u'Dollar', u'currency': u'USD', u'country
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	seguridadprovincia.postquestions1.repl.co
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:04:09:0C)
2022-12-18 00:16:59	Web Content Type	No	Web Spider	0	0	4	0	None	text/css
2022-12-18 00:12:06	Country	No	Country Name Extractor	0	1	2	0	None	Switzerland
2022-12-18 00:19:10	Hosting Provider	No	Hosting Provider Identifier	0	0	3	0	None	register.it: http://we.register.it/
2022-12-18 00:16:58	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:2087
2022-12-18 00:08:52	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'https', u'event_type': u'service', u'ip': u'104.21.28.240', u'vendor': u'', u'port': u'8443', u'transp 03T00:00:00Z'}, u'enabled': True, u'detected': False, u'version': u'TLSv1.3'}, u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'b u'event_fingerprint': u'6d1f2e7c9ee98731735c0f301524bacadf25fc68ad8b5387015c19edd90630eb', u'leak': {u'dataset': {u'files': 0, u'rows s=HZob%2FMOv0l92axuHjMOTiamywxyCjEwA4oSGAVJo%2B6hv7ivKt5PmSbX0XN1vUaI3%2BkLehNnAPyeVX1Tgunl8HGgGL4NlOE5uNXzwt%2FDpC5aAEEoww5fw8gY7qGo u'0000000000000000000000000000000000000000000000000000000000000000', u'certificate': {u'domain': [u'*.sharepointvn.net', u'sharepointvn 03T01:24:37.698461268Z'}, {u'protocol': u'https', u'event_type': u'service', u'ip': u'104.21.28.240', u'vendor': u'', u'port': u'8443 False, u'version': u'TLSv1.3'}, u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'banner': u'', u'fingerprint': u''}, u'reverse':
2022-12-18 00:21:51	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-O
2022-12-18 00:06:42	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.190.129:80
2022-12-18 00:02:43	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=atlas.plague.fun
2022-12-18 00:18:08	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.2:80
2022-12-	WiFi	No	Wigle.net	0	0	5	0	None	

18 00:21:11	Access Point Nearby								CATYLN (Net ID: 00:01:38:86:06:1F)
2022-12-18 00:29:08	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.uk
2022-12-18 00:23:31	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	mail.zerotwo-best-waifu.online. 900 IN CNAME mail-fr.securemail.pro.
2022-12-18 00:06:58	Malicious IP Address	Yes	Internet Storm Center	0	1	2	0	None	Internet Storm Center [188.114.96.1] https://isc.sans.edu/api/ip/188.114.96.1
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	vc657hg.qw653bv.repl.co
2022-12-18 00:30:51	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@godaddy.com
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:03:01	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.95
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	GitHub (Category: coding) https://github.com/rasputain
2022-12-18 00:17:08	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	amen.fr
2022-12-18 00:14:47	Internet Name - Unresolved	No	VirusTotal	0	0	1	0	None	69-sparte.plague.fun
2022-12-18 00:25:44	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	dominiando.uk
2022-12-18 00:21:51	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-(
2022-12-18 00:05:06	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 5, u'search_terms': [{u'id': u'host', u'value': u'20.226.83.185'}], u'result': [{u'environment_id': 110, u'job_id': u'638f u'Malicious site', u'av_detect': u'8', u'environment_description': u'Windows 7 32 bit (HWP Support)', u'threat_score': 63, u'verdict'
2022-12-18 00:06:00	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	registrar-servers.com
2022-12-18 00:04:50	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'631a6
2022-12-18 00:37:36	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.synology.me
2022-12-18 00:32:27	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.tools Registry Domain ID: ecc23f6039fd437480662da9344894d6-DONUTS Registrar WHOIS Server: whois.namecheap.com Reg Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Digital Whois service agree to use the data only for lawful purposes, and under no circumstances may this data be used to: a) allow, the registrar URL listed above. Access to non-public data may be provided, upon request, where it can be reasonably confirmed that th
2022-12-18 00:13:45	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namecheap.com
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:20	Netblock Membership	No	Censys	0	0	2	0	None	188.114.97.0/24
2022-12-18 00:18:04	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.0:443
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:2083
2022-12-18 00:41:01	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	misogyny.com

2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	attentivewellmadeaudit.replealtan.repl.co
2022-12-18 00:21:30	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-(
2022-12-18 00:21:20	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:
2022-12-18 00:04:01	Country	No	Country Name Extractor	0	0	4	0	None	United States
2022-12-18 00:08:41	Internet Name	No	DNS Resolver	0	0	2	0	None	misogyny.wtf
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	vapor (Net ID: 00:02:2D:09:FB:FD)
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	fala00001.falab000bella.repl.co
2022-12-18 00:06:31	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.147.230:8443
2022-12-18 00:18:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.13:80
2022-12-18 00:03:27	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:20:59	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: -
2022-12-18 00:21:02	Netblock Membership	No	Censys	0	0	2	0	None	104.21.16.0/20
2022-12-18 00:04:01	Physical Location	No	ipstack	0	0	2	0	None	United States
2022-12-18 00:25:40	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-186.w90-116.abo.wanadoo.fr
2022-12-18 00:31:11	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.faith Registry Domain ID: D40E9E8E1E2AB4C19B383C4976CE87C41-NSR Registrar WHOIS Server: https://porkbun.com/whois REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIV status codes, please visit https://icann.org/epp The Service is provided so that you may look up certain information in relation to c
2022-12-18 00:04:04	Raw Data from RIRs	No	Hybrid Analysis	0	0	1	0	None	{u'count': 5, u'search_terms': [{u'id': u'domain', u'value': u'misogyny.wtf'}], u'result': [{u'environment_id': 110, u'job_id': u'638 u'Malicious site', u'av_detect': u'8', u'environment_description': u'Windows 7 32 bit (HWP Support)', u'threat_score': 63, u'verdict'
2022-12-18 00:09:12	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.1:80
2022-12-18 00:22:08	Malicious Internet Name	Yes	Cleanbrowsing.org	0	1	2	0	None	Blocked by Cleanbrowsing.org [mail.zerotwo-best-waifu.online]
2022-12-18 00:11:11	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.io Registry Domain ID: ea274f7d6870401abc6e330d5b2844e1-DONUTS Registrar WHOIS Server: whois.ovh.com Registrar UR Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDD lawful purposes, and under no circumstances may this data be used to: a) allow, enable, or otherwise support the transmission by e-ma data may be provided, upon request, where it can be reasonably confirmed that the requester holds a specific legitimate interest and
2022-12-18 00:14:32	Country	No	Country Name Extractor	0	1	3	0	None	Canada
2022-12-18 00:25:52	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [188.114.97.1]
2022-12-18 00:04:34	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 97, u'compromised_ 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' "\\REGISTRY\\MACHINE\\SOFTWARE\\POLICIES\\MICROSOFT\\SYSTEMCERTIFICATES\\TRUSTEDPEOPLE"; Key: "")'}, {u'category': u'General', u'orig (UID: 00000000-00003864)\n Spawned process "IEXPLORE.EXE" with commandline "SCODEF:3864 CREDAT:275457 /prefetch:2" (UID: 00000000-000 (Path: "HKLM\\SOFTWARE\\MICROSOFT\\SYSTEMCERTIFICATES\\AUTHROOT\\CERTIFICATES\\F18B538D1BE903B6A6F056435B171589CAF36BF2"; Key: "BLOB" "UpdatingNewTabPageData"\n "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "Local\\VERMGMTBlockListFileMutex"'}, {u'category': u'General', "5069d1f3fe070000" to virtual address "0xF4E040E0" (part of module "IEFRAME.DLL")\n "iexplore.exe" wrote bytes "b062d1f3fe070000" to
2022-12-18 00:13:51	Internet Name	No	DNS Brute-forcer	0	0	1	0	None	www.zerotwo-best-waifu.online
2022-12-18 00:59:52	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: misogyny.org Registry Domain ID: 306b87640a9a4177b66ed5ee2d15d5eb-LROR Registrar WHOIS Server: whois.namecheap.com Regis REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin only, and Public Interest Registry does not guarantee its accuracy. This service is intended only for query-based access. You agree t

									Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: transfe Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2022-12-17T21:59:51.97Z <<< For more information on W
2022-12-18 00:18:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.5:8443
2022-12-18 00:06:15	Linked URL - Internal	No	Web Spider	0	0	1	0	None	http://misogyny.wtf/
2022-12-18 00:03:10	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.236
2022-12-18 00:21:30	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:24:56	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.179
2022-12-18 00:09:02	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.1:443
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	TEO Network Enterprise (Net ID: 00:01:24:F0:B7:E1)
2022-12-18 00:13:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.128:8080
2022-12-18 00:06:31	Company Name	No	Company Name Extractor	0	0	2	0	None	NameCheap, Inc.
2022-12-18 00:21:20	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:
2022-12-18 00:26:49	Affiliate - Domain Whois	No	Whois	5	0	6	0	None	Domain Name: dominiando.us Registry Domain ID: D19621490-US Registrar WHOIS Server: Registrar URL: https://key-systems.net Updated Da Country: IT Tech Phone: +39.0680693248 Tech Phone Ext: Tech Fax: +39.06233200178 Tech Fax Ext: Tech Email: domini@dominiando.it Tech electronic processes that apply to the registry (or its systems). Compilation, repackaging, dissemination, or other use of the WHOIS
2022-12-18 00:14:32	Country	No	Country Name Extractor	0	1	3	0	None	Iceland
2022-12-18 00:04:28	Email Gateway (DNS MX Records)	No	DNS Raw Records	0	0	1	0	None	eforward4.registrar-servers.com
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:2083
2022-12-18 00:13:46	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	6eadd514503047339410d1e131d27118.protect@withheldforprivacy.com
2022-12-18 00:04:28	Name Server (DNS NS Records)	No	DNS Raw Records	0	0	1	0	None	ns2.amenworld.com
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:19:22	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 4, u'threat_score': 81, u'compromised_ None, u'attck_id': None, u'relevance': 5, u'threat_level': 0, u'type': 7, u'description': u'"GET /file.htm HTTP/1.1\nHost: 5.105.56.8 00011898-00002812-47776-1290-00515857'}, {u'category': u'General', u'origin': u'API Call', u'identifier': u'api-6', u'name': u'Reads Characteristics', u'origin': u'Hooks', u'identifier': u'hooks-8', u'name': u'Installs hooks/patches the running process', u'attck_id_ "\\REGISTRY\\MACHINE\\SYSTEM\\CONTROLSET001\\CONTROL\\NLS\\EXTENDEDLOCALE", Key: "AR-SA")\n "<Input Sample>.exe" (Path: "\\REGISTRY\\ u'name': u'Sets the process error mode to suppress error box', u'attck_id_wiki': None, u'threat_level_human': u'suspicious', u'capec_ u'GetProcessHeap@KERNEL32.DLL at 00011898-00002812-52256-144-004DC170\n GetProcessHeap@KERNEL32.DLL at 00011898-00002812-52256-781-00
2022-12-18 00:08:39	Netblock Membership	No	RIPE	0	0	2	0	None	188.114.97.0/24
2022-12-18 00:09:48	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	autodiscover.webelievenow.com
2022-12-18 00:13:49	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	contact@vosdomaines.com
2022-12-18	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	188.114.97.9:443

00:16:27									
2022-12-18 00:05:37	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:6b:c5:5a:1c:aa:de:11:25:3a:85:ac:27:46:ac:84:c2:a9 Signature Algorithm: ecdsa-w ecdsa-with-SHA256 30:46:02:21:00:C2:6E:51:36:59:0D:CE:4E:3E:93:68: B7:52:EC:0D:A3:64:2B:FD:C3:C4:8C:29:56:48:6F:95: D8:9B:CC:44:7E:02
2022-12-18 00:03:06	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:17:08	SSL Certificate - Issued to	No	SSL Certificate Analyzer	0	0	2	0	None	C=IT,ST=Firenze,O=Register S.p.A.,CN=*.amen.fr
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetCBD2 (Net ID: 00:01:36:59:CB:D0)
2022-12-18 00:07:06	HTTP Status Code	No	Web Spider	0	0	2	0	None	200
2022-12-18 00:14:46	HTTP Status Code	No	Web Spider	0	0	2	0	None	301
2022-12-18 00:31:00	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.chat
2022-12-18 00:05:13	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObjects\\IsoScope_ca8_IESQMMUTEX_0_519"\n [targetUID: 00000000-00003240]\n Dropped file: "3LR45Z23.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\3LR45Z23.txt]- [ta "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "3LR45Z23.txt" has type "ASCII text"- Location: [% u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 5, u'threat_level': 0, u'type': 7, u'descr u'entrypoint': None, u'mitre_attcks': [{u'parent': None, u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'suspicious u'av_detect': 5, u'machine_learning_models': [], u'total_signatures': 10, u'image_base': None, u'error_origin': None, u'ssdeep': u'Ur
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	herron-libson (Net ID: 00:01:24:F1:75:B2)
2022-12-18 00:08:30	Physical Location	No	LeakIX	0	0	1	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	dabancolvalidat.dabancolvalidat.repl.co
2022-12-18 00:13:41	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	administration@nordnet.com
2022-12-18 00:09:29	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'https', u'event_type': u'service', u'ip': u'81.88.52.232', u'vendor': u'', u'port': u'443', u'transpor 02T12:46:08Z'}, u'enabled': True, u'detected': False, u'version': u'TLSv1.3'}, u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'b u''}, u'event_pipeline': [u'CertStream', u'l9scan', u'tcpid', u'HttpPlugin'], u'http': {u'status': 0, u'title': u'302 Found', u'url': u'81.88.52.232', u'vendor': u'', u'port': u'80', u'transport': [u'tcp', u'http'], u'event_source': u'l9explore', u'network': {u'organ u'continent_name': u'Europe', u'region_name': u''}, u'host': u'81.88.52.232', u'summary': u'HTTP/1.1 200 OK\r\nDate: Sun, 30 Oct 2022 u'location': u'https://expochoc4.wixsite.com/moncoutant', u'server': u'Apache'}, u'length': 0, u'favicon_hash': u'', u'root': u''}, u u'time': u'2022-11-14T17:54:48.987769642Z'}, {u'protocol': u'https', u'event_type': u'service', u'ip': u'81.88.52.232', u'vendor': u'
2022-12-18 00:06:45	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.fi
2022-12-18 00:14:47	Internet Name - Unresolved	No	VirusTotal	0	0	1	0	None	sparte.plague.fun
2022-12-18 00:22:01	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:07:47	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.in
2022-12-18 00:08:59	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.0:443
2022-12-18 00:18:27	Affiliate - Internet Name	No	DNS Resolver	0	0	2	0	None	smtp-fr.securemail.pro
2022-12-18 00:16:58	Web Content Type	No	Web Spider	0	0	4	0	None	application/javascript
2022-12-18 00:13:36	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	noc@cloudflare.com
2022-12-18 00:09:16	Physical Location	No	LeakIX	0	0	2	0	None	Campinas, Sao Paulo, Brazil
2022-12-18	Affiliate - Email	No	E-Mail Address Extractor	0	0	2	0	None	anonymous69anonymous666@gmail.com

00:24:07	Address								
2022-12-18 00:09:36	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.12:443
2022-12-18 00:22:04	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found TE: chunked Transfer-Encoding: chunked Content-Type: text/html
2022-12-18 00:18:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.3:8443
2022-12-18 00:08:30	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.52.223:80
2022-12-18 00:04:29	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "77.88.21.119:443"\n "13.249.90.138:80"\n "154.47.36.46:443"\n "142.251.40.42:443"\n "192.184.69.149:443"'}, {u'category': u'General' {0002DF01-0000-0000-C000-000000000046}\\PROGID")\n "iexplore.exe" touched "WebBrowserHandler Proxy" (Path: "HKCU\\CLSID\\{3CB169B3-17 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'descr u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': None, u'threat_level_human': u'in u'origin': u'Registry Access', u'identifier': u'registry-55', u'name': u'Reads the registry for installed applications', u'attck_id_w "https://consolegames.down10.software/bios/pcsx2-playstation-2-bios-3"\n Pattern match: "https://consolegames.down10.software"\n Heur
2022-12-18 00:02:50	IP Address	No	Mnemonic PassiveDNS	0	0	1	0	None	20.195.209.219
2022-12-18 00:21:20	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-O
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	xHamster (Category: XXXPORNXXX) https://xhamster.com/users/rasputain
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	REL (Net ID: 00:02:2D:02:35:63)
2022-12-18 00:12:09	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'188.114.96.0', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2022-12-18 00:02:47	Linked URL - Internal	No	grep.app	1	0	1	0	None	http://zerotwo-best-waifu.online/778112985743251/wap/dsc_injection"
2022-12-18 00:03:12	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-95.w90-116.abo.wanadoo.fr
2022-12-18 00:04:28	Affiliate - Internet Name	No	DNS Raw Records	7	0	1	0	None	garrett.ns.cloudflare.com
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	webpersonspichincha001--webpichinch.repl.co
2022-12-18 00:09:02	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'188.114.97.1', u'vendor': u'', u'port': u'8443', u'transpor NH', u'country_iso_code': u'NL', u'city_name': u'Amsterdam', u'location': {u'lat': 52.3759, u'lon': 4.8975}, u'country_name': u'Nethe u'password': u'', u'noauth': False, u'key': u''}, u'software': {u'modules': None, u'version': u'', u'os': u'', u'name': u'cloudflare' same-origin\r\nCache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\nExpires: Thu, 01 False, u'detected': False, u'version': u''}, u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'banner': u'', u'fingerprint': u''}, u'188.114.96.0/22'}, u'service': {u'credentials': {u'username': u'', u'raw': None, u'password': u'', u'noauth': False, u'key': u''}, GMT\r\nTransfer-Encoding: chunked\r\nConnection: close\r\nCache-Control: max-age=3600\r\nExpires: Tue, 15 Nov 2022 10:09:49 GMT\r\nLo
2022-12-18 00:04:10	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:11:26	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'ht
2022-12-18 00:10:04	BGP AS Membership	No	URLScan.io	0	0	1	0	None	8075
2022-12-18 00:25:14	Affiliate - IP Address	No	DNS Look-aside	0	0	3	0	None	81.88.48.112
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:01:24:F0:65:67)
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2086

2022-12-18 00:06:44	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 16, u'threat_score': None, u'compromis None, 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 [%TEMP%\\5812_2022650426\\shopping_fre.html]- [targetUID: 00000000-00005812]\n "77EC63BDA74BD0D0E0426DC8F8008506" has type "data"- Lo 00005812]\n "Last Browser" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Last Browser]- [targetUID: 0000000 u'description': u'Pattern match: "http://jquery-attribute-selector.barzz12.repl.co/"\n Pattern match: "http://jquery-attribute-select [targetUID: 00000000-00005812]\n Dropped file: "shopping_iframe_driver.js" - Location: [%TEMP%\\5812_2022650426\\shopping_iframe_driv u'threat_level': 0, u'size': None, u'job_id': u'63589b8fa166e1316904a3d3', u'target_url': None, u'interesting': False, u'error_type':
2022-12-18 00:09:38	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	19.koongroup.com
2022-12-18 00:08:56	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.0:8080
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:8443
2022-12-18 00:08:14	Netblock Membership	No	RIPE	4	0	1	0	None	40.112.0.0/13
2022-12-18 00:21:34	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: -
2022-12-18 00:07:17	HTTP Headers	No	Web Spider	1	0	2	0	None	{"date": "Sun, 18 Dec 2022 00:07:17 GMT", "content-length": "213", "content-type": "text/html; charset=utf-8", "connection": "close",
2022-12-18 00:25:45	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [188.114.96.1]
2022-12-18 00:16:58	Web Content	No	Web Spider	1	0	4	0	None	/*! jQuery v3.5.0 | (c) JS Foundation and other contributors | jquery.org/license */ !function(e,t){"use strict";"object"==typeof moc S.each(this,e)},map:function(n){return this.pushStack(S.map(this,function(e,t){return n.call(e,t,e)}))},slice:function(){return this. {for(n=e.length;r<n;r++)if(!1===t.call(e[r],r,e[r]))break}else for(r in e)if(!1===t.call(e[r],r,e[r]))break;return e},makeArray:funct ("+I+"))|)"+M+"*\\]",F=":("+I+")(?:\\(((('((?:\\\\.|[^\\\\']|)*)'|\"((?:\\\\.|[^\\\\\"]|)*)\")|((?:\\\\.|[^\\\\()[\\]]|"+W+")*)|.*)\\)|) {dir:"parentNode",next:"legend"});try{H.apply(t=O.call(p.childNodes),p.childNodes),t[p.childNodes.length].nodeType}catch(e){H={apply: {var n=e.split("|"),r=n.length;while(r--)b.attrHandle[n[r]]=t}function pe(e,t){var n=t&&e,r=n&&1===e.nodeType&&1===t.nodeType&&e.sour e.className="i",!e.getAttribute("className")}),d.getElementsByTagName=ce(function(e){return e.appendChild(C.createComment("")),!e.get
2022-12-18 00:04:46	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 2, u'search_terms': [{u'id': u'host', u'value': u'188.114.97.0'}], u'result': [{u'environment_id': 120, u'job_id': u'62998
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	galiciapersonal00993.tomasnuve11.repl.co
2022-12-18 00:21:20	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-C
2022-12-18 00:21:17	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:02:47	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
2022-12-18 00:10:04	BGP AS Membership	No	URLScan.io	0	0	1	0	None	3215
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pannet-24 (Net ID: 00:01:8E:DA:59:C4)
2022-12-18 00:38:04	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.1] https://www.virustotal.com/en/ip-address/188.114.96.1/information/
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:2096
2022-12-18 00:06:33	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.0:8080
2022-12-18 00:05:13	Linked URL - Internal	No	Hybrid Analysis	0	0	2	0	None	http://misogyny.wtf:2020/copy
2022-12-18 00:20:39	Raw Data from RIRs	No	Censys	0	0	1	0	None	{"last_updated_at": "2022-11-20T03:28:00.922Z", "ip": "20.195.209.219", "location_updated_at": "2022-12-18T00:20:36.645449Z", "autono
2022-12-18 00:04:28	Raw DNS Records	No	DNS Raw Records	0	0	1	0	None	rasputain.fr. 86400 IN NS garrett.ns.cloudflare.com. rasputain.fr. 86400 IN NS journey.ns.cloudflare.com.
2022-12-18 00:03:08	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.194
2022-12-	HTTP	No	Censys	0	0	2	0	None	

18 00:21:20	Headers								{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:20:42	Raw Data from RIRs	No	LeakIX	0	0	3	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'81.88.48.102', u'vendor': u'', u'port': u'80', u'transport' 12.1097}, u'country_name': u'Italy', u'continent_name': u'Europe', u'region_name': u''}, u'host': u'81.88.48.102', u'summary': u'HTTP line-height:0; } .sf-reset .clear_fix:after { display:block; height:0; clear:both; visibility:hidden; } .sf-reset .clear_fix { displa .sf-reset .block_exception { background-color:#ddd; color: #333; padding:20px; -webkit-border-top-left-radius: 16px; -webkit-border-t u'6d1f2e7ca5e9923acf1afc15f62672901ded74cf8b4652db64aad06764aad067', u'leak': {u'dataset': {u'files': 0, u'rows': 0, u'ransom_notes': u'HttpPlugin', u'network': {u'organization_name': u'Register S.p.A.', u'asn': 39729, u'network': u'81.88.48.0/20'}, u'service': {u'cr u'country_iso_code': u'IT', u'city_name': u'', u'location': {u'lat': 43.1479, u'lon': 12.1097}, u'country_name': u'Italy', u'continer
2022-12-18 00:09:21	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.7.179:8080
2022-12-18 00:29:09	Similar Domain - Whois	No	Whois	0	0	2	0	None	Domain name: plague.uk Data validation: Nominet was able to match the registrant's name and address against a 3rd party data source c
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SurfandSip (Net ID: 00:02:2D:03:87:91)
2022-12-18 00:16:59	Web Content Type	No	Web Spider	0	0	4	0	None	text/css
2022-12-18 00:26:53	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.pro
2022-12-18 00:21:03	Web Server	No	Web Server Identifier	0	0	3	0	None	Werkzeug/2.2.2 Python/3.9.11
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Dubtronicssid (Net ID: 00:01:24:F0:BB:A4)
2022-12-18 00:08:10	Netblock Membership	No	RIPE	2	0	1	0	None	137.117.0.0/16
2022-12-18 00:02:43	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2022-12-18 00:09:21	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.7.179:443
2022-12-18 00:13:45	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@1api.net
2022-12-18 00:09:49	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	awf03.com
2022-12-18 00:26:11	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	avira.com [20.226.83.185]
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	grasshopper2 (Net ID: 00:01:38:5A:88:28)
2022-12-18 00:22:01	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:12:39	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'25', u'country_tld': u'.it', u'ip': u'81.88.52.232', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2022-12-18 00:06:26	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u' 132B85B23C3A}"\n "IsoScope_a80_IESQMMUTEX_0_519"\n "IsoScope_a80_IESQMMUTEX_0_303"\n "Local\\URLBLOCK_FILEMAPSWITCH_MUTEX_2688"\n "Lo None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 8, u info"- [targetUID: N/A]\n "AI051CXT.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\AI051CXT.txt]- [ta 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 u'attck_id_wiki': None, u'threat_level_human': u'malicious', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': u'c4e316542b3c0edd73a72152a44e6bac580835dc052a34e48597f37d16bca44ed996e479de866259ce06a96c1e7d4660a0232afd0b4378784b11d43953f1d6a8',
2022-12-18 00:03:10	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 48:20:40:e9:11:6c:46:fc:13:c8:c6:91:95:a6:d1:9b Signature Algorithm: sha256WithRSA keyid:D5:FC:9E:0D:DF:1E:CA:DD:08:97:97:6E:2B:C5:5F:C5:2B:F5:EC:B8 Authority Information Access: OCSP - URI:http://ocsp.pki.goog/s/gts
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:2082
2022-12-18 00:13:56	HTTP Status Code	No	Web Spider	0	0	2	0	None	None

2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:02:52	Domain Whois	No	Whois	11	0	1	0	None	Domain Name: misogyny.wtf Registry Domain ID: 6b6c85a5f2d349d2b2f4dead736615e8-DONUTS Registrar WHOIS Server: whois.namecheap.com Reg Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Digital Whois service agree to use the data only for lawful purposes, and under no circumstances may this data be used to: a) allow, the registrar URL listed above. Access to non-public data may be provided, upon request, where it can be reasonably confirmed that th 7b20cf325f4f4ba4bc3a96b338b107cd.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organizatio
2022-12-18 00:14:32	Country	No	Country Name Extractor	0	0	3	0	None	United States
2022-12-18 00:18:44	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [188.114.97.1] https://www.virustotal.com/en/ip-address/188.114.97.1/information/
2022-12-18 00:03:24	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	179.204.149.34.bc.googleusercontent.com
2022-12-18 00:03:24	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	stream.plague.fun
2022-12-18 00:20:49	Raw Data from RIRs	No	Censys	0	0	1	0	None	{"last_updated_at": "2022-12-01T23:22:41.700Z", "ip": "51.103.210.236", "location_updated_at": "2022-12-18T00:20:46.477571Z", "autono
2022-12-18 00:28:20	Web Framework	No	Web Framework Identifier	0	0	5	0	None	Bootstrap
2022-12-18 00:25:34	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-175.w90-116.abo.wanadoo.fr
2022-12-18 00:21:09	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:
2022-12-18 00:31:07	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.doctor
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WaveLAN Network (Net ID: 00:02:2D:03:8E:D3)
2022-12-18 00:26:58	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	Key-Systems GmbH
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:02:43	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=hook.plague.fun
2022-12-18 00:20:44	Malicious IP on Same Subnet	Yes	CINS Army List	0	0	2	0	None	cinsscore.com [4.224.0.0/12] http://cinsscore.com/list/ci-badguys.txt
2022-12-18 00:13:51	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	tech@ovh.net
2022-12-18 00:18:42	Web Technology	No	Tool - WAFW00F	0	0	2	0	None	None None
2022-12-18 00:06:59	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.gg
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:443
2022-12-18 00:13:55	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:04:11	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-SH X509v3 Basic Constraints: critical CA:FALSE CT Precertificate SCTs: Signed Certificate Timestamp: Version : v1 (0x0) Log ID : E8:3E:D 30:45:02:21:00:d8:35:e0:5c:fe:c9:39:b4:06:5a:95:36:1c: 73:f4:85:1c:c5:6e:6b:ef:48:76:d6:7f:a3:fe:55:ed:82:7f: c5:02:20:7f:8c:86:3a:6f
2022-12-18 00:03:08	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.192

2022-12-18 00:09:49	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	backracerebe.tk
2022-12-18 00:09:42	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.15:8080
2022-12-18 00:21:27	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3037::6815:13f3:80
2022-12-18 00:09:45	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.9:8443
2022-12-18 00:06:31	Company Name	No	Company Name Extractor	0	0	3	0	None	Cloudflare\, Inc.
2022-12-18 00:02:48	Internet Name	No	grep.app	0	0	1	0	None	zerotwo-best-waifu.online
2022-12-18 00:21:02	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:18:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.17:8443
2022-12-18 00:20:36	Netblock Membership	No	Censys	0	0	1	0	None	137.117.0.0/16
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	101 (Net ID: 00:01:03:7B:E0:44)
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	Instagram (Category: social) https://instagram.com/rasputain
2022-12-18 00:27:44	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	7	0	None	abuse@key-systems.net
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:13	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:
2022-12-18 00:14:14	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.144:80
2022-12-18 00:09:39	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	4719296.com.cdn.cloudflare.net
2022-12-18 00:04:47	Malicious IP Address	Yes	Maltiverse	0	1	2	0	None	Maltiverse [172.67.137.37]
2022-12-18 00:09:40	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	95662222i.com
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	MarvellAP8x (Net ID: 00:01:36:16:7E:FB)
2022-12-18 00:31:03	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: plague.cloud Registry Domain ID: D9A716FCF9ACE438D92BBF2B661AE6BBB-GDREG Registrar WHOIS Server: whois-service.virtualcl REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Ad our database. Use of the Service is subject to our policies, in particular you should familiarise yourself with our Acceptable Use Po 02-15T19:19:58Z Registrar: SAV.COM, LLC Registrar IANA ID: 609 Registrar Abuse Contact Email: SUPPORT@SAV.COM Registrar Abuse Contact NS1.SEDOPARKING.COM Name Server: NS2.SEDOPARKING.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wo
2022-12-18 00:21:03	Web Technology	No	Web Server Identifier	0	0	4	0	None	Express
2022-12-18 00:06:06	Affiliate - Domain Name	No	DNS Resolver	1	0	2	0	None	securemail.pro
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:2086
2022-12-18 00:06:07	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 17, u'threat_score': None, "Local\\SM0:4284:304:WilStaging_02"\n "Local\\SM0:4284:120:WilError_01"\n "Local\\ChromeProcessSingletonStartup!"\n "\\Sessions\\1\\E b45898592ebc.tmp]- [targetUID: 00000000-00004284]\n "load_statistics.db-wal" has type "SQLite Write-Ahead Log version 3007000"- Locat type "ASCII text with very long lines with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Netw 00000000-00004284]\n "edge_tracking_page_validator.js" has type "UTF-8 Unicode text with very long lines with CRLF line terminators"-

									directory', u'attck_id_wiki': None, u'threat_level_human': u'suspicious', u'capec_id': None, u'attck_id': None, u'relevance': 5, u'th 10, u'threat_level': 1, u'type': 8, u'description': u'"Part-RU" has type "DOS executable (COM)"- Location: [%TEMP%\\4284_441219492\\F
2022-12-18 00:16:57	Linked URL - Internal	No	Web Spider	5	0	2	0	None	http://webmail.zerotwo-best-waifu.online/
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:2053
2022-12-18 00:21:30	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-O
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	GOAT (Net ID: 00:00:C5:D3:87:1C)
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	matrix (Net ID: 00:02:2D:03:92:64)
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Apple Network 3668a9 (Net ID: 00:02:2D:00:C6:8F)
2022-12-18 00:03:03	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.103
2022-12-18 00:09:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.11:8443
2022-12-18 00:03:48	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:e2:2d:48:dd:4c:ac:71:43:1c:ff:e5:61:16:60:4c:1f:a4 Signature Algorithm: sha256W X509v3 Authority Key Identifier: keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1 Authority Information Access: OCSP f5:81:77:be:6a:1b:cb:ab:d2:cc:b4:26:2f:34:2d:60:2d:fa: 7f:45:1d:72:b4:4a:39:a9:9f:7c:44:6a:07:34:0c:fd:f5:d4: fa:57:f3:6e:29:4b:a4:23
2022-12-18 00:02:45	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:3b:c1:da:8c:2d:8d:3c:49:c8:fb:3d:44:b5:c2:87:b4:3a Signature Algorithm: ecdsa-w : ecdsa-with-SHA256 30:45:02:20:4B:FA:2E:39:B5:4A:7E:1E:99:95:86:B9: B3:8A:E4:80:9D:CD:AB:17:D7:B7:40:4F:C3:9B:ED:54: 24:9C:11:BD:02:
2022-12-18 00:21:20	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:23:29	Internet Name	No	DNS Raw Records	0	0	2	0	None	zerotwo-best-waifu.online
2022-12-18 00:04:24	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:2f:49:07:90:93:a8:06:e6:05:0c:26:40:50:ef:77:d7:82 Signature Algorithm: sha256W Identifier: keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6 Authority Information Access: OCSP - URI:http://r3.o.le 03:53:f1:4b:65:8d:5a:4f:22:bb:a3:87:3b:cd:ed:50:46:83: 89:e2:9c:10:a5:4e:08:c6:11:2f:ff:ad:73:d8:bc:dd:ba:01: 53:6c:af:1a:3d:5d:46:36
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conn
2022-12-18 00:16:27	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	188.114.97.3:443
2022-12-18 00:18:19	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.7:443
2022-12-18 00:02:53	IP Address	No	Mnemonic PassiveDNS	205	0	1	0	None	34.149.204.188
2022-12-18 00:08:40	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2022-12-18 00:09:43	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'188.114.97.3', u'vendor': u'', u'port': u'80', u'transport' u'city_name': u'Amsterdam', u'location': {u'lat': 52.3759, u'lon': 4.8975}, u'country_name': u'Netherlands', u'continent_name': u'Eur {u'files': 0, u'rows': 0, u'ransom_notes': None, u'infected': False, u'collections': 0, u'size': 0}, u'type': u'', u'severity': u'', s=RoJDd3f5fsjuWB5klGxf3PlyBwXw8IOKUGUFQ2%2BJVDB0oVRQ%2B8%2BjMLE6CEynphqbYQ0aqV%2Bc%2FIIw6bOp0eLfqOqe04shN5U0MD%2BbY1SMZqRKI7EzAj%2BGF u'TLS_AES_128_GCM_SHA256', u'jarm': u'00000000000000000000000000000000000000000000000000000000000000', u'certificate': {u'domain': [u https://duckduckgo.com https://*.duckduckgo.com https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/ \'unsafe-inli s=WhCBu%2F7vZPBwdh6Ds1Iv04iqoNUqAvmYyNuXdvfAVvaV5b8kgGRWOjkk3IhaHAJkA6wpbWwrt2wqvmQcUuX6M4JX%2BmhVDewz%2ByZewI06QkfquV5isBpzZnAK"}],'
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:04:09:0C)
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	knottyshrillwireframes.bienlineagts.repl.co
2022-12-18 00:23:30	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	ftp.zerotwo-best-waifu.online. 577 IN CNAME zerotwo-best-waifu.online.
2022-12-18 00:03:10	Co-Hosted Site -	No	SSL Certificate Analyzer	0	0	1	0	None	webapps.net

	Domain Name								
2022-12-18 00:06:44	Open TCP Port	No	Pulsedive	0	0	2	0	None	104.21.19.243:8080
2022-12-18 00:05:48	Raw Data from RIRs	No	Certificate Transparency	1	0	1	0	None	[{u'not_after': u'2022-12-19T21:18:05', u'not_before': u'2022-09-20T21:18:06', u'issuer_ca_id': 180753, u'name_value': u'*.misogyny.w 23T20:47:28', u'issuer_ca_id': 183283, u'name_value': u'*.misogyny.wtf\nmisogyny.wtf', u'issuer_name': u"C=US, O=Let's Encrypt, CN=E1
2022-12-18 00:21:13	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-O
2022-12-18 00:31:08	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namecheap.com
2022-12-18 00:31:49	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: PLAGUE.ONLINE Registry Domain ID: D209164753-CNIC Registrar WHOIS Server: whois.west.cn Registrar URL: http://www.west.c abuse@west.cn Registrar Abuse Contact Phone: +86.2862778877 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/w Status: ok http://www.icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: REDACTED FOR PRIVACY Regi Name Server: ns2.myhostadmin.net DNSSEC: signedDelegation Registrar Abuse Contact Email: westabuse@gmail.com Registrar Abuse Contact
2022-12-18 00:51:57	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.54] https://www.virustotal.com/en/ip-address/188.114.96.54/information/
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	XVIDEOS-profiles (Category: XXXPORNXXX) https://www.xvideos.com/profiles/rasputain
2022-12-18 00:22:01	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:09	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-O
2022-12-18 00:20:59	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-O
2022-12-18 00:03:35	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3240.webapps.net
2022-12-18 00:02:48	IP Address	No	Mnemonic PassiveDNS	134	0	1	0	None	172.67.147.230
2022-12-18 00:09:31	Physical Location	No	LeakIX	0	0	2	0	None	United States
2022-12-18 00:08:28	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.52.222:80
2022-12-18 00:09:47	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	auroramediagroup.xyz
2022-12-18 00:18:27	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [188.114.96.1] https://www.virustotal.com/en/ip-address/188.114.96.1/information/
2022-12-18 00:09:46	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	atmospherecomm.store
2022-12-18 00:16:35	Physical Location	No	numverify	0	0	3	0	None	IS
2022-12-18 00:13:15	Affiliate Description - Category	No	DuckDuckGo	0	0	2	0	None	Technology companies based in the San Francisco Bay Area
2022-12-18 00:25:26	Physical Location	No	MetaDefender	0	0	2	0	None	Burt, United States
2022-12-18 00:16:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:04:28	Email Gateway (DNS MX Records)	No	DNS Raw Records	0	0	1	0	None	eforward5.registrar-servers.com
2022-12-18 00:32:11	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.tech
2022-12-18 00:03:04	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.107
2022-12-	Linked URL	No	URLScan.io	0	0	1	0	None	http://misogyny.wtf:2020/parser

18 00:10:04	- Internal								
2022-12-18 00:04:28	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	eforward5.registrar-servers.com
2022-12-18 00:08:56	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'188.114.96.0', u'vendor': u'', u'port': u'443', u'transport u'country_iso_code': u'NL', u'city_name': u'Amsterdam', u'location': {u'lat': 52.3759, u'lon': 4.8975}, u'country_name': u'Netherlanc u'', u'noauth': False, u'key': u''}, u'software': {u'modules': None, u'version': u'', u'os': u'', u'name': u'cloudflare', u'fingerpri 655\r\nConnection: close\r\nCF-RAY: -\r\n\nPage title: 400 The plain HTTP request was sent to HTTPS port\n\n<html>\r\n<head><title>40 0}, u'type': u'', u'severity': u'', u'stage': u''}, u'event_pipeline': [u'CertStream', u'l9scan', u'tcpid', u'HttpPlugin'], u'http': s=HCmfoNU%2B9oL6YPNZivxNLj9YuvCgpcm7upjIeEeo2Ov70Dcmfm8WvkBJc3R%2FcUtDC0b8h4PdroQq07nXdZDhyODsMBUFw0wBGWiEM3DsGWja8vIzvw0b%2F6vZ3XgyY u'location': u'https://www.literaryscout.co.uk/', u'server': u'cloudflare'}, u'length': 0, u'favicon_hash': u'', u'root': u''}, u'tag
2022-12-18 00:04:00	Country	No	Country Name Extractor	0	0	1	0	None	France
2022-12-18 00:03:14	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet8682 (Net ID: 00:01:36:5B:86:80)
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2082
2022-12-18 00:12:08	Physical Location	No	ipapi.co	0	0	2	0	None	Toronto, Ontario, ON, Canada, CA
2022-12-18 00:13:55	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:08:38	BGP AS Membership	No	RIPE	0	0	2	0	None	8075
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:06:44	Open TCP Port	No	Pulsedive	0	0	2	0	None	104.21.19.243:80
2022-12-18 00:03:23	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-113.w90-116.abo.wanadoo.fr
2022-12-18 00:16:26	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3
2022-12-18 00:13:49	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@godaddy.com
2022-12-18 00:20:16	Netblock Membership	No	RIPE	0	0	3	0	None	90.116.0.0/16
2022-12-18 00:18:28	IP Address	No	DNS Resolver	22	0	2	0	None	81.88.48.102
2022-12-18 00:09:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.0:443
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WaveLAN Network VHome2B (Net ID: 00:02:2D:03:03:11)
2022-12-18 00:03:29	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3225.webapps.net
2022-12-18 00:23:29	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	autoconfig.zerotwo-best-waifu.online. 359 IN CNAME tb-fr.securemail.pro.
2022-12-18 00:21:20	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-(
2022-12-18	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-(

00:21:27									
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F0:97:C1)
2022-12-18 00:31:46	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.nyc Registry Domain ID: D2449566-NYC Registrar WHOIS Server: whois.godaddy.com Registrar URL: whois.godaddy.com U Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: REDACTED nyc Street: REDACTED FOR PRIVACY nyc Street: REDACTED FOR PRIVACY nyc City: REDACTED FOR PRIVACY nyc State/Province: REDACTED FOR PRI your access to the Service at any time, and * the copying, compilation, repackaging, dissemination or other use of the information pr Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=plague.nyc Name Server: NS17.DOMAINCONTROL.COM Name S terms may result in termination of access to the Whois database. These terms may be subject to modification at any time without notic
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WestEd (Net ID: 00:02:2D:05:7E:85)
2022-12-18 00:09:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.8:80
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	BJNPSETUP (Net ID: 00:00:85:F4:1C:9A)
2022-12-18 00:06:15	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 8, u'threat_score': 100, u'compromised "pythoncom310.dll" has an executable section named ".text"\n "python310.dll" has an executable section named ".text"\n "libffi-7.dll' 1,movqword ptr [r13 + rax*8 + 0x18], rdx,addrax, 1,cmprax, 0x14,jne0x140001128,movrdx, r13,movrcx, r14,callrbx,subqword ptr [r13], 1, 0x4bff2],callqword ptr [rip + 0x4bfdc],movrcx, rax,"\n "python310.dll" file has an entrypoint instructions - "movqword ptr [rsp + 8], 0x2d990],movabsrbx, 0x2b992ddfa232,cmprax, rbx,jne0x1801206f3,"\n "vcruntime140.dll" file has an entrypoint instructions - "movqword + 8], rbx,movqword ptr [rsp + 0x10], rsi,pushrdi,subrsp, 0x20,movrdi, r8,movebx, edx,movrsi, rcx,cmpedx, 1,jne0x180001371,call0x18000 ptr [rsp + 8], rbx,movqword ptr [rsp + 0x10], rsi,pushrdi,subrsp, 0x20,movrdi, r8,movebx, edx,movrsi, rcx,cmpedx, 1,jne0x180001381,ca
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:22:14	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-(
2022-12-18 00:04:12	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	sni.cloudflaressl.com
2022-12-18 00:25:13	Physical Location	No	MetaDefender	0	0	1	0	None	Amsterdam, Netherlands
2022-12-18 00:20:42	Physical Location	No	LeakIX	0	0	3	0	None	Italy
2022-12-18 00:21:37	Open TCP Port	No	Censys	0	0	2	0	None	20.226.83.185:5050
2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	https://plague.fun/
2022-12-18 00:04:01	Physical Location	No	ipstack	0	0	2	0	None	United States
2022-12-18 00:06:03	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	registrar-servers.com
2022-12-18 00:04:32	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 87, u'compromised_ u'name': u'Drops files marked as clean', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id "\\Sessions\\1\\BaseNamedObjects\\Local\\!BrowserEmulation!SharedMemory!Mutex"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\VERMGMTBloc u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1012', u'threat_level_human': u'informative', u'capec_id': u'CAPEC-647', u'a "HKCU\\SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\WINTRUST\\TRUST PROVIDERS\\SOFTWARE PUBLISHING"; Key: "STATE")'}, {u'category': "HKLM\\SOFTWARE\\MICROSOFT\\SYSTEMCERTIFICATES\\AUTHROOT\\CERTIFICATES\\B51C067CEE2B0C3DF855AB2D92F4FE39D4E70F0E"; Key: "BLOB")\n "ie "80320801703208010032080160320801503208014032080130320801000000002cc9b975c021080100000000901708015023080100180801601f0801203608010000
2022-12-18 00:07:18	HTTP Headers	No	Web Spider	2	0	3	0	None	{"content-length": "1554", "x-powered-by": "Express", "accept-ranges": "bytes", "keep-alive": "timeout=5", "last-modified": "Sun, 11
2022-12-18 00:04:10	Raw Data from RIRs	No	Hybrid Analysis	0	0	1	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObjects\\IsoScope_fe0_IESQMMUTEX_0_519"\r 00004064]\n Dropped file: "36YYHGU3.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\36YYHGU3.txt]- [targetUID: 00000000-000 [%LOCALAPPDATA%\\Microsoft\\Internet Explorer\\DomainSuggestions\\en-US.4]- [targetUID: 00000000-00004064]\n "~DF8FB903D113AF51F8.TMP u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 5, u'threat_level': 0, u'type': 7, u'descr was identified as malicious by a trusted Antivirus engine', u'attck_id_wiki': None, u'threat_level_human': u'malicious', u'capec_id': u'ac8062a45cb524ba2f43df875b64dd040e0bb013e30c292b2ba51c6ed020380142aeb95b0842cb0ee3bfb8b7b9ba3e7c80b45c584b6e8f34fe099a9b70e52277',
2022-12-18 00:13:55	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-	Raw Data	No	ipapi.co	0	0	2	0	None	{u'region_code': u'NJ', u'country_tld': u'.us', u'ip': u'2606:4700:3036::ac43:a9d7', u'currency_name': u'Dollar', u'currency': u'USD'

18 00:12:44	from RIRs								
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:05:12	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObjects\\IsoScope_fe0_IESQMMUTEX_0_519"\r 00004064]\n Dropped file: "36YYHGU3.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\36YYHGU3.txt]- [targetUID: 00000000-000 [%LOCALAPPDATA%\\Microsoft\\Internet Explorer\\DomainSuggestions\\en-US.4]- [targetUID: 00000000-00004064]\n "~DF8FB903D113AF51F8.TMP u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 5, u'threat_level': 0, u'type': 7, u'descr was identified as malicious by a trusted Antivirus engine', u'attck_id_wiki': None, u'threat_level_human': u'malicious', u'capec_id': u'ac8062a45cb524ba2f43df875b64dd040e0bb013e30c292b2ba51c6ed020380142aeb95b0842cb0ee3bfb8b7b9ba3e7c80b45c584b6e8f34fe099a9b70e52277',
2022-12-18 00:09:52	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.20:80
2022-12-18 00:03:20	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-109.w90-116.abo.wanadoo.fr
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	07:55:46 (Net ID: 00:02:2D:05:BB:87)
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	SoundCloud (Category: music) https://soundcloud.com/rasputain
2022-12-18 00:12:14	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_pop
2022-12-18 00:03:06	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:09:41	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	acncnfrm.rcvry.workers.dev
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	crushingswelteringprogram.w467ujhgs3.repl.co
2022-12-18 00:41:01	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: misogyny.co Registry Domain ID: DE1B7F6E7E80840FABD3515F2E19A8DEC-NSR Registrar WHOIS Server: whois.namecheap.com Regist REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Ad individuals and organisations with a legitimate interest in accessing this data not outweighed by the fundamental privacy rights of t whatsoever, you agree to abide by these terms. In some limited cases, domains that might appear as available in whois might not actua service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province:
2022-12-18 00:20:42	BGP AS Membership	No	Censys	0	0	1	0	None	8075
2022-12-18 00:22:07	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Connection": "DISPLAY_UTF8"}, "Connection": ["close"]}
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:2086
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet55FA (Net ID: 00:01:36:59:55:F8)
2022-12-18 00:11:20	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 configurati
2022-12-18 00:36:38	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.239] https://www.virustotal.com/en/ip-address/81.88.52.239/information/
2022-12-18 00:16:37	Physical Location	No	numverify	0	0	3	0	None	FR
2022-12-18 00:06:13	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:3b:c1:da:8c:2d:8d:3c:49:c8:fb:3d:44:b5:c2:87:b4:3a Signature Algorithm: ecdsa-w : ecdsa-with-SHA256 30:45:02:20:4B:FA:2E:39:B5:4A:7E:1E:99:95:86:B9: B3:8A:E4:80:9D:CD:AB:17:D7:B7:40:4F:C3:9B:ED:54: 24:9C:11:BD:02:
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:2082
2022-12-18 00:18:30	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-313-183.w90-116.abo.wanadoo.fr
2022-12-18 00:21:09	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:07:17	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "Local\\InternetShortcutMutex"\n "{5312EE61-79E3-4A24-BFE1-132B85B23C3A}"\n "Local\\URLBLOCK_HASHFILESWITCH_MUTEX"\n "Local\\!Browser 44A7-89C5-5595FE6B30EE}\\SHELLFOLDER")\n "iexplore.exe" touched "Shockwave Flash Object" (Path: "HKCU\\CLSID\\{D27CDB6E-AE6D-11CF-96E

									{00000105-0000-0010-8000-00AA006D2EA4}\\IMPLEMENTED CATEGORIES\\{00021493-0000-0000-C000-000000000046}")\n "iexplore.exe" touched "DA u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': No "3C428B1A3E5F57D887EC4B864FAC5DCC" has type "data"\n "style.min_1_.css" has type "ASCII text with very long lines"\n "strocke-gap-ico 10, u'threat_level': 0, u'type': 2, u'description': u'Pattern match: "https://etl.am/"\n Pattern match: "https://etl.am"\n Heuristic
2022-12-18 00:04:28	Affiliate - Internet Name	No	DNS Raw Records	2	0	1	0	None	dns2.registrar-servers.com
2022-12-18 00:14:01	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.138:80
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:06:31	Company Name	No	Company Name Extractor	0	0	3	0	None	Cloudflare\, Inc.
2022-12-18 00:06:06	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	rasputin.fr
2022-12-18 00:09:54	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	buf-noodles.ga
2022-12-18 00:41:03	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@godaddy.com
2022-12-18 00:28:11	Similar Domain - Whois	No	Whois	1	0	2	0	None	% TCI Whois Service. Terms of use: % https://tcinet.ru/documents/whois_ru_rf.pdf (in Russian) % https://tcinet.ru/documents/whois_su.
2022-12-18 00:21:34	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T23:07:37.915Z", "ip": "104.21.19.243", "location_updated_at": "2022-12-14T07:44:38.029234Z", "autonom 27T13:36:45.994782676Z"}, "www.eskisehirescortol.net": {"record_type": "A", "resolved_at": "2022-11-29T17:19:25.591007856Z"}, "www.de "czasvodtaigor.cf": {"record_type": "A", "resolved_at": "2022-12-03T12:31:28.723371551Z"}, "coutupalimuldo.gq": {"record_type": "A", {"record_type": "A", "resolved_at": "2022-11-25T13:07:30.409393420Z"}, "www.bouquinistescoop.com": {"record_type": "A", "resolved_at" 13T14:29:38.631014889Z"}, "laybetting.com.au": {"record_type": "A", "resolved_at": "2022-12-10T12:09:48.597886439Z"}, "6v7trustee.sho "pilgrimhostel.ru": {"record_type": "A", "resolved_at": "2022-11-27T16:24:55.059333564Z"}, "kyotonbirdringverdi.tk": {"record_type": 07T15:43:19.629791588Z"}, "speedaruactela.ga": {"record_type": "A", "resolved_at": "2022-12-07T15:07:57.819689114Z"}, "cladmoderyra.m
2022-12-18 00:11:02	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.biz Registry Domain ID: D8343439-BIZ Registrar WHOIS Server: whois.godaddy.com Registrar URL: whois.godaddy.com U FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Stre 2022-12-18T00:11:02Z <<< For more information on Whois status codes, please visit https://icann.org/epp The Service is provided so th Domain ID: D8343439-BIZ Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2022-12-02T11: Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results. collection of this data, in part or in its entirety, for any purpose, such as transmission by e-mail, telephone, postal mail, facsimi
2022-12-18 00:41:56	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.15] https://www.virustotal.com/en/ip-address/188.114.96.15/information/
2022-12-18 00:04:59	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise Object" (Path: "HKCU\\CLSID\\{D27CDB6E-AE6D-11CF-96B8-444553540000}\\INPROCSERVER32")\n "iexplore.exe" touched "Security Manager" (Pa 000000000046}\\IMPLEMENTED CATEGORIES\\{00021493-0000-0000-C000-000000000046}")\n "iexplore.exe" touched "ItemMoniker" (Path: "HKLM\\ u'Created Mutant', u'identifier': u'mutant-0', u'name': u'Creates mutants', u'attck_id_wiki': None, u'threat_level_human': u'informat u'identifier': u'network-1', u'name': u'Contacts server', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': "80237EE4964FC9C409AAF55BF996A292_D46D6FA25B74360E1349F9015B5CCE53" has type "data"\n "favicon_2_.ico" has type "MS Windows icon reso match: "https://w.epicedufinder.org/main/https:/www.google.com.hk/async/bgasy"\n Pattern match: "https://w.epicedufinder.org"\n Heuri
2022-12-18 00:12:26	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'compromised_ deflate\nHost: performance.radar.cloudflare.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "user-agent: ")'}, {u'category': u'Gener 0, u'type': 7, u'description': u'"188.114.97.3:80"\n "104.18.31.78:443"'}, {u'category': u'Unusual Characteristics', u'origin': u'Bin [%APPDATA%\\Microsoft\\Windows\\Cookies\\63CJVUP7.txt]- [targetUID: 00000000-00002832]\n "LM0USI2F.txt" has type "ASCII text"- Locati 32x32 32 bits/pixel"- [targetUID: N/A]\n "~DF6F835D267B734551.TMP" has type "data"- Location: [%TEMP%\\~DF6F835D267B734551.TMP]- [tar application/javascript, */*;q=0.8\nReferer: http://188.114.97.3/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Tr None, u'interesting': False, u'error_type': None, u'state': u'SUCCESS', u'entrypoint': None, u'mitre_attcks': [{u'parent': None, u'at
2022-12-18 00:10:04	BGP AS Membership	No	URLScan.io	0	0	1	0	None	8075
2022-12-18 00:16:34	Raw Data from RIRs	No	numverify	0	0	3	0	None	{u'international_format': u'+19854014545', u'local_format': u'9854014545', u'number': u'19854014545', u'valid': True, u'line_type': u
2022-12-18 00:11:20	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 4.3 Description: OpenVPN, when using a 64-bit block cipher, makes
2022-12-18 00:14:32	Country	No	Country Name Extractor	0	0	3	0	None	France
2022-12-18 00:04:49	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "HKCU\\CLSID\\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\\SHELLFOLDER")\n "iexplore.exe" touched "Memory Mapped Cache Mgr" (Path: "HKCU\\

									00AA006D2EA4}\\IMPLEMENTED CATEGORIES\\{00021493-0000-0000-C000-000000000046}")\n "iexplore.exe" touched "DAO.TableDef.36" (Path: "HK "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "Local\\VERMGMTBlockListFileMutex"\n "Local\\URLBLOCK_HASHFILESWITCH_MUTEX"\n "Local\\ZonesLockedC "6BADA8974A10C4BD62CC921D13E43B18_28DEA62A0AE77228DD387E155AD0BA27" has type "data"\n "77EC63BDA74BD0D0E0426DC8F8008506" has type "da u'description': u'"iexplore.exe" (Path: "HKCU\\SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\APP PATHS\\IEXPLORE.EXE")\n "iexplore.ex "https://proapkgame.com/wp-includes/certificates/dsajlkwqe/web/"\n Pattern match: "http://www.w3.org/1999/02/22-rdf-syntax-ns#"\n Pat
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:01:24:F2:17:BC)
2022-12-18 00:21:02	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T23:14:05.428Z", "ip": "104.21.28.240", "location_updated_at": "2022-12-14T10:04:49.134613Z", "autonom "A", "resolved_at": "2022-11-26T17:07:07.854117382Z"}, "mail.wikimachine.com": {"record_type": "A", "resolved_at": "2022-11-30T14:18: 10T12:12:10.879895874Z"}, "holistic-holidays.com": {"record_type": "A", "resolved_at": "2022-11-20T13:29:50.235437517Z"}, "manandmeat 10T13:03:00.468363640Z"}, "thenheppsinforddantca.tk": {"record_type": "A", "resolved_at": "2022-12-09T16:45:26.377109728Z"}, "cpanel. {"record_type": "A", "resolved_at": "2022-11-14T16:49:07.690130423Z"}, "www.generalia.online.cdn.cloudflare.net": {"record_type": "A" 16T16:38:55.275899988Z"}, "majeronibraces.com": {"record_type": "A", "resolved_at": "2022-12-16T13:31:16.728181958Z"}, "www.bettingma "2022-11-18T12:15:11.721015572Z"}, "propdifportfidolo.ml": {"record_type": "A", "resolved_at": "2022-12-11T15:21:35.046116976Z"}, "cp
2022-12-18 00:06:14	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.com
2022-12-18 00:05:59	Affiliate - Domain Name	No	DNS Resolver	2	0	2	0	None	registrar-servers.com
2022-12-18 00:04:00	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:5f:2b:c4:e2:52:ac:ba:5b:55:25:2b:3c:57:78:0c:6b:4f Signature Algorithm: sha256W Identifier: keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6 Authority Information Access: OCSP - URI:http://r3.o.le 1c:d2:43:47:36:d4:6f:4a:b3:42:ed:98:0f:cc:f8:88:ab:f9: 42:42:17:25:8b:39:55:d4:b8:65:63:af:0d:c1:cd:ba:03:81: 81:9e:3c:10:74:65:96:bf
2022-12-18 00:02:39	Internet Name	No	SpiderFoot UI	147	0	0	0	None	plague.fun
2022-12-18 00:03:14	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-99.w90-116.abo.wanadoo.fr
2022-12-18 00:16:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	sni.cloudflaressl.com
2022-12-18 00:10:04	Internet Name - Unresolved	No	URLScan.io	0	0	1	0	None	obf.plague.fun
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:25:00	Physical Location	No	MetaDefender	0	0	1	0	None	Amsterdam, Netherlands
2022-12-18 00:22:01	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2a06:98c1:3121::/48
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:09:24	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.7:8443
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	18c34ac2-fa7a-4b78-b7ff-ef204b07e192.id.repl.co
2022-12-18 00:02:49	Raw Data from RIRs	No	Certificate Transparency	6	0	1	0	None	[{u'not_after': u'2023-02-02T13:11:40', u'not_before': u'2022-11-04T13:11:41', u'issuer_ca_id': 183267, u'name_value': u'atlas.plague u'name_value': u'*.plague.fun\nplague.fun', u'issuer_name': u"C=US, O=Let's Encrypt, CN=E1", u'common_name': u'*.plague.fun', u'seria u'0443a47d291f150e6bac86e44bc0be6971a9', u'entry_timestamp': u'2022-10-06T21:16:48.471', u'id': 7688527736}, {u'not_after': u'2022-11 7401145896}, {u'not_after': u'2022-11-22T16:36:09', u'not_before': u'2022-08-24T16:36:10', u'issuer_ca_id': 183267, u'name_value': u' u'api.plague.fun', u'issuer_name': u"C=US, O=Let's Encrypt, CN=R3", u'common_name': u'api.plague.fun', u'serial_number': u'042f490796 u'03d81f4b915bd7bf2fbe6e278c6c60f68680', u'entry_timestamp': u'2022-05-06T18:46:04.096', u'id': 6677169275}, {u'not_after': u'2022-07 {u'not_after': u'2022-06-06T17:39:26', u'not_before': u'2022-03-08T17:39:27', u'issuer_ca_id': 183283, u'name_value': u'*.plague.fun\
2022-12-18 00:13:48	Web Content Language	No	Language Detector	0	0	3	0	None	English
2022-12-18 00:09:42	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	aiiasp.com
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:2095
2022-12-18 00:08:59	Physical Location	No	LeakIX	0	0	2	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:32:06	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.software

2022-12-18 00:09:47	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	autoconceitoveiculos.com.br
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:2053
2022-12-18 00:24:02	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: PLAGUE.NET Registry Domain ID: 33118110_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.PublicDomainRegistry.com Registrar the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2022-09-03T19:07:30Z info.thorofare.biz DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Pho
2022-12-18 00:06:04	Affiliate - Domain Name	No	DNS Resolver	2	0	2	0	None	cloudflare.com
2022-12-18 00:02:48	IP Address	No	Mnemonic PassiveDNS	64	0	1	0	None	172.67.190.129
2022-12-18 00:04:30	Email Gateway (DNS MX Records)	No	DNS Raw Records	0	0	1	0	None	mail-fr.securemail.pro
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	serviciosbancpichinchacomecu.ecuador0.repl.co
2022-12-18 00:03:07	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.187
2022-12-18 00:18:28	Affiliate - Domain Name	No	DNS Resolver	2	0	3	0	None	setupdns.net
2022-12-18 00:10:04	Raw Data from RIRs	No	URLScan.io	0	0	1	0	None	[{u'sort': [1666956116154, u'38aa66fb-392e-4d9e-b65f-c673218e73c9'], u'task': {u'domain': u'rasputain.fr', u'uuid': u'38aa66fb-392e-4
2022-12-18 00:14:29	Malicious IP Address	Yes	Internet Storm Center	0	1	2	0	None	Internet Storm Center [188.114.96.3] https://isc.sans.edu/api/ip/188.114.96.3
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:2052
2022-12-18 00:21:58	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-16T03:45:34.561Z", "ip": "2a06:98c1:3120::1", "location_updated_at": "2022-12-06T04:37:36.513741Z", "aut {"record_type": "AAAA", "resolved_at": "2022-09-24T19:46:42.025854438Z"}, "password.moeking.me": {"record_type": "AAAA", "resolved_at content=\"text/html; charset=UTF-8\" />\n<meta http-equiv=\"X-UA-Compatible\" content=\"IE=Edge\" />\n<meta name=\"robots\" content=\ id=\"cookie-alert\" data-translate=\"enable_cookies\">Please enable cookies. \n <div id=\"cf-error-details\" class=\"p-0\">\n <h interested in learning more about Cloudflare, please <a href=\"https://www.cloudflare.com/5xx-error-landing/\" target=\"_blank\">visi class=\"cf-footer-item sm:block sm:mb-1\">Performance & security by <a rel=\"noopener noreferrer\" href=\"https://ww "X_Frame_Options": "DISPLAY_UTF8", "Cache_Control": "DISPLAY_UTF8"}, "Referrer_Policy": ["same-origin"], "Expires": ["Thu, 01 Jan 197
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	20:35:09 (Net ID: 00:02:2D:05:BE:2A)
2022-12-18 00:05:59	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 0, u'threat_score': None, u'compromise for MS Windows', u'file_metadata': None, u'dll_characteristics': [], u'vx_family': u'Lazy.Generic', u'environment_description': u'Sta u'name': u'Contains PDB pathways', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': Non "HKLM\\SOFTWARE\\POLICIES\\MICROSOFT\\SYSTEMCERTIFICATES\\CA\\CTLS"; Key: "")\n "powershell.exe" (Path: "HKCU\\SOFTWARE\\POLICIES\\MI u'capec_id': None, u'attck_id': None, u'relevance': 0, u'threat_level': 0, u'type': 9, u'description': u'Report process "WerFault.exe "HKLM\\SOFTWARE\\MICROSOFT\\SYSTEMCERTIFICATES\\FLIGHTROOT"; Key: "")\n "Loader.exe" (Path: "HKLM\\SOFTWARE\\MICROSOFT\\SYSTEMCERTIFI environment. -->\n\n Windows Vista -->\n <supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}" />-->\n\n Windows 7 -->\n <supporte
2022-12-18 00:21:47	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T21:38:21.662Z", "ip": "2606:4700:3032::ac43:8925", "location_updated_at": "2022-12-03T18:33:45.372439 "nerdietech.com": {"record_type": "AAAA", "resolved_at": "2022-12-14T14:00:07.987200637Z"}, "pghbusinessplus.com": {"record_type": "A "resolved_at": "2022-11-30T13:19:53.251533196Z"}, "www.bulkwear.club": {"record_type": "AAAA", "resolved_at": "2022-12-03T12:35:06.13 09T13:32:30.257830741Z"}, "marcjacobsbagsshops.com": {"record_type": "AAAA", "resolved_at": "2022-11-28T13:29:45.465305047Z"}, "ido.m {"record_type": "AAAA", "resolved_at": "2022-12-01T15:43:49.524130454Z"}, "rjoutdoorsolutions.com": {"record_type": "AAAA", "resolved 22T15:58:03.273859266Z"}, "torrent.dylansheffer.app": {"record_type": "AAAA", "resolved_at": "2022-11-30T12:06:29.302819464Z"}, "www. {"record_type": "AAAA", "resolved_at": "2022-12-14T15:20:56.567076509Z"}, "pl.ukrainianwomen.date": {"record_type": "AAAA", "resolved
2022-12-18 00:21:06	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-
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	validarpichincha--ecuadorr.repl.co
2022-12-18 00:40:30	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.10] https://www.virustotal.com/en/ip-address/188.114.96.10/information/
2022-12-18 00:03:10	SSL Certificate - Issued to	No	SSL Certificate Analyzer	0	0	1	0	None	C=IT,ST=Firenze,O=Register S.p.A.,CN=*.webapps.net
2022-12-18 00:10:04	Web Server	No	URLScan.io	0	1	1	0	None	Werkzeug/2.2.2 Python/3.8.10

2022-12-18 00:02:48	Co-Hosted Site	No	CertSpotter	0	0	1	0	None	sni.cloudflaressl.com
2022-12-18 00:32:13	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.tools
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:24:56	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.178
2022-12-18 00:23:32	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	webmail.zerotwo-best-waifu.online. 900 IN CNAME webmail-fr.setupdns.net.
2022-12-18 00:33:43	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.188:8080
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:8443
2022-12-18 00:09:40	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	a-prime-us-credit-cards.zone
2022-12-18 00:18:46	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.20:443
2022-12-18 00:32:33	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.154:80
2022-12-18 00:31:32	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.link
2022-12-18 00:08:24	Netblock Membership	No	RIPE	0	0	2	0	None	188.114.96.0/24
2022-12-18 00:05:27	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 50, u'compromised_ u'network-1', u'name': u'Contacts server', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_ "4K1MNPLT.txt" has type "ASCII text"\n "77EC63BDA74BD0D0E0426DC8F8008506" has type "data"\n "RecoveryStore._C7A4F1AE-D920-11E7-B48D-0 "https://loginslink.com"\n Heuristic match: "loginslink.com"\n Pattern match: "https://www.msn.com/spartan/ientpgbconfig?locale=en-us None, u'attck_id': None, u'relevance': 0, u'threat_level': 1, u'type': 12, u'description': u'1/93 Antivirus vendors marked sample as u'md5': u'e42f8f7948a2967d4cc53f65162d9389', u'network_mode': u'default', u'processes': [], u'sha1': u'ff9b29c3034fc1f366f8d7fd7b8b97
2022-12-18 00:21:11	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)
2022-12-18 00:18:35	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.15:80
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:13:56	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:29:08	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.org.uk
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	krillnet (Net ID: 00:01:8E:15:D4:A6)
2022-12-18 00:11:10	Similar Domain - Whois	No	Whois	1	0	2	0	None	% The WHOIS service offered by EURid and the access to the records % in the EURid WHOIS database are provided for information purpose content of the WHOIS database. % % By submitting the query you agree to abide by this policy and accept % that EURid can take measure
2022-12-18 00:12:04	Country	No	Country Name Extractor	0	0	3	0	None	United States
2022-12-18 00:16:27	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
2022-12-18 00:09:14	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.2:80
2022-12-18 00:07:06	HTTP Headers	No	Web Spider	1	0	2	0	None	{"date": "Sun, 18 Dec 2022 00:07:06 GMT", "content-length": "213", "content-type": "text/html; charset=utf-8", "connection": "close",
2022-12-18 00:14:46	Internet Name - Unresolved	No	VirusTotal	0	0	1	0	None	obf.plague.fun

2022-12-18 00:03:19	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-108.w90-116.abo.wanadoo.fr
2022-12-18 00:09:31	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.169.215:443
2022-12-18 00:20:42	Open TCP Port	No	LeakIX	0	0	3	0	None	81.88.48.102:443
2022-12-18 00:14:05	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 4.3 Description: OpenVPN, when using a 64-bit block cipher, makes
2022-12-18 00:27:14	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.48.102:443
2022-12-18 00:21:02	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:30:48	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.app
2022-12-18 00:25:33	Affiliate - Domain Name	No	DNS Resolver	0	0	3	0	None	securemail.pro
2022-12-18 00:04:28	Raw DNS Records	No	DNS Raw Records	0	0	1	0	None	misogyny.wtf. 1800 IN MX 20 eforward5.registrar-servers.com. misogyny.wtf. 1800 IN MX 15 eforward4.registrar-servers.com. misogyny.wt
2022-12-18 00:21:03	Web Technology	No	Web Server Identifier	0	0	4	0	None	Express
2022-12-18 00:21:03	Web Technology	No	Web Server Identifier	0	0	3	0	None	Express
2022-12-18 00:10:49	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 5.0 Description: The DES and Triple DES ciphers, as used in the T
2022-12-18 00:02:55	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:43:a4:7d:29:1f:15:0e:6b:ac:86:e4:4b:c0:be:69:71:a9 Signature Algorithm: sha256W SHA256 30:46:02:21:00:B6:95:B7:C7:1C:80:2B:FD:7A:41:2D: D1:EE:2B:F0:0C:C7:D5:AD:4A:C9:E0:25:F1:61:3A:42: F4:C7:98:23:BC:02:21:00:B0:8
2022-12-18 00:31:50	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: PLAGUE.ONL Registry Domain ID: D425500000332721757-AGRS Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://A guaranteed. This service is intended only for query-based access. You agree that you will use this data only for lawful purposes and clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#client Ext: Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=plague.onl Name Server: NS65. to comply with these terms may result in termination of access to the Whois database. These terms may be subject to modification at a
2022-12-18 00:14:30	Malicious IP Address	Yes	Internet Storm Center	0	1	2	0	None	Internet Storm Center [188.114.97.3] https://isc.sans.edu/api/ip/188.114.97.3
2022-12-18 00:12:19	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+19854014545
2022-12-18 00:10:04	Linked URL - Internal	No	URLScan.io	0	0	1	0	None	http://misogyny.wtf:8080/
2022-12-18 00:07:29	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:12:44	Physical Location	No	ipapi.co	0	0	2	0	None	Newark, New Jersey, NJ, United States, US
2022-12-18 00:24:07	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	info@newtabgallery.com
2022-12-18 00:07:19	HTTP Status Code	No	Web Spider	0	0	3	0	None	200
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2052
2022-12-18 00:06:07	Internet Name	No	DNS Resolver	0	0	2	0	None	misogyny.wtf
2022-12-	Open TCP	No	Pulsedive	0	0	3	0	None	

18 00:18:19	Port								188.114.97.7:80
2022-12-18 00:22:14	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-O
2022-12-18 00:25:06	Physical Location	No	MetaDefender	0	0	1	0	None	Zuerich, Switzerland
2022-12-18 00:21:13	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:
2022-12-18 00:18:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.11:8080
2022-12-18 00:12:00	Physical Location	No	ipapi.co	1	0	1	0	None	Zurich, Zurich, ZH, Switzerland, CH
2022-12-18 00:05:02	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'compromised_ u'network-1', u'name': u'Contacts server', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_ /prefetch:2" (UID: 00065504-00001828)'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-0', u'name variables: "PATH="%PROGRAMFILES%\\Internet Explorer;""\n Process "iexplore.exe" (UID: 00065473-00003164) was launched with modified e "iexplore.exe" wrote bytes "401cd5f4fe070000" to virtual address "0xFD962390" (part of module "GDI32.DLL")\n "iexplore.exe" wrote byt "MSCTF.DLL")\n "iexplore.exe" wrote bytes "00efd5f4fe070000" to virtual address "0xFDAD0A30" (part of module "OLEAUT32.DLL")\n "iexpl text"\n "prebid_1_.js" has type "ASCII text with very long lines"\n "bl-04a3385-0e6d5adc_1_.js" has type "ASCII text with very long l
2022-12-18 00:09:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.8:8443
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conn
2022-12-18 00:02:50	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:6b:c5:5a:1c:aa:de:11:25:3a:85:ac:27:46:ac:84:c2:a9 Signature Algorithm: ecdsa-w 30:03:c9:aa:f7:e7:41:d6:3c:a5:0a:5a:1b:57:5a:06:d4:2b: b1:c3:23:17:ba:be:0f:99:c0:9a:36:c9:f2:ce:f3:30:3e:9e: a0:05:0c:ae:61:ce:b0:e0
2022-12-18 00:05:56	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 22, u'threat_score': None, u'compromis "Local\\ChromeProcessSingletonStartup!"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:648:120:WilError_01"\n "\\Sessions\\1\\BaseNam "f_00023e" has type "JPEG image data JFIF standard 1.01 aspect ratio density 1x1 segment length 16 baseline precision 8 1613x1075 com Data\\CertificateRevocation\\6498.2022.5.1\\manifest.fingerprint]- [targetUID: 00000000-00000648]\n "data_2" has type "dBase III DBT u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 2, u'description': u'Pattern match: "https://mis [targetUID: 00000000-00000648]\n Dropped file: "notification.bundle.js" - Location: [%TEMP%\\648_1384275148\\Notification\\notificati [%TEMP%\\648_1384275148\\wallet.bundle.js]- [targetUID: 00000000-00000648]\n Dropped file: "edge_confirmation_page_validator.js" - Lo
2022-12-18 00:04:11	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	188.114.97.0:443
2022-12-18 00:05:36	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 17, u'threat_score': 100, u u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_human': u'informat [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 00000000-00008116]\n "edge [targetUID: 00000000-00007968]\n "ecf59d3c-3e59-4f4d-88b1-71807e9fa5d6.tmp" has type "UTF-8 Unicode text with very long lines with no 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'desc [%TEMP%\\8116_958770106\\edge_confirmation_page_validator.js]- [targetUID: 00000000-00008116]\n Dropped file: "shopping_iframe_driver u'"msedge.exe" wrote 8192 bytes starting with PE header signature to file "%TEMP%\\8116_1522156826_platform_specific\\win_x64\\wide
2022-12-18 00:04:12	Linked URL - Internal	No	Hybrid Analysis	4	0	1	0	None	http://misogyny.wtf:2020/copy
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	03086f92-df30-4cdf-b616-eecb6721ccc7.id.repl.co
2022-12-18 00:34:43	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.231] https://www.virustotal.com/en/ip-address/81.88.52.231/information/
2022-12-18 00:09:27	Open TCP Port	No	LeakIX	0	0	2	0	None	34.149.204.188:443
2022-12-18 00:32:11	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.222] https://www.virustotal.com/en/ip-address/81.88.52.222/information/
2022-12-18 00:21:51	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: -
2022-12-18 00:24:06	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	7a26cfb315a34ab485d0721288efdfea.protect@withheldforprivacy.com
2022-12-18 00:09:45	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'https', u'event_type': u'service', u'ip': u'188.114.96.9', u'vendor': u'', u'port': u'443', u'transpor u'key_algo': u'ECDSA', u'not_before': u'2022-11-04T12:56:12Z'}, u'enabled': True, u'detected': False, u'version': u'TLSv1.3'}, u'mac' u'network': u'188.114.96.0/22'}, u'service': {u'credentials': {u'username': u'', u'raw': None, u'password': u'', u'noauth': False, u' u'host': u'top10bistro.com', u'summary': u'Date: Fri, 04 Nov 2022 13:56:42 GMT\r\nTransfer-Encoding: chunked\r\nConnection: close\r\n 0}, u'type': u'', u'severity': u'', u'stage': u''}, u'event_pipeline': [u'CertStream', u'l9scan', u'tcpid', u'HttpPlugin'], u'http':

									s=CpJYObmrZxUEjtvW%2BcEZwM5ZylF18DqyYGiCT4ibPJNc6EQerraynSTrS9chLpdcVMZyGUFDAkdko5KHdF2qiiGOwZTLrq34JOTiRm7FLofnmnMGih1q%2BFdH%2FAfZe u'0000000000000000000000000000000000000000000000000000000000000000', u'certificate': {u'domain': [u'*.thropadvenra.tk', u'thropadvenra.
2022-12-18 00:41:03	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	46710fa45d0846bc845a969a73e8377e.protect@withheldforprivacy.com
2022-12-18 00:04:11	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
2022-12-18 00:03:05	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.110
2022-12-18 00:03:05	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.113
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:8443
2022-12-18 00:09:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.10:8443
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:03:34	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3237.webapps.net
2022-12-18 00:31:37	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.media Registry Domain ID: 6625164ce7ec46d0ab55b0957b9dd14b-DONUTS Registrar WHOIS Server: whois.godaddy.com/ Regi Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED Whois service for information purposes, and to assist persons in obtaining information about or related to a domain name registration Public Data] tag indicates that such data is not made publicly available due to applicable data privacy laws or requirements. Should
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:10:59	Affiliate - Domain Whois	No	Whois	3	0	4	0	None	%% %% This is the AFNIC Whois server. %% %% complete date format: YYYY-MM-DDThh:mm:ssZ %% %% Rights restricted by copyright. %% See h 29T00:00:00Z reachstatus: not identified source: FRNIC nic-hdl: BLF14-FRNIC type: PERSON contact: Beatrice Leopold Fenu address: 78 C
2022-12-18 00:21:20	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:
2022-12-18 00:07:57	Malicious Internet Name	Yes	Cleanbrowsing.org	0	1	1	0	None	Blocked by Cleanbrowsing.org [zerotwo-best-waifu.online]
2022-12-18 00:02:48	IP Address	No	Mnemonic PassiveDNS	56	0	1	0	None	104.21.19.243
2022-12-18 00:04:38	Raw Data from RIRs	No	Maltiverse	3	0	2	0	None	{u'asn_registry': u'arin', u'country_code': u'US', u'classification': u'suspicious', u'asn_country_code': u'US', u'is_open_proxy': Fa False, u'as_name': u'AS13335 - Cloudflare, Inc.', u'is_vpn_node': False}
2022-12-18 00:08:28	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.52.222:443
2022-12-18 00:09:00	Physical Location	No	LeakIX	0	0	2	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:03:05	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	hook.plague.fun
2022-12-18 00:03:25	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	182.204.149.34.bc.googleusercontent.com
2022-12-18 00:03:09	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.228
2022-12-18 00:41:00	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	misogyny.co
2022-12-18 00:22:09	Malicious Internet Name	Yes	Cleanbrowsing.org	0	1	2	0	None	Blocked by Cleanbrowsing.org [webmail.zerotwo-best-waifu.online]
2022-12-18 00:18:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.8:80
2022-12-18 00:03:04	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:a4:99:c7:6c:cb:8c:60:87:12:4d:ac:6d:aa:bc:48:46:46 Signature Algorithm: ecdsa-w with-SHA256 30:45:02:21:00:C6:AF:8E:EE:35:F5:BA:0F:D5:07:B3: CD:FF:DA:80:2E:52:74:BF:5E:FA:32:A4:C1:96:32:07: EA:B1:FD:8C:77:02:20:55
2022-12-	Open TCP	No	Pulsedive	0	0	3	0	None	

18 00:09:18	Port								188.114.96.4:8080
2022-12-18 00:04:28	Email Gateway (DNS MX Records)	No	DNS Raw Records	0	0	1	0	None	eforward2.registrar-servers.com
2022-12-18 00:03:05	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.114
2022-12-18 00:03:04	IP Address	No	DNS Resolver	56	0	1	0	None	172.67.169.215
2022-12-18 00:21:51	Netblock Membership	No	Censys	0	0	2	0	None	172.67.128.0/20
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:11:27	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
2022-12-18 00:21:37	Open TCP Port	No	Censys	0	0	2	0	None	20.226.83.185:2020
2022-12-18 00:16:59	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2022-12-18 00:22:07	Physical Location	No	Censys	1	0	2	0	None	Kansas City, Missouri, 64184, United States, North America
2022-12-18 00:23:19	Country	No	Country Name Extractor	0	0	3	0	None	United States
2022-12-18 00:04:28	Affiliate - Internet Name	No	DNS Raw Records	2	0	1	0	None	dns1.registrar-servers.com
2022-12-18 00:09:48	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	autodiscover.nensi.eu
2022-12-18 00:22:14	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-O
2022-12-18 00:09:33	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.27.242:80
2022-12-18 00:13:35	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@cloudflare.com
2022-12-18 00:25:32	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [188.114.96.0]
2022-12-18 00:20:56	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:4700:3031::/48
2022-12-18 00:03:07	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.186
2022-12-18 00:10:20	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 configurati
2022-12-18 00:02:53	IP Address	No	Mnemonic PassiveDNS	35	0	1	0	None	90.116.166.104
2022-12-18 00:13:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.128:80
2022-12-18 00:06:41	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise 132B85B23C3A}"\n "UpdatingNewTabPageData"\n "Local\\URLBLOCK_HASHFILESWITCH_MUTEX"\n "IsoScope_ca8_IESQMMUTEX_0_331"\n "IsoScope_ca8_ */*\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflat Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: dinamico.vencimiento.repl dinamico.vencimiento.repl.co\nDNT: 1\nConnection: Keep-Alive" (Indicator: "user-agent: ")\n "GET /hfh/ui.css HTTP/1.1\nAccept: text/c https://dinamico.vencimiento.repl.co/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Ge 6.1; Trident/7.0; rv:11.0) like Gecko\nOrigin: https://dinamico.vencimiento.repl.co\nAccept-Encoding: gzip, deflate\nHost: dinamico.v
2022-12-18 00:04:38	Malicious IP Address	Yes	Maltiverse	0	1	2	0	None	Maltiverse [172.67.147.230]
2022-12-18 00:25:34	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-173.w90-116.abo.wanadoo.fr
2022-12-	Web	No	Web Spider	0	0	4	0	None	/*! * Font Awesome 4.4.0 by @davegandy - http://fontawesome.io - @fontawesome * License - http://fontawesome.io/license (Font: SIL OF

18 00:16:59	Content								right{margin-left:.3em}.fa-spin{-webkit-animation:fa-spin 2s infinite linear;animation:fa-spin 2s infinite linear}.fa-pulse{-webkit-a height:2em;vertical-align:middle}.fa-stack-1x,.fa-stack-2x{position:absolute;left:0;width:100%;text-align:center}.fa-stack-1x{line-he volume-down:before{content:"\f027"}.fa-volume-up:before{content:"\f028"}.fa-qrcode:before{content:"\f029"}.fa-barcode:before{content: forward:before{content:"\f051"}.fa-eject:before{content:"\f052"}.fa-chevron-left:before{content:"\f053"}.fa-chevron-right:before{cont folder:before{content:"\f07b"}.fa-folder-open:before{content:"\f07c"}.fa-arrows-v:before{content:"\f07d"}.fa-arrows-h:before{content: left:before{content:"\f0a5"}.fa-hand-o-up:before{content:"\f0a6"}.fa-hand-o-down:before{content:"\f0a7"}.fa-arrow-circle-left:before{
2022-12-18 00:31:08	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	116cc296f60d4885bbe79883230f5566.protect@withheldforprivacy.com
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	wobblyfalallogin00.fdawfa0002.repl.co
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:2083
2022-12-18 00:12:19	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+14259744689
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:24:07	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	support@newtabwallpaperstheme.com
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:09:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.11:443
2022-12-18 00:10:04	Linked URL - Internal	No	URLScan.io	2	0	1	0	None	http://rasputain.fr/
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	redwood (Net ID: 00:01:38:85:C1:F8)
2022-12-18 00:07:11	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'172.67.169.215'}], u'result': [{u'environment_id': 160, u'job_id': u'639
2022-12-18 00:20:44	Malicious IP on Same Subnet	Yes	CINS Army List	0	0	2	0	None	cinsscore.com [20.192.0.0/10] http://cinsscore.com/list/ci-badguys.txt
2022-12-18 00:12:13	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_pop
2022-12-18 00:07:13	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 2, u'threat_score': None, u'compromise "HKLM\\SOFTWARE\\MICROSOFT\\SYSTEMCERTIFICATES\\FLIGHTROOT\\CERTIFICATES"; Key: "08745487E891C19E3078C1F2A07E452950EF36F6")\n "Ledger "0x37f800" greater than 0x100000\n Raw size of ".text" is "0x211e00" greater than 0x100000'}, {u'category': u'General', u'origin': u' ".text"\n "nsis7z.dll" has an executable section named ".text"\n "ledger.exe" has an executable section named ".text"\n "Uninstall Le Virtual size of ".data" is "0x15e198" greater than 0x100000'}, {u'category': u'General', u'origin': u'String', u'identifier': u'strir u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 2, u'descr u'General', u'origin': u'Static Parser', u'identifier': u'static-95', u'name': u'PE file contains writable sections', u'attck_id_wiki
2022-12-18 00:07:55	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.io
2022-12-18 00:25:44	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	ns.dominiando.uk
2022-12-18 00:21:47	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-(
2022-12-18 00:09:54	Hosting Provider	No	Hosting Provider Identifier	0	1	1	0	None	Microsoft Azure: http://www.windowsazure.com/en-us/
2022-12-18 00:18:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.4:8443
2022-12-	Malicious IP	Yes	MetaDefender	0	0	1	0	None	

18 00:24:54	Address								webroot.com [4.228.83.86]
2022-12-18 00:12:03	Physical Location	No	ipapi.co	1	0	2	0	None	Newark, New Jersey, NJ, United States, US
2022-12-18 00:11:12	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: IFU.ONLINE Registry Domain ID: D9964885-CNIC Registrar WHOIS Server: whois.ascio.com Registrar URL: http://www.ascio.com https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2022-12-18T00:11:12.0Z <<< For more information on Whois status codes, Name: Not Disclosed Registrant Organization: Not Disclosed Registrant Street: Not Disclosed Registrant City: Not Disclosed Registrant provided by Ascio Technologies for information purposes only. By submitting a WHOIS query, you agree that you will use this data only
2022-12-18 00:04:52	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "IsoScope_db8_ConnHashTable<3512>_HashTable_Mutex"\n "UpdatingNewTabPageData"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\!BrowserEmul [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\6BADA8974A10C4BD62CC921D13E43B18_28DEA62A0AE77228DD387E155AD0BA27]- [targ [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\57C8EDB95DF3F0AD4EE2DC2B8CFD4157]- [targetUID: 00000000-00003512]\n "main_ 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' Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: 188.114.96.1\nDNT: 1\nConnection: Keep-Alive"'}, {u'category' u'entrypoint_section': None, u'md5': u'0f5534822f97323db2ede42413f1e07d', u'network_mode': u'default', u'processes': [], u'sha1': u'c
2022-12-18 00:03:10	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:09:14	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.2:8080
2022-12-18 00:10:04	Linked URL - Internal	No	URLScan.io	0	0	1	0	None	http://misogyny.wtf/inject/UsRjS959Rqm4sPG4
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:443
2022-12-18 00:08:28	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.52.222:21
2022-12-18 00:09:41	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	acnscrt.rcvry.workers.dev
2022-12-18 00:26:44	Physical Location	No	MetaDefender	0	0	2	0	None	Kansas City, United States
2022-12-18 00:21:34	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-O
2022-12-18 00:19:10	Hosting Provider	No	Hosting Provider Identifier	0	0	3	0	None	register.it: http://we.register.it/
2022-12-18 00:21:37	Netblock Membership	No	Censys	0	0	2	0	None	20.192.0.0/10
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	20:35:09 (Net ID: 00:02:2D:05:BE:2A)
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:8080
2022-12-18 00:12:49	Physical Location	No	ipapi.co	0	0	2	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2022-12-18 00:20:39	Physical Location	No	Censys	1	0	1	0	None	Campinas, Sao Paulo, Brazil, South America
2022-12-18 00:09:52	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	blogcast.support
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:443
2022-12-18 00:21:20	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:
2022-12-18 00:26:58	Affiliate - Company Name	No	Company Name Extractor	0	0	7	0	None	Registry Services, LLC
2022-12-18 00:02:54	Domain Registrar	No	Whois	0	0	1	0	None	ENOM, INC.
2022-12-18 00:12:04	Country	No	Country Name Extractor	0	0	3	0	None	United States
2022-12-	Domain	No	DNS Resolver	0	0	1	0	None	

18 00:03:05	Name								rasputain.fr
2022-12-18 00:09:27	Physical Location	No	LeakIX	0	0	2	0	None	Kansas City, Missouri, United States
2022-12-18 00:04:01	Country	No	Country Name Extractor	0	0	2	0	None	France
2022-12-18 00:06:37	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 15, u'threat_score': 100, u "Local\\ChromeProcessSingletonStartup!"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:7300:304:WilStaging_02"\n "\\Sessions\\1\\Base [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\CertificateRevocation\\6498.2022.5.1\\manifest.json]- [targetUID: 00000000-00007300]\n ' terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\6f303046-038f-4d70-8605-69e3084c809f.tmp]- [targetUID: 00000000- "https://567893.568093.repl.co"\n Heuristic match: "567893.568093.repl.co"\n Heuristic match: "1t;ps_//\'56_893.__6_C93.repl.co"'}, { "product_page.js" - Location: [%TEMP%\\7300_288640161\\product_page.js]- [targetUID: 00000000-00007300]\n Dropped file: "edge_checkou Data\\Default\\blob_storage\\d0313995-11ad-4fbc-ac47-fb134ed2e3e0" (Indicator: "microsoft\\edge\\user data") in Source: 00000000-0000
2022-12-18 00:13:51	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	support@ovh.net
2022-12-18 00:07:55	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.info
2022-12-18 00:07:17	Web Content Type	No	Web Spider	0	0	2	0	None	text/html; charset=utf-8
2022-12-18 00:21:02	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:09:43	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.3:80
2022-12-18 00:03:25	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	185.204.149.34.bc.googleusercontent.com
2022-12-18 00:02:48	IPv6 Address	No	Mnemonic PassiveDNS	13	0	1	0	None	2606:4700:3033::6815:1cf0
2022-12-18 00:05:42	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u' u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https:// u'binary-5', u'name': u'Drops cabinet archive files', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': Nor [targetUID: 00000000-00001336]'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u number 1 6 datablocks 0x1 compression"- Location: [%TEMP%\\CabA62.tmp]- [targetUID: 00000000-00001336]\n "jquery.min_3_.js" has type u'description': u'Pattern match: "https://lightsalmonstickyopenlook.eberech.repl.co/#kazuharu.fujimori%40aviationweek.com"\n Pattern {u'category': u'General', u'origin': u'Binary File', u'identifier': u'binary-11', u'name': u'The analysis extracted a file that was i
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:8880
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Dubtronicssid (Net ID: 00:01:24:F0:BB:A4)
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom2888 (Net ID: 00:01:38:85:BD:9E)
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet4862 (Net ID: 00:01:36:5B:48:60)
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SurfandSip (Net ID: 00:02:2D:03:87:91)
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	410HowardStudios (Net ID: 00:02:2D:00:25:63)
2022-12-18 00:24:21	Malicious Internet Name	Yes	MetaDefender	0	1	1	0	None	avira.com [misogyny.wtf]
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:08:31	Netblock Membership	No	RIPE	1	0	2	0	None	104.21.0.0/20
2022-12-18 00:21:58	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-C

2022-12-18 00:09:41	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	acnscrty.rcvry.workers.dev
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom1330 (Net ID: 00:01:38:92:E5:07)
2022-12-18 00:42:27	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.17] https://www.virustotal.com/en/ip-address/188.114.96.17/information/
2022-12-18 00:04:00	Physical Location	No	ipstack	0	0	1	0	None	Netherlands
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	validarpichincha.ecuadorr.repl.co
2022-12-18 00:25:33	Affiliate - Domain Name	No	DNS Resolver	0	0	3	0	None	securemail.pro
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	2WIRE522 (Net ID: 00:01:E6:93:CB:2D)
2022-12-18 00:06:06	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	ras.putain.fr
2022-12-18 00:02:45	Raw Data from RIRs	No	CertSpotter	1	0	1	0	None	[{u'pubkey_sha256': u'432961d5f32390043415639e54b3b0f65069a835707a1a3b93e937e211e4a25d', u'revoked': False, u'not_after': u'2022-12-1 u'81c617224289d583511688ac79d71981676bc4671feb811a1401928a0e1512e2', u'type': u'cert'}, u'dns_names': [u'*.misogyny.wtf', u'misogyny. u'MIIEfDCCA2SgAwIBAgIRAPTw+i+rKMN9DrACX58GsQwwDQYJKoZIhvcNAQELBQAwRjELMAkGA1UEBhMCVVMxIjAgBgNVBAoTGUdvb2dsZSBUcnVzdCBTZXJ2aWNlcyBMTEN u'sha256': u'966c4fc32756a6311ee52ac60b7e048a878007f9ee4f33ec45eb1f0391fa782f', u'type': u'precert'}, u'dns_names': [u'*.misogyny.wtf
2022-12-18 00:08:22	Netblock Membership	No	RIPE	105	0	2	0	None	188.114.96.0/24
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	YouTube User (Category: video) https://www.youtube.com/user/rasputain/about
2022-12-18 00:20:59	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:4700:3033::/48
2022-12-18 00:02:39	Internet Name	No	SpiderFoot UI	74	0	0	0	None	misogyny.wtf
2022-12-18 00:41:06	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.12] https://www.virustotal.com/en/ip-address/188.114.96.12/information/
2022-12-18 00:03:10	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:12:19	Phone Number	No	Phone Number Extractor	3	0	2	0	None	+19854014545
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:8443
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	0b21a147-2b2b-4fde-92c4-f3d74ff2845b.id.repl.co
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	House (Net ID: 00:02:2D:09:FC:0D)
2022-12-18 00:07:25	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 0f:0e:0e:28:f1:c6:cb:2f:ce:67:1d:a6:c8:b8:7a:b2 Signature Algorithm: ecdsa-with-SH Constraints: critical CA:FALSE CT Precertificate Poison: critical NULL Signature Algorithm: ecdsa-with-SHA256 30:45:02:20:6f:73:02:9b
2022-12-18 00:09:52	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.20:8080
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	ecuapichin--ecuapichin.repl.co
2022-12-18 00:12:16	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'NJ', u'country_tld': u'.us', u'ip': u'2606:4700:3032::ac43:be81', u'currency_name': u'Dollar', u'currency': u'USD'
2022-12-18 00:04:11	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3

2022-12-18 00:18:29	Internet Name	No	DNS Resolver	0	0	3	0	None	webmail.zerotwo-best-waifu.online
2022-12-18 00:26:57	Physical Location	No	MetaDefender	0	0	2	0	None	San Francisco, United States
2022-12-18 00:08:38	Open TCP Port	No	LeakIX	0	0	1	0	None	20.195.209.219:80
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:2082
2022-12-18 00:08:02	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.it
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Twist Studio (Net ID: 00:02:2D:07:96:23)
2022-12-18 00:09:48	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	autodiscover.theerathornnft.com
2022-12-18 00:08:56	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.0:80
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:80
2022-12-18 00:03:34	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3238.webapps.net
2022-12-18 00:24:06	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	z22lglbqy5igu1vav@registerprivateregistration.com
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	webpersonaspichincha1--webpichinch.repl.co
2022-12-18 00:16:49	Malicious IP Address	Yes	VirusTotal	0	1	1	0	None	VirusTotal [51.103.210.236] https://www.virustotal.com/en/ip-address/51.103.210.236/information/
2022-12-18 00:11:20	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 protoc
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:8880
2022-12-18 00:03:24	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	180.204.149.34.bc.googleusercontent.com
2022-12-18 00:03:06	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:43:16	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.20] https://www.virustotal.com/en/ip-address/188.114.96.20/information/
2022-12-18 00:08:45	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:05:13	Linked URL - Internal	No	Hybrid Analysis	0	0	2	0	None	http://misogyny.wtf/grab/UsRjS959Rqm4sPG4
2022-12-18 00:06:35	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.0:8080
2022-12-18 00:16:52	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Sectigo
2022-12-18 00:07:01	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:3b:c1:da:8c:2d:8d:3c:49:c8:fb:3d:44:b5:c2:87:b4:3a Signature Algorithm: ecdsa-w 43:a3:8d:79:ff:59:63:32:3d:8c:92:53:12:59:3a:b1:60:01: 58:91:c2:32:0d:d7:e9:cb:b7:70:ff:a3:a2:56:80:bd:93:6a: 54:5c:52:12:8b:bd:3b:4e
2022-12-18 00:09:32	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	distighrufcirawsdisr.tk

2022-12-18 00:21:20	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:20:49	Netblock Membership	No	Censys	0	0	1	0	None	51.103.0.0/16
2022-12-18 00:03:11	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.241
2022-12-18 00:02:55	IP Address	No	Mnemonic PassiveDNS	42	0	1	0	None	81.88.52.232
2022-12-18 00:02:56	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:50:42:ff:9a:7a:0a:ec:db:51:55:79:18:dd:8f:ed:52:b0 Signature Algorithm: sha256W Identifier: keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6 Authority Information Access: OCSP - URI:http://r3.o.le 93:a8:59:22:29:14:c8:c4:1c:b8:85:56:bd:a3:04:4a:a6:7c: 5a:3d:fc:76:55:4e:2b:05:58:c7:a6:e2:8c:25:27:c5:b2:a4: 7b:2e:58:c7:6b:bd:23:e1
2022-12-18 00:09:54	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:04:01	Physical Location	No	ipstack	0	0	2	0	None	Colombia
2022-12-18 00:12:41	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'172.67.169.215', u'currency_name': u'Dollar', u'currency': u'CAD', u'country
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	55 2nd PMO (Net ID: 00:01:21:10:85:60)
2022-12-18 00:08:25	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 41:cf:04:f8:c0:f2:7b:cd:70:73:3f:d3:40:5f:a0:ad Signature Algorithm: sha384WithRSA critical CA:FALSE X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication X509v3 Certificate Policies 6c:5d:20:75:e6:9b:b2:11:94:70:13:ea:ee:9f:8f:dc:aa:25: 3c:43:c3:ad:c3:40:19:ef:a8:fb:4b:4e:73:4c:9a:7b:c5:a5: 09:33:df:42:95:71:29:98
2022-12-18 00:21:17	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-(
2022-12-18 00:08:36	Physical Location	No	LeakIX	0	0	1	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:14:31	Physical Location	No	ipstack	0	0	2	0	None	Colombia
2022-12-18 00:09:41	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	acversing.cf
2022-12-18 00:37:18	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.xen.prgmr.com
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:2087
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:08:41	Open TCP Port	No	LeakIX	0	0	1	0	None	40.113.112.131:80
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	RyanLG (Net ID: 00:01:36:4F:9A:F0)
2022-12-18 00:39:59	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.8] https://www.virustotal.com/en/ip-address/188.114.96.8/information/
2022-12-18 00:12:58	Malicious IP on Same Subnet	Yes	blocklist.de	0	0	2	0	None	blocklist.de List [4.224.0.0/12] http://lists.blocklist.de/lists/all.txt
2022-12-18 00:06:07	Internet Name	No	DNS Resolver	0	0	2	0	None	misogyny.wtf
2022-12-18 00:02:39	IP Address	No	SpiderFoot UI	14	0	0	0	None	137.117.157.128
2022-12-18 00:09:37	Physical Location	No	LeakIX	0	0	2	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:38:37	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.3] https://www.virustotal.com/en/ip-address/188.114.96.3/information/

2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:13:44	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	private@register.it
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	logitec-a53131 (Net ID: 00:01:8E:A5:31:30)
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:8880
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpaceStation (Net ID: 00:02:2D:01:CF:F8)
2022-12-18 00:06:40	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.1:8080
2022-12-18 00:11:55	Physical Location	No	ipapi.co	1	0	1	0	None	Campinas, Sao Paulo, SP, Brazil, BR
2022-12-18 00:06:51	Malicious IP Address	Yes	Internet Storm Center	0	1	1	0	None	Internet Storm Center [20.195.209.219] https://isc.sans.edu/api/ip/20.195.209.219
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2083
2022-12-18 00:03:15	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-101.w90-116.abo.wanadoo.fr
2022-12-18 00:12:08	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'172.67.147.230', u'currency_name': u'Dollar', u'currency': u'CAD', u'country
2022-12-18 00:23:11	Raw Data from RIRs	No	CRXcavator	0	0	1	0	None	[{"platform": "Chrome", "version": "4.0.2", "data": {"risk": {"total": 7, "webstore": {"website": 1, "privacy_policy": 1, "users": 1,
2022-12-18 00:12:33	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'cour
2022-12-18 00:06:02	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'compromised_ "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "Local\\URLBLOCK_FILEMAPSWITCH_MUTEX_3076"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\!BrowserEmul (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: portalpersonasparatodo.tdavivienda.repl.co\r fonts.gstatic.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GET /s/ibmplexsans/v14/zYXgKVElMYYaJe8bpLHnCwDKhdH u'binary-37', u'name': u'Drops files inside appdata directory', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'cape 08002704E6C2_.dat" has type "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "zYXgKVElMYYaJe8bpLHnC 00003076]'}, {u'category': u'Network Related', u'origin': u'String', u'identifier': u'string-102', u'name': u'Decrypted SSL network t
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	fse2 (Net ID: 00:01:38:A0:A1:09)
2022-12-18 00:09:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.0:8080
2022-12-18 00:26:50	Physical Location	No	MetaDefender	0	0	2	0	None	Firenze, Italy
2022-12-18 00:03:10	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	1	0	None	webapps.net
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2087
2022-12-18 00:32:23	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.world
2022-12-18 00:22:07	Raw Data from RIRs	No	Censys	4	0	2	0	None	{"last_updated_at": "2022-12-17T20:42:12.354Z", "ip": "34.149.204.188", "location_updated_at": "2022-12-14T04:27:41.707226Z", "autono 22T12:40:13.151572843Z"}, "tilamour.mvp.ng": {"record_type": "CNAME", "resolved_at": "2022-12-11T16:31:05.536832979Z"}, "yolandasinti 11T12:41:16.752277025Z"}, "hendrapramana.repl.co": {"record_type": "A", "resolved_at": "2022-12-13T12:38:53.367761692Z"}, "rizki-nurr "diaznoviyanto.repl.co": {"record_type": "A", "resolved_at": "2022-12-06T12:47:45.883833821Z"}, "jacobshaw2.repl.co": {"record_type": {"record_type": "A", "resolved_at": "2022-12-06T12:48:00.114118443Z"}, "andimotovlog.repl.co": {"record_type": "A", "resolved_at": "2 "2022-12-02T12:43:56.720634312Z"}, "gabo-contra-los.repl.co": {"record_type": "A", "resolved_at": "2022-12-03T13:03:11.081447886Z"}, "mbn92.repl.co": {"record_type": "A", "resolved_at": "2022-11-23T13:59:19.586349175Z"}, "firmannurhakim.repl.co": {"record_type": "A"
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-	Country	No	Country Name	0	0	7	0	None	

18 00:27:49			Extractor						Italy
2022-12-18 00:12:24	Physical Location	No	ipapi.co	0	0	2	0	None	Campinas, Sao Paulo, SP, Brazil, BR
2022-12-18 00:59:52	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	41c364fb5187478eb52fa456269b7aef.protect@withheldforprivacy.com
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:8443
2022-12-18 00:05:13	Linked URL - Internal	No	Hybrid Analysis	0	0	2	0	None	http://misogyny.wtf:8080/
2022-12-18 00:30:56	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namecheap.com
2022-12-18 00:05:26	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 20, u'threat_score': 100, u'compromise "Local\\SM0:5864:120:WilError_01"\n "Local\\SM0:5864:304:WilStaging_02"\n "Local\\InternetShortcutMutex"\n "Local\\SM0:5660:304:WilSt 42d6-4da2-b87c-cac737035349.tmp" has type "ASCII text with very long lines with no line terminators"- [targetUID: N/A]\n "41962708-5f "03cc95bd-1754-476e-b462-79536e7625ef.tmp" has type "UTF-8 Unicode text with very long lines with no line terminators"- Location: [%U "ASCII text with very long lines with no line terminators"- Location: [%TEMP%\\5660_724844775\\runtime.bundle.js]- [targetUID: 000000 [%TEMP%\\5660_1719137669\\edge_tracking_page_validator.js]- [targetUID: 00000000-00005660]\n Dropped file: "product_page.js" - Locati "bnpl_driver.js" - Location: [%TEMP%\\5660_724844775\\bnpl_driver.js]- [targetUID: 00000000-00005660]\n Dropped file: "edge_confirmat
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:12:14	Physical Location	No	ipapi.co	0	0	2	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:2083
2022-12-18 00:09:29	Open TCP Port	No	LeakIX	0	0	2	0	None	81.88.52.232:443
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ProCare-Guest (Net ID: 00:01:21:1C:30:F0)
2022-12-18 00:16:53	Company Name	No	Company Name Extractor	0	0	3	0	None	Cloudflare\, Inc.
2022-12-18 00:21:54	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:18:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.4:80
2022-12-18 00:06:31	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.147.230:80
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	bancosneomc.itaumcneonm.repl.co
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	RyanLG (Net ID: 00:01:36:4F:9A:F0)
2022-12-18 00:17:00	HTTP Headers	No	Web Spider	0	0	4	0	None	{"content-length": "39680", "accept-ranges": "bytes", "last-modified": "Wed, 15 Dec 2021 09:50:30 GMT", "connection": "keep-alive", "
2022-12-18 00:09:39	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	7626679.com
2022-12-18 00:21:51	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-(
2022-12-18 00:04:11	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-Sh X509v3 Basic Constraints: critical CA:FALSE CT Precertificate SCTs: Signed Certificate Timestamp: Version : v1 (0x0) Log ID : E8:3E:D

									30:45:02:21:00:d8:35:e0:5c:fe:c9:39:b4:06:5a:95:36:1c: 73:f4:85:1c:c5:6e:6b:ef:48:76:d6:7f:a3:fe:55:ed:82:7f: c5:02:20:7f:8c:86:3a:6
2022-12-18 00:11:30	Physical Address	No	GLEIF	0	0	3	0	None	C/O CORPORATION SERVICE COMPANY, 251 LITTLE FALLS DRIVE, WILMINGTON, US-DE, US, 19808
2022-12-18 00:09:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.0:2053
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:2087
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:2082
2022-12-18 00:12:47	Physical Location	No	ipapi.co	0	0	2	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2022-12-18 00:16:57	Linked URL - Internal	No	Web Spider	4	0	3	0	None	http://webmail.zerotwo-best-waifu.online/js/vendor/jquery-3.5.0.min.js
2022-12-18 00:20:19	Netblock Membership	No	RIPE	0	0	3	0	None	81.88.48.0/20
2022-12-18 00:06:53	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.fr
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	pichinchaonline.ecuados.repl.co
2022-12-18 00:31:03	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.club
2022-12-18 00:06:37	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.1:80
2022-12-18 00:06:25	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: f4:f0:fa:2f:ab:28:c3:7d:0e:b0:02:5f:9f:06:b1:0c Signature Algorithm: sha256WithRSA keyid:D5:FC:9E:0D:DF:1E:CA:DD:08:97:97:6E:2B:C5:5F:C5:2B:F5:EC:B8 Authority Information Access: OCSP - URI:http://ocsp.pki.goog/s/gts
2022-12-18 00:15:47	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	keep-alive: timeout=5
2022-12-18 00:09:35	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	imdmorat.ga
2022-12-18 00:31:52	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@godaddy.com
2022-12-18 00:10:05	Web Server	No	URLScan.io	0	1	1	0	None	Apache
2022-12-18 00:25:33	Affiliate - Domain Name	No	DNS Resolver	0	0	3	0	None	setupdns.net
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:12:42	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'104.21.27.242', u'currency_name': u'Dollar', u'currency': u'CAD', u'country_
2022-12-18 00:03:10	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.237
2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:17:54	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [188.114.96.0] https://www.virustotal.com/en/ip-address/188.114.96.0/information/
2022-12-18 00:08:39	Netblock Membership	No	RIPE	0	0	2	0	None	188.114.97.0/24
2022-12-18 00:21:51	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-

2022-12-18 00:04:11	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	188.114.96.1:443
2022-12-18 00:03:06	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.184
2022-12-18 00:21:44	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:08:32	Raw Data from RIRs	No	LeakIX	0	0	1	0	None	{u'Services': None, u'Leaks': None}
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpeedStream (Net ID: 00:01:24:F0:B4:05)
2022-12-18 00:21:06	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	043320 (Net ID: 00:02:2D:04:33:20)
2022-12-18 00:03:12	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SurfandSip (Net ID: 00:02:2D:03:7C:7A)
2022-12-18 00:09:12	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.1:443
2022-12-18 00:23:12	Raw Data from RIRs	No	CRXcavator	1	0	1	0	None	[{"platform": "Chrome", "version": "0.37", "data": {"extcalls": ["https://home.newtabgallery.com/", "https://newtabgallery.com/welcom GO HD Wallpapers New Tab"}, "fpmmkkfgclmhcolgmcpjdkfpehgbedim": {"rating": 5, "users": 1000, "platform": "", "short_description": "Re "icon": "https://lh3.googleusercontent.com/jluPSHf4IjMjgqd0rNVMuTfq1f4786G1iiu5koA7B4jo2el8s3MKIzpNpo-cmXd9ET9SnGZW=w128-h128-e365", "dephgmdllolfchlbencncbldjdnkdbok": {"rating": 3.1818182, "users": 735, "platform": "", "short_description": "Minecraft Classic wallp new tab and was made for all fans of Cat.", "icon": "https://lh3.googleusercontent.com/I_EAJDo-eiJhq-8CLSqi3_SGwaA57lw48w0g_SRK3a7BS3 OLn6ENkBDJvHobXQLQG0hDXCyxQVHIZ8LffkazMFHdpZJJqp4XSbooLtSKGmgvmebncQs=w128-h128-e365-rj-sc0x00ffffff", "rating_users": 36, "name": "P "manifest": {"update_url": "https://clients2.google.com/service/update2/crx", "description": "Includes HD wallpaper images of the gam
2022-12-18 00:06:06	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	hook.plague.fun
2022-12-18 00:14:32	Country	No	Country Name Extractor	0	0	3	0	None	Italy
2022-12-18 00:36:48	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.ddns.net
2022-12-18 00:12:18	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'NJ', u'country_tld': u'.us', u'ip': u'2606:4700:3037::6815:13f3', u'currency_name': u'Dollar', u'currency': u'USD'
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet2EE2 (Net ID: 00:01:36:5B:2E:E0)
2022-12-18 00:04:12	Raw Data from RIRs	No	Hybrid Analysis	0	0	1	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObjects\\IsoScope_ca8_IESQMMUTEX_0_519"\r [targetUID: 00000000-00003240]\n Dropped file: "3LR45Z23.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\3LR45Z23.txt]- [ta "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "3LR45Z23.txt" has type "ASCII text"- Location: [% u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 5, u'threat_level': 0, u'type': 7, u'descr u'entrypoint': None, u'mitre_attcks': [{u'parent': None, u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1105', u'suspicious u'av_detect': 5, u'machine_learning_models': [], u'total_signatures': 10, u'image_base': None, u'error_origin': None, u'ssdeep': u'Ur
2022-12-18 00:05:47	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': u'Windows Gui', u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 1, u'threat_score': 100, u'c "\\Sessions\\1\\BaseNamedObjects\\Local\\ZonesLockedCacheCounterMutex"\n "\\Sessions\\1\\BaseNamedObjects\\RasPbFile"\n "Local\\Zones u'"Sims2RPCSettings.exe" (Path: "HKLM\\SOFTWARE\\MICROSOFT\\SYSTEMCERTIFICATES\\AUTHROOT\\AUTOUPDATE"; Key: "DISALLOWEDCERTSYNCDELTAT "HKLM\\SOFTWARE\\MICROSOFT\\SYSTEMCERTIFICATES\\DISALLOWED\\CERTIFICATES\\61793FCBFA4F9008309BBA5FF12D2CB29CD4151A"; Key: "BLOB")'}, u'threat_level': 0, u'type': 7, u'description': u'"ocsp.sectigo.com"'}, {u'category': u'General', u'origin': u'Binary File', u'identi "34.149.204.188:443"'}, {u'category': u'General', u'origin': u'Registry Access', u'identifier': u'registry-18', u'name': u'Accesses S "Sims2RPCSettings.exe" (Path: "HKLM\\SOFTWARE\\POLICIES\\MICROSOFT\\SYSTEMCERTIFICATES\\TRUSTEDPEOPLE\\CTLS"; Key: "")\n "Sims2RPCSet
2022-12-18 00:06:31	Company Name	No	Company Name Extractor	0	0	2	0	None	ENOM, INC.
2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://plague.fun/
2022-12-	Raw Data	No	Hybrid Analysis	0	0	2	0	None	

18 00:06:59	from RIRs								[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'compromised_ 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, "\\Sessions\\1\\BaseNamedObjects\\IsoScope_140_IESQMMUTEX_0_303"\n "\\Sessions\\1\\BaseNamedObjects\\IsoScope_140_IESQMMUTEX_0_331"\n [targetUID: 00000000-00002856]\n Dropped file: "8QR1102B.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\8QR1102B.txt]- [ta "CAF4703619713E3F18D8A9D5D88D6288_A7725538C46DE2D0088EE44974E2CEBA" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptr [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776]- [targ 1em;\n }\n\n .footer-item {\n margin: 1em;\n display: flex;\n justify-content: center;\n align-items: center;\n }\n\n .link-icon {\n
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	sniuopgfsdfsdfahgf.snigup.repl.co
2022-12-18 00:08:30	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.52.223:443
2022-12-18 00:22:04	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T01:52:06.746Z", "ip": "90.116.166.104", "location_updated_at": "2022-12-13T03:22:34.443512Z", "autono ["chunked"], "Content_Type": ["text/html"]}, "html_tags": ["<title>Not Found</title>"], "status_reason": "Not Found"}, "supports_http
2022-12-18 00:21:23	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:14:31	Physical Location	No	ipstack	0	0	2	0	None	Colombia
2022-12-18 00:29:09	Similar Domain - Whois	No	Whois	0	0	2	0	None	Domain name: plague.co.uk Registrant: TwentyTwenty Media Limited Registrant type: UK Limited Company, (Company number: 3730401) Regis
2022-12-18 00:19:10	Hosting Provider	No	Hosting Provider Identifier	0	0	3	0	None	register.it: http://we.register.it/
2022-12-18 00:08:38	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2022-12-18 00:03:06	Internet Name	No	DNS Resolver	0	0	2	0	None	misogyny.wtf
2022-12-18 00:06:51	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.137.37:80
2022-12-18 00:04:10	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
2022-12-18 00:13:48	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	domregteam3@eurodns.com
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:2096
2022-12-18 00:08:42	Malicious IP on Same Subnet	Yes	CleanTalk Spam List	0	0	3	0	None	CleanTalk Spam List [81.88.48.0/20] https://iplists.firehol.org/files/cleantalk_7d.ipset
2022-12-18 00:03:05	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.111
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	serviciosbancpichinchacomecu--ecuador0.repl.co
2022-12-18 00:21:06	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T23:35:44.052Z", "ip": "172.67.147.230", "location_updated_at": "2022-12-10T07:08:41.264508Z", "autono {"record_type": "A", "resolved_at": "2022-12-02T13:27:01.611968342Z"}, "aninfio.ml": {"record_type": "A", "resolved_at": "2022-12-0 cards.zone": {"record_type": "A", "resolved_at": "2022-12-10T19:10:07.986427709Z"}, "bongocat.click": {"record_type": "A", "resolved_ {"record_type": "A", "resolved_at": "2022-10-29T18:59:35.908349611Z"}, "opantupa.tk": {"record_type": "A", "resolved_at": "2022-11-25 "johnparkeraesthetics.com": {"record_type": "A", "resolved_at": "2022-12-14T13:44:36.052499508Z"}, "davisresearch.org": {"record_type {"record_type": "A", "resolved_at": "2022-11-26T13:38:16.539310269Z"}, "www.hookup.directory": {"record_type": "A", "resolved_at": "2 12-13T13:44:08.455137791Z"}, "mail.algoritmoexpert.com.br": {"record_type": "A", "resolved_at": "2022-11-18T12:15:11.721015572Z"}, "p
2022-12-18 00:11:01	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: y.wtf Registry Domain ID: 2621e215e11c46369a501d648eada907-DONUTS Registrar WHOIS Server: whois.1api.net Registrar URL: Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Re and under no circumstances may this data be used to: a) allow, enable, or otherwise support the transmission by e-mail, telephone, or provided, upon request, where it can be reasonably confirmed that the requester holds a specific legitimate interest and a proper leg FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Post unsolicited, commercial advertising or solicitations via E-mail ; (spam); or ; 2) enable high volume, automated, electronic processes
2022-12-18 00:40:47	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.11] https://www.virustotal.com/en/ip-address/188.114.96.11/information/
2022-12-18 00:04:38	Malicious IP Address	Yes	Maltiverse	0	1	2	0	None	Maltiverse [188.114.96.0]
2022-12-18 00:04:01	Physical Location	No	ipstack	0	0	2	0	None	Brazil
2022-12-	Similar	Yes	TLD Searcher	1	0	1	0	None	

18 00:05:54	Domain								plague.ca
2022-12-18 00:18:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.1:80
2022-12-18 00:16:57	Linked URL - Internal	No	Web Spider	4	0	3	0	None	http://webmail.zerotwo-best-waifu.online/css/qbert_theme/template/master.css?v=1.7.0
2022-12-18 00:18:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.3:80
2022-12-18 00:16:58	HTTP Headers	No	Web Spider	0	0	4	0	None	{"content-length": "89493", "accept-ranges": "bytes", "last-modified": "Wed, 15 Dec 2021 09:50:30 GMT", "connection": "keep-alive", "
2022-12-18 00:26:44	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [34.149.204.188]
2022-12-18 00:16:54	Malicious Internet Name	Yes	CloudFlare Malware DNS	0	1	2	0	None	Blocked by CloudFlare DNS [autoconfig.zerotwo-best-waifu.online]
2022-12-18 00:16:59	HTTP Headers	No	Web Spider	0	0	4	0	None	{"content-length": "1305", "accept-ranges": "bytes", "last-modified": "Fri, 12 Feb 2021 14:43:40 GMT", "connection": "keep-alive", "e
2022-12-18 00:33:43	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.188:8443
2022-12-18 00:27:43	Similar Domain - Whois	No	Whois	0	0	2	0	None	% The WHOIS service offered by ROTLD and the access to the records in the ROTLD WHOIS database % are provided for information purpose the ROTLD website www.rotld.ro Domain Name: plague.ro Registered On: 2019-08-19 Expires On: 2023-08-18 Registrar: ICI - Registrar Ref
2022-12-18 00:11:29	Legal Entity Identifier	No	GLEIF	0	0	3	0	None	549300F1AETTPWFIQC02
2022-12-18 00:06:15	HTTP Headers	No	Web Spider	1	0	1	0	None	{"date": "Sun, 18 Dec 2022 00:06:15 GMT", "content-length": "29", "content-type": "text/html; charset=utf-8", "connection": "close",
2022-12-18 00:03:07	Internet Name	No	DNS Resolver	0	0	2	0	None	rasputain.fr
2022-12-18 00:06:21	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.de
2022-12-18 00:16:57	Web Content Type	No	Web Spider	0	0	2	0	None	text/html; charset=UTF-8
2022-12-18 00:13:24	Internet Name	No	DNS Brute-forcer	7	1	1	0	None	ftp.zerotwo-best-waifu.online
2022-12-18 00:16:54	Malicious Internet Name	Yes	CloudFlare Malware DNS	0	1	2	0	None	Blocked by CloudFlare DNS [mail.zerotwo-best-waifu.online]
2022-12-18 00:03:01	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.94
2022-12-18 00:09:18	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'https', u'event_type': u'service', u'ip': u'172.67.137.37', u'vendor': u'', u'port': u'443', u'transpo u'detected': False, u'version': u'TLSv1.3'}, u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'banner': u'', u'fingerprint': u''}, u'software': {u'modules': None, u'version': u'', u'os': u'', u'name': u'cloudflare', u'fingerprint': u''}}, u'event_fingerprint': u'6 Thu, 03 Nov 2022 16:49:11 GMT\r\nContent-Length: 0\r\nConnection: close\r\nCache-Control: no-store, no-cache\r\nCF-Cache-Status: DYNA site', u'url': u'', u'header': {u'server': u'cloudflare'}, u'length': 0, u'favicon_hash': u'', u'root': u''}, u'tags': [], u'ssl': {u 02T07:40:10.302455138Z'}, {u'protocol': u'https', u'event_type': u'service', u'ip': u'172.67.137.37', u'vendor': u'', u'port': u'8443 u'not_before': u'2022-05-21T00:00:00Z'}, u'enabled': True, u'detected': False, u'version': u'TLSv1.3'}, u'mac': u'', u'ssh': {u'motd'
2022-12-18 00:21:47	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3032::ac43:8925:443
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:8443
2022-12-18 00:02:44	Internet Name - Unresolved	No	grep.app	0	0	1	0	None	atlas.plague.fun
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	55 2nd PMO (Net ID: 00:01:21:10:61:00)
2022-12-18 00:21:06	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-O
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2083
2022-12-	Linked URL	No	Web Spider	4	0	3	0	None	http://webmail.zerotwo-best-waifu.online/css/qbert_theme/template/custom.css?v=1.7.0

18 00:16:57	- Internal								
2022-12-18 00:09:23	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	zerotwo-best-wa.ifu.online
2022-12-18 00:11:20	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 5.0 Description: The DES and Triple DES ciphers, as used in the T
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:24:59	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.192
2022-12-18 00:07:01	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise server', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'thre files inside appdata directory', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, "6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptr [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\265C0DEB29181DD1891051371C5F863A_14F2E352CCFE495001982FFDAAC3BE84]- [targe "~DFFB264EBDB98B9664.TMP" has type "data"- Location: [%TEMP%\\~DFFB264EBDB98B9664.TMP]- [targetUID: 00000000-00004016]'}, {u'category font-family: "IBM Plex Sans", "sans";\n padding: 1em;\n margin: 1em;\n }\n\n .footer-item {\n margin: 1em;\n display: flex;\n justify
2022-12-18 00:32:27	Malicious Affiliate IP Address	Yes	VirusTotal	0	1	3	0	None	VirusTotal [81.88.52.223] https://www.virustotal.com/en/ip-address/81.88.52.223/information/
2022-12-18 00:04:28	DNS TXT Record	No	DNS Raw Records	0	0	1	0	None	v=spf1 include:spf.efwd.registrar-servers.com ~all
2022-12-18 00:23:08	Raw Data from RIRs	No	CRXcavator	1	0	1	0	None	[{"platform": "Chrome", "version": "12.0.7", "data": {"entrypoints": {"window.addEventListener": {"/tmp/bifklmkjcgfnoholohpcenkjpdmk "https://api.lovelytab.com/api/index.php?api=lovelytab_api_v1&module=siteplug&id=", "http://lovelytab.com/extensions/admarketplace.ph wallpaper backgrounds. Themes designed for black fans.", "icon": "https://lh3.googleusercontent.com/PgWt9mKR5tShJw8dWkpcEKbp6n6XvePlb "lgglnjfaglblnglkdmmdhmjcpplmjdfj": {"rating": 4, "users": 99, "platform": "", "short_description": "Includes HD wallpaper images of "https://lh3.googleusercontent.com/w5KW2IQeXksHUMjE5hwX8fBRCs2w3fPyESP4LXmUlZyDAhLPhjt5NBAiTfes8PZLoBPli1Ox=w128-h128-e365-rj-sc0x00f Thrones New Tab Extension brings a new look to your Chrome browser.", "icon": "https://lh3.googleusercontent.com/I26WkaS9ESAzuYaWq2Gh "anbnnbjeebeigjndlammohpajdojepdj": {"rating": 4.5, "users": 2000, "platform": "", "short_description": "Sword Art Online SAO New Tab
2022-12-18 00:04:28	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	eforward3.registrar-servers.com
2022-12-18 00:02:47	Raw Data from RIRs	No	grep.app	0	0	1	0	None	{u'repo': {u'raw': u'aceeontop/wasp-stealer'}, u'total_matches': {u'raw': u'1'}, u'content': {u'snippet': u'<table class="highlight-t </tr></table>'}, u'branch': {u'raw': u'main'}, u'path': {u'raw': u'OldWaspsVersions/wasp-1.1.1.py'}, u'id': {u'raw': u'g/aceeontop/wa
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:80
2022-12-18 00:14:47	Internet Name - Unresolved	No	VirusTotal	0	0	1	0	None	stream.plague.fun
2022-12-18 00:23:30	Affiliate - Internet Name	No	DNS Raw Records	1	0	2	0	None	tb-fr.securemail.pro
2022-12-18 00:31:04	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: plague.club Registry Domain ID: D1C093C1CE747444390668EB5348FF659-NSR Registrar WHOIS Server: whois.namecheap.com Regist REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR P information in relation to domain names that we store in our database. Use of the Service is subject to our policies, in particular y 15T06:18:37.01Z Creation Date: 2020-04-14T23:55:11.78Z Registrar Registration Expiration Date: 2023-04-14T23:55:11.78Z Registrar: NAM Tech Fax Ext: Tech Email: 116cc296f60d4885bbe79883230f5566.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Nam
2022-12-18 00:16:27	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	188.114.96.9:443
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:18:25	IP Address	No	DNS Resolver	0	0	2	0	None	81.88.52.232
2022-12-18 00:03:05	Domain Name	No	DNS Resolver	0	0	1	0	None	zerotwo-best-waifu.online
2022-12-18 00:20:59	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:12:39	Physical Location	No	ipapi.co	1	0	2	0	None	Bergamo, Lombardy, 25, Italy, IT
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:2096
2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/

2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	S-lan (Net ID: 00:01:24:F1:91:41)
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:01:E6:93:CF:EC)
2022-12-18 00:09:39	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.9:80
2022-12-18 00:32:18	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@west.cn
2022-12-18 00:21:30	Netblock Membership	No	Censys	0	0	2	0	None	172.67.176.0/20
2022-12-18 00:04:11	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
2022-12-18 00:11:48	Malicious Affiliate IP Address	Yes	Greensnow	0	1	3	0	None	greensnow.co [81.88.52.223] https://blocklist.greensnow.co/greensnow.txt
2022-12-18 00:05:30	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'34.149.204.188'}], u'result': [{u'environment_id': 160, u'job_id': u'63 u'environment_description': u'Windows 7 32 bit', u'threat_score': 15, u'verdict': u'malicious', u'submit_name': u'sample.url', u'sha2 {u'environment_id': 120, u'job_id': u'6396afc3f29bea42ac015f44', u'analysis_start_time': u'2022-12-12 04:48:46', u'vx_family': u'Phis threat', u'submit_name': u'sample.url', u'sha256': u'ccb4b08d86a8b7e872a8f20d9687306e4ec5f0e0c2229710e0c0312ae34bd11b', u'type': None u'analysis_start_time': u'2022-11-22 02:57:04', u'vx_family': u'Phishing site', u'av_detect': u'5', u'environment_description': u'Wir u'84a9b0dc38c6b99cb034101ea52a1f71e691e5687fa133ba4146832b796a7fd8', u'type': None, u'type_short': u'url', u'size': 75}, {u'environme u'0', u'environment_description': u'Windows 10 64 bit', u'threat_score': 12, u'verdict': u'suspicious', u'submit_name': u'sample.url'
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	usernamervali.bancoesername.repl.co
2022-12-18 00:04:28	Affiliate - Internet Name - Unresolved	No	DNS Raw Records	0	0	1	0	None	spf.efwd.registrar-servers.com
2022-12-18 00:03:36	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	stream.plague.fun
2022-12-18 00:05:58	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	www.plague.fun
2022-12-18 00:21:27	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date"
2022-12-18 01:00:21	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.87] https://www.virustotal.com/en/ip-address/188.114.96.87/information/
2022-12-18 00:12:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 6, u'search_terms': [{u'id': u'host', u'value': u'188.114.96.3'}], u'result': [{u'environment_id': 160, u'job_id': u'63922 u'environment_description': u'Windows 7 64 bit', u'threat_score': 12, u'verdict': u'suspicious', u'submit_name': u'sample.url', u'sha
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SurfandSip Wavelan (Net ID: 00:02:2D:01:79:94)
2022-12-18 00:32:21	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.148:443
2022-12-18 00:09:50	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 protoc
2022-12-18 00:07:06	Web Content Type	No	Web Spider	0	0	2	0	None	text/html; charset=UTF-8
2022-12-18 00:18:26	IP Address	No	DNS Resolver	19	0	2	0	None	81.88.48.101
2022-12-18 00:02:50	IPv6 Address	No	Mnemonic PassiveDNS	13	0	1	0	None	2a06:98c1:3121::1
2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://obf.plague.fun
2022-12-18 00:03:04	IP Address	No	DNS Resolver	0	0	1	0	None	20.226.83.185
2022-12-	HTTP	No	Censys	0	0	2	0	None	

18 00:21:02	Headers								{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:08:30	IP Address	No	LeakIX	24	0	1	0	None	188.114.97.9
2022-12-18 00:23:00	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	3	0	None	amen.fr
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet24CE (Net ID: 00:01:36:59:24:CC)
2022-12-18 00:20:59	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3033::6815:1cf0:443
2022-12-18 00:03:08	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	www.plague.fun
2022-12-18 00:09:34	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	eventmobilelegend22.cf
2022-12-18 00:18:04	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.0:8080
2022-12-18 00:21:06	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-(
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	role.davimoore.repl.co
2022-12-18 00:03:29	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3224.webapps.net
2022-12-18 00:22:04	Open TCP Port	No	Censys	0	0	2	0	None	90.116.166.104:50997
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pancakes (Net ID: 00:00:48:67:6D:D1)
2022-12-18 00:19:07	Country	No	Country Name Extractor	0	0	4	0	None	Italy
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:2083
2022-12-18 00:12:19	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+3544212434
2022-12-18 00:12:00	Raw Data from RIRs	No	ipapi.co	0	0	1	0	None	{u'region_code': u'ZH', u'country_tld': u'.ch', u'ip': u'51.103.210.236', u'currency_name': u'Franc', u'currency': u'CHF', u'country_
2022-12-18 00:16:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:09:39	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	66793246.com
2022-12-18 00:21:09	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-(
2022-12-18 00:03:25	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	www.plague.fun

2022-12-18 00:03:22	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	www.plague.fun
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:2082
2022-12-18 00:20:19	BGP AS Membership	No	RIPE	0	0	4	0	None	12363
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	7717 7361 (Net ID: 00:00:C5:FC:FE:34)
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:21:20	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conn
2022-12-18 00:09:33	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.27.242:443
2022-12-18 00:08:40	BGP AS Membership	No	RIPE	0	0	3	0	None	3215
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	dvdbeyond (Net ID: 00:01:24:F2:B3:12)
2022-12-18 00:08:16	Netblock Membership	No	RIPE	0	0	1	0	None	20.192.0.0/10
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:26:18	Physical Location	No	MetaDefender	0	0	2	0	None	Campinas, Brazil
2022-12-18 00:21:13	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:13:36	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@cloudflare.com
2022-12-18 00:11:10	Similar Domain - Whois	No	Whois	2	0	2	0	None	%% %% This is the AFNIC Whois server. %% %% complete date format: YYYY-MM-DDThh:mm:ssZ %% %% Rights restricted by copyright. %% See h eppstatus: active eligstatus: not identified reachstatus: not identified source: FRNIC nic-hdl: ANO00-FRNIC type: PERSON contact: Anc
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:443
2022-12-18 00:22:07	BGP AS Membership	No	Censys	0	0	2	0	None	15169
2022-12-18 00:06:37	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.1:8080
2022-12-18 00:03:08	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:54:d1:cf:73:f4:06:da:67:36:31:1b:04:19:11:b7:02:21 Signature Algorithm: ecdsa-w 3d:be:52:da:80:dc:a2:9d:50:94:22:a3:e3:f8:29:ec:b0:25: 63:d5:de:74:71:c9:c1:71:0e:8c:0d:1d:3a:6e:b9:c4:0a:9e: 23:22:2b:9c:de:86:d5:f4
2022-12-18 00:21:47	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:13:15	Internet Name	No	DNS Brute-forcer	7	1	1	0	None	autoconfig.zerotwo-best-waifu.online
2022-12-18 00:04:00	Physical Location	No	ipstack	0	0	1	0	None	Switzerland
2022-12-18 00:16:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	sni.cloudflaressl.com
2022-12-18 00:09:42	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.15:8443
2022-12-18 00:13:47	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	info@nettalk.nl
2022-12-18 00:18:35	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.15:443

2022-12-18 00:26:11	Physical Location	No	MetaDefender	0	0	2	0	None	Campinas, Brazil
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:2087
2022-12-18 00:08:42	Open TCP Port	No	LeakIX	0	0	1	0	None	51.103.210.236:80
2022-12-18 00:12:31	URL (Purely Static)	No	Page Information	0	0	3	0	None	http://misogyny.wtf/grab/UsRjS959Rqm4sPG4
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:37	Open TCP Port	No	Censys	0	1	2	0	None	20.226.83.185:3389
2022-12-18 00:21:02	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conn
2022-12-18 00:09:39	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	733rr.com
2022-12-18 00:04:01	Physical Location	No	ipstack	0	0	2	0	None	Colombia
2022-12-18 00:14:36	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:24:06	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	abuse@register.it
2022-12-18 00:07:17	Web Content	No	Web Spider	2	0	2	0	None	<!doctype html> <html lang=en> <title>403 Forbidden</title> <h1>Forbidden</h1> <p>You don't have the permission to access the rec
2022-12-18 00:08:41	Internet Name	No	DNS Resolver	0	0	2	0	None	misogyny.wtf
2022-12-18 00:04:36	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:43:e4:fc:51:db:21:42:a6:26:a1:af:57:d7:7c:1f:09:d4 Signature Algorithm: ecdsa-w 31:00:eb:3f:e4:2f:4c:57:97:77:3f:dd:d6:ab:3b:c1:ef:85: 47:a0:a6:99:62:c9:31:7b:f5:c6:c6:03:dc:f8:80:fc:da:81: 41:e5:0b:5f:ff:ad:15:77
2022-12-18 00:21:34	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-O
2022-12-18 00:03:12	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:22:07	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Connection": "DISPLAY_UTF8"}, "Connection": ["close"]}
2022-12-18 00:14:56	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:09:49	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	banadislifo.tk
2022-12-18 00:03:24	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	178.204.149.34.bc.googleusercontent.com
2022-12-18 00:08:41	Internet Name	No	DNS Resolver	0	0	2	0	None	misogyny.wtf
2022-12-18 00:21:30	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-O
2022-12-18 00:08:45	Internet Name	No	DNS Resolver	0	0	2	0	None	zerotwo-best-waifu.online
2022-12-18 00:10:03	Internet Name - Unresolved	No	URLScan.io	0	0	1	0	None	wasp.plague.fun
2022-12-18 00:21:17	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:
2022-12-18 00:22:14	Netblock Membership	No	Censys	0	0	2	0	None	172.67.160.0/20

2022-12-18 00:09:12	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.1:8443
2022-12-18 00:09:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.9:80
2022-12-18 00:18:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.12:8443
2022-12-18 00:21:58	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:25:19	Physical Location	No	MetaDefender	0	0	2	0	None	San Jose, United States
2022-12-18 00:10:04	Raw Data from RIRs	No	URLScan.io	0	0	1	0	None	[{u'sort': [1670411037724, u'b8459fd2-83fd-4e66-8ab8-cc2bb30aa35b'], u'task': {u'domain': u'misogyny.wtf', u'uuid': u'b8459fd2-83fd-4 u'uuid': u'f83c1f25-0fe2-4b77-81e1-0c361dbbb86a', u'tags': [u'falconsandbox'], u'url': u'http://misogyny.wtf:2020/parser', u'visibili {u'url': u'http://misogyny.wtf:8080/', u'domain': u'misogyny.wtf'}}, {u'sort': [1670340399738, u'19665abc-7aa0-4a45-a797-773dbc687d87 u'http://misogyny.wtf/inject/UsRjS959Rqm4sPG4', u'domain': u'misogyny.wtf'}}, {u'sort': [1670266722965, u'cec606b8-c7e8-440e-b5c1-e54 u'https://urlscan.io/screenshots/cf6b010e-dcf1-45ea-8d1c-72a1761a13f0.png', u'result': u'https://urlscan.io/api/v1/result/cf6b010e-dc {u'sort': [1669730057154, u'81c71b8b-5519-4298-b6c9-9aa5fe59adbd'], u'task': {u'domain': u'misogyny.wtf', u'uuid': u'81c71b8b-5519-42 u'result': u'https://urlscan.io/api/v1/result/f790fc7c-b381-40d2-bf28-46b8634c5620/', u'_id': u'f790fc7c-b381-40d2-bf28-46b8634c5620'
2022-12-18 00:23:00	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	amen.fr
2022-12-18 00:09:19	Physical Location	No	LeakIX	0	0	2	0	None	United States
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	spottedelectroniclibrary.0300fllas.repl.co
2022-12-18 00:09:54	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:03:07	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.189
2022-12-18 00:06:15	Web Content	No	Web Spider	1	0	1	0	None	https://discord.gg/uD2nwtBvbP
2022-12-18 00:21:17	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:
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	movil.pacificow.repl.co
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:00:21:01)
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	Reddit (Category: social) https://www.reddit.com/user/rasputain
2022-12-18 00:15:36	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:07:17	Web Content Type	No	Web Spider	0	0	2	0	None	text/html; charset=UTF-8
2022-12-18 00:03:05	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.178
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	daviseguridad.wwwcomm.repl.co
2022-12-18 00:26:05	Physical Location	No	MetaDefender	0	0	2	0	None	San Jose, United States
2022-12-18 00:08:15	Netblock Membership	No	RIPE	1	0	1	0	None	51.103.0.0/16
2022-12-18 00:18:19	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.7:8080
2022-12-18 00:07:18	HTTP Status Code	No	Web Spider	0	0	3	0	None	404
2022-12-18 00:09:54	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/

2022-12-18 00:20:56	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:11:27	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'autocompl
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:12:05	Country	No	Country Name Extractor	0	0	5	0	None	Italy
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:8880
2022-12-18 00:32:33	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.154:53
2022-12-18 00:04:12	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:02:52	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:d8:1f:4b:91:5b:d7:bf:2f:be:6e:27:8c:6c:60:f6:86:80 Signature Algorithm: ecdsa-w with-SHA256 30:45:02:20:4B:23:C5:C7:DA:43:E1:C7:33:EC:22:06: 46:DB:FD:FD:6E:26:73:6A:42:93:5E:C8:48:8D:94:08: 6A:63:AE:77:02:21:00:D6
2022-12-18 00:05:13	Linked URL - Internal	No	Hybrid Analysis	0	0	2	0	None	http://misogyny.wtf:2020/parser
2022-12-18 00:33:16	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.226] https://www.virustotal.com/en/ip-address/81.88.52.226/information/
2022-12-18 00:08:56	Physical Location	No	LeakIX	0	0	2	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:08:29	Netblock Membership	No	RIPE	1	0	2	0	None	172.67.128.0/20
2022-12-18 00:12:17	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'compromised_ u'network-51', u'name': u'Queries DNS server', u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1071/004', u'threat_level_hum [%APPDATA%\\Microsoft\\Windows\\Cookies\\BJZ8QG4I.txt]- [targetUID: 00000000-00002788]\n Dropped file: "13L0SVE5.txt" - Location: [%A "6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptr "~DF2EA3D3EAFAB86FB1.TMP" has type "data"- Location: [%TEMP%\\~DF2EA3D3EAFAB86FB1.TMP]- [targetUID: 00000000-00002788]\n "57C8EDB95DF http://188.114.96.3:2052/j.ad\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAcc u'attck_id': None, u'relevance': 3, u'threat_level': 1, u'type': 2, u'description': u'Potential IP "188.114.96.3" found in string "ht
2022-12-18 00:09:31	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	calpehuturgaza.ml
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	herron-libson (Net ID: 00:01:24:F1:75:B2)
2022-12-18 00:16:59	Web Content	No	Web Spider	0	0	4	0	None	body { background: #eee none repeat scroll 0 0; } h1{ color: #888;} .navbar {display:none;} .main-content{background: none;} .company
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:16:34	Physical Location	No	numverify	0	0	3	0	None	Ponchatoul, US
2022-12-18 00:22:07	Open TCP Port	No	Censys	0	0	2	0	None	34.149.204.188:443
2022-12-18 00:06:45	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.eu
2022-12-18 00:16:26	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	188.114.96.3:443
2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://wasp.plague.fun/inject/PDS1ays5XQVjXMk3
2022-12-18 00:06:13	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "user-agent: ")\n "GET /assets/css/styles.css HTTP/1.1\nAccept: text/css, */*\nReferer: https://uuuytttt89999.57f7f7cff7f7f.repl.co/\ HTTP/1.1\nAccept: application/javascript, */*;q=0.8\nReferer: https://uuuytttt89999.57f7f7cff7f7f.repl.co/\nAccept-Language: en-US\nU (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nHost: uuuytttt89999.57f7f7cff7f7f.repl.co\nDNT: 1\nConnection: Keep-Alive" (Indica "mozilla/5.0 (")\n "GET /s/roboto/v30/KFOlCnqEu92Fr1MmWUlvAA.woff HTTP/1.1\nAccept: */*\nReferer: https://uuuytttt89999.57f7f7cff7f7f 1\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GET /s/roboto/v30/KFOmCnqEu92Fr1Me5g.woff HTTP/1.1\nAccept: */*\nReferer: gzip, deflate\nHost: fonts.gstatic.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GET /s/roboto/v30/KFOlCnqEu92

2022-12-18 00:22:01	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-O
2022-12-18 00:03:02	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:54:d1:cf:73:f4:06:da:67:36:31:1b:04:19:11:b7:02:21 Signature Algorithm: ecdsa-w with-SHA256 30:44:02:20:70:F2:E0:AE:CF:85:A2:03:22:79:FB:17: 39:F6:2F:87:C6:15:E4:F1:18:13:A9:F1:82:72:E6:C7: 7E:9E:29:13:02:20:30:0A
2022-12-18 00:16:35	Raw Data from RIRs	No	numverify	0	0	3	0	None	{u'international_format': u'+3544212434', u'local_format': u'4212434', u'number': u'3544212434', u'valid': True, u'line_type': u'land
2022-12-18 00:12:19	Phone Number	No	Phone Number Extractor	3	0	2	0	None	+492283296859
2022-12-18 00:13:04	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Companies formerly listed on the London Stock Exchange
2022-12-18 00:12:19	Phone Number	No	Phone Number Extractor	0	0	2	0	None	+492283296859
2022-12-18 00:26:12	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.pl
2022-12-18 00:27:16	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [188.114.96.3]
2022-12-18 00:02:39	Domain Name	No	SpiderFoot UI	46	0	0	0	None	plague.fun
2022-12-18 00:15:16	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:2095
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:09:F8:70)
2022-12-18 00:22:07	Open TCP Port	No	Censys	0	1	2	0	None	34.149.204.188:5900
2022-12-18 00:07:06	HTTP Headers	No	Web Spider	2	0	2	0	None	{"content-length": "68", "x-powered-by": "Express", "accept-ranges": "bytes", "keep-alive": "timeout=5", "last-modified": "Wed, 02 No
2022-12-18 00:09:44	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	ancient-cell-1aa7.2864713421.workers.dev
2022-12-18 00:13:44	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	abuse@register.it
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	56544.56554.repl.co
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetCBD2 (Net ID: 00:01:36:59:CB:D0)
2022-12-18 00:23:10	Raw Data from RIRs	No	CRXcavator	1	0	1	0	None	[{"platform": "Chrome", "version": "1342", "data": {"webstore": {"website": "", "rating": 0, "privacy_policy": "", "last_updated": "2 "short_description": "Command & Conquer Tiberium Alliances introduces an all new way to play with your friends in a browser-based, fr "https://lh3.googleusercontent.com/rYfXlSeN63sJW6ll6pKFK-MqErn5KGPgUz7qxlikWS3SUyAGcEJBDS38OKLMBTqbQxDZrqz-1Yp0aysTJBUnIaUu=w128-h128 {"rating": 3.8280256, "users": 10000, "platform": "", "short_description": "Do you have what it takes to become a Legend? Gather your "https://lh3.googleusercontent.com/o7i1oeutKe1UW8s0ECUXnCi6VplTAYUoMLQp7S9ba9f1efR1X7M7jFlgS49CclfFbMRwhHBtmDDkEyP9Yj2Az439qA=w128-h1 {"rating": 4.0218296, "users": 60000, "platform": "", "short_description": "Build magnificent cities, forge mighty alliances, utilize "name": "Plague Inc", "default_locale": "en", "icons": {"128": "icon.png", "16": "icon.png"}, "app": {"background": {"page": "app_mai
2022-12-18 00:20:46	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.me
2022-12-18 00:08:17	Netblock Membership	No	RIPE	1	0	2	0	None	104.21.16.0/20
2022-12-18 00:09:11	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.190.129:80
2022-12-18	Affiliate - Email	No	E-Mail Address Extractor	0	0	3	0	None	registrar-abuse@google.com

00:32:28	Address								
2022-12-18 00:06:57	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "184.31.203.241:443"'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-0', u'name': u'Contacts dom Characteristics', u'origin': u'Binary File', u'identifier': u'binary-37', u'name': u'Drops files inside appdata directory', u'attck_i None, u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 8, u'description': u'"urlblockindex_1_.bin" has type "data"- [00000000-00002488]\n "6399055E5DDC20781CB1B49666322796" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\ "6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptr u'relevance': 3, u'threat_level': 0, u'type': 2, u'description': u'"GET / HTTP/1.1\nAccept: text/html, application/xhtml+xml, */*\nAc
2022-12-18 00:13:34	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	rir@cloudflare.com
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	bancaweb--pichiweb.repl.co
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	FriendFinder (Category: dating) https://friendfinder.com/profile/rasputain
2022-12-18 00:09:02	Physical Location	No	LeakIX	0	0	2	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:08:44	Physical Location	No	LeakIX	0	0	1	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:19:01	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'PAC', u'country_tld': u'.fr', u'ip': u'90.116.149.183', u'currency_name': u'Euro', u'currency': u'EUR', u'country_
2022-12-18 00:31:36	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.media
2022-12-18 00:21:13	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:
2022-12-18 00:21:20	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:03:31	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3230.webapps.net
2022-12-18 00:22:01	Open TCP Port	No	Censys	0	0	2	0	None	2a06:98c1:3121::1:443
2022-12-18 00:21:23	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://wasp.plague.fun/inject/Fu643XzaSbmCcnGN
2022-12-18 00:03:01	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.96
2022-12-18 00:21:51	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:09:36	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	samplicongcy.ga
2022-12-18 00:08:46	Internet Name	No	DNS Resolver	0	0	3	0	None	www.zerotwo-best-waifu.online
2022-12-18 00:03:05	IPv6 Address	No	DNS Resolver	2	0	1	0	None	2606:4700:3036::ac43:a9d7
2022-12-18 00:04:28	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	eforward4.registrar-servers.com
2022-12-18 00:09:31	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.169.215:8080
2022-12-18 00:29:08	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.co.uk
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	GOAT (Net ID: 00:00:C5:D3:87:1C)

2022-12-18 00:02:43	Raw Data from RIRs	No	CertSpotter	4	0	1	0	None	[{u'pubkey_sha256': u'eed16361070909e64009401f21e37cfc30dd63ff7c8f701bfc59a6437ea80bc8', u'revoked': False, u'not_after': u'2023-01-0 u'MIIEWzCCA0OgAwIBAgISBEOkfSkfFQ5rrIbkS8C+aXGpMA0GCSqGSIb3DQEBCwUAMDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQDEwJ u'8841f6cbb8d7c763c61eaa51603a73de43f3a7e57f918aadcf54ea83ea9981a5', u'type': u'cert'}, u'dns_names': [u'hook.plague.fun'], u'tbs_sha u'MIIEVjCCAz6gAwIBAgISBNDRocx8IO3rAfyF3UXM5RvaMA0GCSqGSIb3DQEBCwUAMDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQDEwJ u'3e85be100bffaa41aba2e11a1f798d83d44538d9ccd62a4edf68e383abdb3c4e', u'type': u'cert'}, u'dns_names': [u'api.plague.fun'], u'tbs_sha2 u'MIIDvzCCA0WgAwIBAgISBGvFWhyq3hElOoWsJ0ashMKpMAoGCCqGSM49BAMDMDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQDEwJFMTA u'2022-10-30T18:19:31Z', u'issuer': {u'pubkey_sha256': u'276fe8a8c4ec7611565bf9fce6dcace9be320c1b5bea27596b2204071ed04f10', u'name': u'MIIEdTCCA12gAwIBAgIQSCBA6RFsRvwTyMaRlabRmzANBgkqhkiG9w0BAQsFADBGMQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzE u'sha256': u'e90fee33471e445f420dc6f027f4c54e500b881c2f610a9e165722ea988fac0e', u'type': u'precert'}, u'dns_names': [u'*.plague.fun', u'MIIEWjCCA0KgAwIBAgISA/hAB6kqKfqV4l/q8ul1eVeOMA0GCSqGSIb3DQEBCwUAMDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQDEwJ u'1e9cb916ccc4fd493f7420d2e58d07274fd1c30f24785e0b9764ffd07e7fc73f', u'type': u'cert'}, u'dns_names': [u'atlas.plague.fun'], u'tbs_sh
2022-12-18 00:21:30	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-O
2022-12-18 00:02:44	Raw Data from RIRs	No	grep.app	0	0	1	0	None	{u'repo': {u'raw': u'billythegoat356/billythegoat356.github.io'}, u'total_matches': {u'raw': u'1'}, u'content': {u'snippet': u'<table class="p">></pre> </td></tr></table>'}, u'branch': {u'raw': u'main'}, u'path': {u'raw': u'index.html'}, u'id': {u'raw'
2022-12-18 00:23:31	Affiliate - Internet Name	No	DNS Raw Records	0	0	2	0	None	mail-fr.securemail.pro
2022-12-18 00:06:33	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.0:2053
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:443
2022-12-18 00:08:28	Netblock Membership	No	RIPE	0	0	2	0	None	20.192.0.0/10
2022-12-18 00:27:45	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@reg.ru
2022-12-18 00:03:08	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	stream.plague.fun
2022-12-18 00:22:07	Open TCP Port Banner	No	Censys	0	1	2	0	None	SSH-2.0-Go
2022-12-18 00:13:49	Internet Name	No	DNS Brute-forcer	32	0	1	0	None	webmail.zerotwo-best-waifu.online
2022-12-18 00:03:11	Affiliate - Internet Name	No	DNS Resolver	6	0	2	0	None	lfbn-nic-1-332-104.w90-116.abo.wanadoo.fr
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	nbangoemp.pmencjdo.repl.co
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:2082
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:09:37	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	trabneumaunosu.cf
2022-12-18 00:21:51	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:21:10	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)
2022-12-18 00:06:01	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	registrar-servers.com
2022-12-18 00:25:35	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-177.w90-116.abo.wanadoo.fr
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:2086

2022-12-18 00:07:06	HTTP Status Code	No	Web Spider	0	0	2	0	None	403
2022-12-18 00:10:04	Linked URL - Internal	No	URLScan.io	0	0	1	0	None	http://misogyny.wtf/
2022-12-18 00:13:56	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:21:13	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-(
2022-12-18 00:04:00	Physical Location	No	ipstack	0	0	1	0	None	Brazil
2022-12-18 00:09:34	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	gardensbyvasa.com.au
2022-12-18 00:09:43	Physical Location	No	LeakIX	0	0	2	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:05:24	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:d8:1f:4b:91:5b:d7:bf:2f:be:6e:27:8c:6c:60:f6:86:80 Signature Algorithm: ecdsa-w 7d:15:20:77:67:d0:90:38:10:5b:48:dd:57:cb:ca:a1:52:ea: 8d:85:f7:05:57:5c:7e:54:a9:74:9f:1f:0b:f4:23:4d:b1:38: 0d:58:4c:ba:2e:9d:cc:fc
2022-12-18 00:22:01	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:21:06	Netblock Membership	No	Censys	0	0	2	0	None	172.67.144.0/20
2022-12-18 00:18:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.9:443
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:2083
2022-12-18 00:03:04	Domain Name	No	DNS Resolver	0	0	1	0	None	misogyny.wtf
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:2083
2022-12-18 00:04:43	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'banker', u'dridex'], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score' 00002316) was launched with modified environment variables: "CommonProgramFiles, PROCESSOR_ARCHITECTURE, ProgramFiles"\n Process "reg "HKLM\\SOFTWARE\\POLICIES\\MICROSOFT\\SYSTEMCERTIFICATES\\DISALLOWED"; Key: "")\n "EXCEL.EXE" (Path: "HKLM\\SOFTWARE\\POLICIES\\MICRO u'identifier': u'registry-72', u'name': u'Overview of unique CLSIDs touched in registry', u'attck_id_wiki': None, u'threat_level_huma 000000000046}\\PROGID")\n "EXCEL.EXE" touched "Microsoft Excel-Vorschau" (Path: "HKLM\\SOFTWARE\\CLASSES\\WOW6432NODE\\CLSID\\{000208 u'CAPEC-203', u'attck_id': u'T1112', u'relevance': 10, u'threat_level': 0, u'type': 3, u'description': u'"EXCEL.EXE" (Path: "HKCU\\SC u'Creates mutants', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance'
2022-12-18 00:33:50	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.duckdns.org
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:8080
2022-12-18 00:08:54	Physical Location	No	LeakIX	0	0	2	0	None	United States
2022-12-18 00:06:31	Company Name	No	Company Name Extractor	0	0	2	0	None	(c) CentralNic Ltd
2022-12-18 00:21:17	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:
2022-12-18 00:11:29	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'549300F1AETTPWFIQC02'}, u'links': {u'related': u'ht
2022-12-18 00:08:30	IP Address	No	LeakIX	32	0	1	0	None	188.114.97.3
2022-12-18 01:02:39	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	misogyny.tv
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	Pinterest (Category: social) https://www.pinterest.com/rasputain/
2022-12-18	Raw Data from RIRs	No	LeakIX	0	0	3	0	None	{u'Services': None, u'Leaks': None}

00:20:39									
2022-12-18 00:13:04	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 configurati
2022-12-18 00:03:09	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.227
2022-12-18 00:03:07	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:e2:2d:48:dd:4c:ac:71:43:1c:ff:e5:61:16:60:4c:1f:a4 Signature Algorithm: sha256W X509v3 Authority Key Identifier: keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1 Authority Information Access: OCSP
2022-12-18 00:31:52	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@godaddy.com
2022-12-18 00:21:27	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conn
2022-12-18 00:03:12	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-94.w90-116.abo.wanadoo.fr
2022-12-18 00:09:49	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 4.3 Description: OpenVPN, when using a 64-bit block cipher, makes
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Twist Studio (Net ID: 00:02:2D:07:96:23)
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	webpersonspichincha001.webpichinch.repl.co
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F2:68:C6)
2022-12-18 00:21:11	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)
2022-12-18 00:09:33	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'https', u'event_type': u'service', u'ip': u'104.21.27.242', u'vendor': u'', u'port': u'8443', u'transp u'version': u'TLSv1.3'}, u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'banner': u'', u'fingerprint': u''}, u'reverse': u'', u' u'6d1f2e7c9ee98731cbe0777147f6cea56397bac293093c74cd11f41aab407d3c', u'leak': {u'dataset': {u'files': 0, u'rows': 0, u'ransom_notes': DYNAMIC\r\nReport-To: {"endpoints":[{"url":"https:\\/\\/a.nel.cloudflare.com\\/report\\/v3?s=V955oUFCMGVGAQRwwGvjZhBfanO%2BAL3Z9Rjin4 {u'cypher_suite': u'TLS_AES_128_GCM_SHA256', u'jarm': u'00000000000000000000000000000000000000000000000000000000000000', u'certificat 29=":443"; ma=86400\r\n\nPage title: Tab Exotic Group (Hotel & Resorts)', u'time': u'2022-11-03T02:09:47.82234924Z'}, {u'protocol': u u'af4ce661fba34939b39d90789bbff1b008b6fa360aac04754b2796654528cbc7', u'key_algo': u'RSA', u'not_before': u'2022-10-04T11:54:56Z'}, u'
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:03:36	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3242.webapps.net
2022-12-18 00:21:06	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-O
2022-12-18 00:03:27	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	196.204.149.34.bc.googleusercontent.com
2022-12-18 00:21:20	Physical Location	No	Censys	0	0	2	0	None	Amsterdam, North Holland, 1012, Netherlands, Europe
2022-12-18 00:22:01	Open TCP Port	No	Censys	0	0	2	0	None	2a06:98c1:3121::1:80
2022-12-18 00:02:51	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:d0:d1:a1:cc:7c:20:ed:eb:01:fc:85:dd:45:cc:e5:1b:da Signature Algorithm: sha256W with-SHA256 30:45:02:21:00:A9:DD:3E:19:3D:08:47:5F:9B:B1:90: AB:C2:AD:E2:91:05:EF:EF:95:99:23:9E:12:BB:18:C5: F2:98:2C:7F:FF:02:20:30
2022-12-18 00:03:07	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.190
2022-12-18 00:12:34	Physical Location	No	ipapi.co	0	0	2	0	None	London, England, ENG, United Kingdom, GB
2022-12-18 00:21:11	WiFi Access	No	Wigle.net	0	0	5	0	None	" (Cloaked) (Net ID: 00:01:36:59:CB:CF)

	Point Nearby								
2022-12-18 00:10:20	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 protoc
2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://plague.fun
2022-12-18 00:04:45	Raw Data from RIRs	No	Maltiverse	3	0	2	0	None	{u'asn_registry': u'arin', u'country_code': u'US', u'classification': u'neutral', u'asn_country_code': u'US', u'is_open_proxy': False
2022-12-18 00:59:52	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namecheap.com
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	BodyBuilding.com (Category: health) http://bodyspace.bodybuilding.com/rasputain/
2022-12-18 00:07:39	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:04:06	Raw Data from RIRs	No	Hybrid Analysis	0	0	1	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised "\\Sessions\\1\\BaseNamedObjects\\Local\\!BrowserEmulation!SharedMemory!Mutex"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\VERMGMTBloc [targetUID: 00000000-00003048]\n Dropped file: "XXQS23FV.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\XXQS23FV.txt]- [ta type "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "~DF23DB81915CF93D1F.TMP" has type "data"- Lo 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'desc trusted Antivirus engine', u'attck_id_wiki': None, u'threat_level_human': u'malicious', u'capec_id': None, u'attck_id': None, u'relev Transfer', u'informative_identifiers': [], u'tactic': u'Command and Control', u'informative_identifiers_count': 1, u'suspicious_ident
2022-12-18 00:05:57	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u' u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 4, u'descr [%APPDATA%\\Microsoft\\Windows\\Cookies\\UOY3MQVE.txt]- [targetUID: 00000000-00003272]\n Dropped file: "T8SUW2BB.txt" - Location: [%A type "UTF-8 Unicode (with BOM) text with CRLF line terminators"- [targetUID: N/A]\n "RecoveryStore._714D72AB-6A0C-11ED-B810-08002797D u'https://attack.mitre.org/techniques/T1573', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1573', u'rele u'threat_level_human': u'suspicious', u'capec_id': None, u'attck_id': None, u'relevance': 0, u'threat_level': 1, u'type': 12, u'descr u'attck_id_wiki': u'https://attack.mitre.org/techniques/T1573', u'suspicious_identifiers': [], u'attck_id': u'T1573', u'malicious_ide
2022-12-18 00:02:48	IP Address	No	Mnemonic PassiveDNS	81	0	1	0	None	188.114.96.0
2022-12-18 00:08:45	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	obf.plague.fun
2022-12-18 00:10:04	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://misogyny.wtf:1337/inject/UsRjS959Rqm4sPG4/
2022-12-18 00:16:53	Company Name	No	Company Name Extractor	0	0	3	0	None	Cloudflare\, Inc.
2022-12-18 00:04:30	DNS SPF Record	No	DNS Raw Records	0	0	1	0	None	v=spf1 include:spf.webapps.net ~all
2022-12-18 00:06:21	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.cz
2022-12-18 00:31:52	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@west.cn
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:21:02	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:09:14	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.19.243:443
2022-12-18 00:13:49	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	contact@kifcorp.fr
2022-12-	IP Address	No	SpiderFoot UI	15	0	0	0	None	20.195.209.219

18 00:02:39									
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:09:38	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.13:8443
2022-12-18 00:20:18	Netblock Membership	No	RIPE	0	0	3	0	None	81.88.48.0/20
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:2095
2022-12-18 00:21:03	Web Server	No	Web Server Identifier	0	0	3	0	None	Werkzeug/2.2.2 Python/3.9.11
2022-12-18 00:28:34	Physical Location	No	MetaDefender	0	0	3	0	None	Firenze, Italy
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:08:30	IP Address	No	LeakIX	32	0	1	0	None	188.114.96.3
2022-12-18 00:02:43	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 48:20:40:e9:11:6c:46:fc:13:c8:c6:91:95:a6:d1:9b Signature Algorithm: sha256WithRSA keyid:D5:FC:9E:0D:DF:1E:CA:DD:08:97:97:6E:2B:C5:5F:C5:2B:F5:EC:B8 Authority Information Access: OCSP - URI:http://ocsp.pki.goog/s/gts
2022-12-18 00:08:38	BGP AS Membership	No	RIPE	0	0	2	0	None	17916
2022-12-18 00:06:27	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'compromised_ like Gecko\nAccept-Encoding: gzip, deflate\nHost: instructivesystemcall.securyful.repl.co\nDNT: 1\nConnection: Keep-Alive" (Indicator like Gecko\nHost: instructivesystemcall.securyful.repl.co\nDNT: 1\nConnection: Keep-Alive" (Indicator: "user-agent: ")\n "GET /s/ibmp https://instructivesystemcall.securyful.repl.co/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11 "UpdatingNewTabPageData"\n "Local\\VERMGMTBlockListFileMutex"\n "IsoScope_ca4_IE_EarlyTabStart_0xdbc_Mutex"\n "IsoScope_ca4_IESQMMUTE directory', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 3, u't "css_2_.css" has type "ASCII text"- [targetUID: N/A]\n "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has type "MS Windows icon
2022-12-18 00:12:14	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 15, u'threat_score': 35, u'compromised "Local\\SM0:7844:120:WilError_01"\n "Local\\ChromeProcessSingletonStartup!"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:7844:120:W Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Network\\1a8f52a0-4099-4402-b391-421fc08473ee.tmp]- [targetUID: 00000 7175f0cedd28.tmp]- [targetUID: 00000000-00007844]\n "870b1947-b37b-41dc-a12d-92436625da90.tmp" has type "UTF-8 Unicode text with very u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 2, u'description': u'Pattern mat [%TEMP%\\7844_1603751462\\product_page.js]- [targetUID: 00000000-00007844]\n Dropped file: "edge_driver.js" - Location: [%TEMP%\\7844 "C:\\Users\\HAPUBWS\\AppData\\Local\\Microsoft\\Edge\\User Data\\Default\\EdgePushStorageWithConnectTokens" (Indicator: "microsoft\\e
2022-12-18 00:08:37	Raw Data from RIRs	No	Certificate Transparency	1	0	2	0	None	[{u'not_after': u'2022-09-18T23:59:59', u'not_before': u'2022-06-20T00:00:00', u'issuer_ca_id': 158800, u'name_value': u'www.zerotwo-
2022-12-18 00:18:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.17:8080
2022-12-18 00:06:18	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "\\Sessions\\1\\BaseNamedObjects\\{5312EE61-79E3-4A24-BFE1-132B85B23C3A}"\n "\\Sessions\\1\\BaseNamedObjects\\IsoScope_cb4_IESQMMUTE Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: 000 (Indicator: "mozilla/5.0 (")\n "GET /css/main.css HTTP/1.1\nAccept: text/css, */*\nReferer: https://0006352.841600.repl.co/\nAccept-L */*;q=0.5\nReferer: https://0006352.841600.repl.co/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv https://0006352.841600.repl.co/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nC "data")\n Antivirus vendors marked dropped file "Tar2648.tmp" as clean (type is "data")'}, {u'category': u'Unusual Characteristics',
2022-12-18 00:16:32	Physical Location	No	numverify	0	0	3	0	None	Bonn, DE
2022-12-18 00:39:05	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: MISOGYNY.COM.AU Registry Domain ID: D407400000112218537-AU Registrar WHOIS Server: whois.auda.org.au Registrar URL: http (a) aggregating, collecting or compiling information from the WHOIS database, whether for personal or commercial purposes; (b) enabli Registrant: GEARAP PTY LTD Registrant ID: ABN 29656097504 Eligibility Type: Company >>> Last update of WHOIS database: 2022-12-18T00:
2022-12-18 00:30:56	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: PLAGUE.BAR Registry Domain ID: D259269512-CNIC Registrar WHOIS Server: whois.namecheap.com Registrar URL: https://namech Abuse Contact Phone: +1.9854014545 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of W Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransf information on Whois status codes, please visit https://icann.org/epp
2022-12-18 00:20:42	Raw Data from RIRs	No	Censys	0	0	1	0	None	{"last_updated_at": "2022-12-08T00:47:57.786Z", "ip": "4.228.83.86", "location_updated_at": "2022-12-18T00:20:39.887003Z", "autonomou

2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2087
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	onlinepichinchabankingecuinfor.ecuador1.repl.co
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	beigekhakiprocedurallanguage.pichinncha3ec.repl.co
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	1.porseguridad.repl.co
2022-12-18 00:27:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.48.101:143
2022-12-18 00:09:35	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	goldmenrockfirokan.gq
2022-12-18 00:25:58	Physical Location	No	MetaDefender	0	0	2	0	None	Knoxville, United States
2022-12-18 00:21:58	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:31:16	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.games
2022-12-18 00:02:44	Internet Name - Unresolved	No	CertSpotter	0	0	1	0	None	atlas.plague.fun
2022-12-18 00:13:55	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:04:11	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F0:17:4A)
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	matrix (Net ID: 00:02:2D:03:92:64)
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:2053
2022-12-18 00:08:41	Raw Data from RIRs	No	LeakIX	0	0	1	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'40.113.112.131', u'vendor': u'', u'port': u'80', u'transpor {u'region_iso_code': u'NL-NH', u'country_iso_code': u'NL', u'city_name': u'Amsterdam', u'location': {u'lat': 52.3759, u'lon': 4.8975} length': u'94', u'server': u'Werkzeug/2.2.2 Python/3.10.0'}, u'length': 0, u'favicon_hash': u'', u'root': u''}, u'tags': [], u'ssl': u'key': u''}, u'software': {u'modules': [{u'version': u'3.10.0', u'name': u'Python', u'fingerprint': u''}], u'version': u'2.2.2', u'c GMT\r\nContent-Type: text/html; charset=utf-8\r\nContent-Length: 94\r\nConnection: close\r\n\r\nRoses are red Violets are blue
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	6562 7451 (Net ID: 00:00:C5:D7:2F:EC)
2022-12-18 00:07:16	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:16:57	Linked URL - Internal	No	Web Spider	4	0	3	0	None	http://webmail.zerotwo-best-waifu.online/css/vendor/font-awesome-4.4.0/css/font-awesome.min.css
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:2095
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	3c7db43e-a280-41f9-8469-621300b1364c.id.repl.co
2022-12-18 00:09:37	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	www.fancyacake.net
2022-12-18 00:07:20	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 2, u'threat_score': None, u'compromise "HKLM\\SOFTWARE\\MICROSOFT\\SYSTEMCERTIFICATES\\FLIGHTROOT\\CERTIFICATES"; Key: "08745487E891C19E3078C1F2A07E452950EF36F6")\n "Ledger "0x37f800" greater than 0x100000\n Raw size of ".text" is "0x211e00" greater than 0x100000'}, {u'category': u'General', u'origin': u' ".text"\n "nsis7z.dll" has an executable section named ".text"\n "ledger.exe" has an executable section named ".text"\n "Uninstall Le Virtual size of ".data" is "0x15e198" greater than 0x100000'}, {u'category': u'General', u'origin': u'String', u'identifier': u'strin u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 2, u'descr u'General', u'origin': u'Static Parser', u'identifier': u'static-95', u'name': u'PE file contains writable sections', u'attck_id_wiki

2022-12-18 00:17:36	Physical Coordinates	No	OpenStreetMap	91	0	4	0	None	37.780462,-122.390564
2022-12-18 00:21:44	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:05:18	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 20, u'threat_score': 100, u'compromise "Local\\SM0:5864:120:WilError_01"\n "Local\\SM0:5864:304:WilStaging_02"\n "Local\\InternetShortcutMutex"\n "Local\\SM0:5660:304:WilSt 42d6-4da2-b87c-cac737035349.tmp" has type "ASCII text with very long lines with no line terminators"- [targetUID: N/A]\n "41962708-5f "03cc95bd-1754-476e-b462-79536e7625ef.tmp" has type "UTF-8 Unicode text with very long lines with no line terminators"- Location: [%L "ASCII text with very long lines with no line terminators"- Location: [%TEMP%\\5660_724844775\\runtime.bundle.js]- [targetUID: 000000 [%TEMP%\\5660_1719137669\\edge_tracking_page_validator.js]- [targetUID: 00000000-00005660]\n Dropped file: "product_page.js" - Locati "bnpl_driver.js" - Location: [%TEMP%\\5660_724844775\\bnpl_driver.js]- [targetUID: 00000000-00005660]\n Dropped file: "edge_confirmat
2022-12-18 00:21:17	Physical Location	No	Censys	0	0	2	0	None	Amsterdam, North Holland, 1012, Netherlands, Europe
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:22:14	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:05:33	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u' {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries DNS server', u'attck_id_wik File', u'identifier': u'binary-5', u'name': u'Drops cabinet archive files', u'attck_id_wiki': None, u'threat_level_human': u'informat [%APPDATA%\\Microsoft\\Windows\\Cookies\\9PWEDQN7.txt]- [targetUID: 00000000-00003692]'}, {u'category': u'Installation/Persistence', [%TEMP%\\CabC0DE.tmp]- [targetUID: 00000000-00003692]\n "L7ALW6TW.txt" has type "ASCII text"- Location: [%APPDATA%\\Microsoft\\Window long lines"- [targetUID: N/A]'}, {u'category': u'Network Related', u'origin': u'String', u'identifier': u'string-3', u'name': u'Found Kestrel\nLocation: https://www.msn.com/spartan/ientpgbconfig?locale=en-us&market=us\nRequest-Context: appId=cid-v1:b47e5e27-bf85-45ba
2022-12-18 00:08:40	Netblock Membership	No	RIPE	0	0	2	0	None	188.114.96.0/24
2022-12-18 00:22:01	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:
2022-12-18 00:22:01	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T19:12:26.206Z", "ip": "2a06:98c1:3121::1", "location_updated_at": "2022-12-13T16:38:32.429523Z", "aut "DISPLAY_HEX"}, "http": {"request": {"headers": {"_encoding": {"User_Agent": "DISPLAY_UTF8", "Accept": "DISPLAY_UTF8"}, "User_Agent": Type\",\"application/json\");b.setRequestHeader(\"Sparrow-Source-Key\",\"c771f0e4b54944bebf4261d44bd79a1e\");\nb.send(JSON.stringify(light\">Direct IP access not allowed</h2>\n </header>\n\n <section class=\"w-240 lg:w-full mx-auto mb-8 lg:px-8\">\n <div id=\"what-h Thank you for your feedback!\n \n \n\n\n <div class=\"cf-error-footer cf-wrapper w-240 lg:w-full py-10 sm:py-4 sm:px-8 mx- wrapper -->\n\n <script>\n window._cf_translation = {};\n \n \n</script>\n\n</body>\n</html>\n", "_encoding": {"body": "DISPLAY_UTF8" name=\"robots\" content=\"noindex, nofollow\" />", "<meta name=\"viewport\" content=\"width=device-width,initial-scale=1\" />"], "sta
2022-12-18 00:21:09	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-O
2022-12-18 00:21:09	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-O
2022-12-18 00:04:11	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	sni.cloudflaressl.com
2022-12-18 00:31:33	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.lol
2022-12-18 00:06:31	Company Name	No	Company Name Extractor	0	0	3	0	None	Cloudflare\, Inc.
2022-12-18 00:14:01	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.138:8443
2022-12-18 00:13:50	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	domains@secommerce.com
2022-12-18 00:14:06	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:24:06	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namecheap.com
2022-12-18 00:24:05	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	aes128-gcm@openssh.com

2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:2096
2022-12-18 00:21:54	Netblock Membership	No	Censys	0	0	2	0	None	104.21.0.0/20
2022-12-18 00:03:05	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.112
2022-12-18 00:21:47	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:22:07	Open TCP Port	No	Censys	0	0	2	0	None	34.149.204.188:22
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:2086
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:2087
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:8080
2022-12-18 00:21:13	Netblock Membership	No	Censys	0	0	2	0	None	188.114.97.0/24
2022-12-18 00:12:21	Physical Location	No	ipapi.co	0	0	2	0	None	Toronto, Ontario, ON, Canada, CA
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WestEd (Net ID: 00:02:2D:05:7E:93)
2022-12-18 00:09:46	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	apoveppacomp.tk
2022-12-18 00:03:06	Internet Name	No	DNS Resolver	0	0	2	0	None	misogyny.wtf
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	logitecgameuser (Net ID: 00:01:8E:15:D4:A7)
2022-12-18 00:16:40	Blacklisted Affiliate Internet Name	Yes	DNS for Family	0	0	2	0	None	DNS for Family [dns1.registrar-servers.com]
2022-12-18 00:12:57	Malicious IP on Same Subnet	Yes	blocklist.de	0	0	2	0	None	blocklist.de List [20.192.0.0/10] http://lists.blocklist.de/lists/all.txt
2022-12-18 00:25:06	Malicious IP Address	Yes	MetaDefender	0	1	1	0	None	avira.com [51.103.210.236]
2022-12-18 00:25:37	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-179.w90-116.abo.wanadoo.fr
2022-12-18 00:21:20	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-(
2022-12-18 00:04:01	Physical Location	No	ipstack	0	0	2	0	None	Colombia
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:01:E6:93:CF:EC)
2022-12-18 00:02:48	IPv6 Address	No	Mnemonic PassiveDNS	13	0	1	0	None	2606:4700:3032::ac43:be81
2022-12-18 00:10:04	Web Server	No	URLScan.io	0	1	1	0	None	Werkzeug/2.2.2 Python/3.9.10
2022-12-18 00:09:49	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	avdeccatchsvalunin.ml
2022-12-18	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.137.37:8443

00:09:19									
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	70882af9-37da-4505-b503-98e1e3f95d9b.id.repl.co
2022-12-18 00:12:05	Country	No	Country Name Extractor	0	0	4	0	None	France
2022-12-18 00:02:44	Raw Data from RIRs	No	grep.app	0	0	1	0	None	{u'repo': {u'raw': u'stamparm/maltrail'}, u'total_matches': {u'raw': u'8'}, u'content': {u'snippet': u'<table class="highlight-table'
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:32:08	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.store
2022-12-18 00:06:55	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:09:29	Physical Location	No	LeakIX	0	0	2	0	None	Italy
2022-12-18 00:11:27	Physical Address	No	GLEIF	2	0	3	0	None	101 Townsend Street, San Francisco, US-CA, US, 94107
2022-12-18 00:22:07	HTTP Headers	No	Censys	0	0	2	0	None	{"Date": ["<REDACTED>"], "_encoding": {"Date": "DISPLAY_UTF8", "Replit_Cluster": "DISPLAY_UTF8", "Via": "DISPLAY_UTF8", "Content_Type
2022-12-18 00:03:18	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-107.w90-116.abo.wanadoo.fr
2022-12-18 00:24:56	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.177
2022-12-18 00:03:40	Malicious Internet Name	Yes	CloudFlare Malware DNS	0	1	1	0	None	Blocked by CloudFlare DNS [zerotwo-best-waifu.online]
2022-12-18 00:12:31	URL (Purely Static)	No	Page Information	0	0	3	0	None	http://misogyny.wtf/inject/UsRjS959Rqm4sPG4
2022-12-18 00:09:14	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.19.243:80
2022-12-18 00:09:31	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	befunctiruse.tk
2022-12-18 00:10:05	BGP AS Membership	No	URLScan.io	0	0	1	0	None	39729
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	validatusdatos.provinciaba.repl.co
2022-12-18 00:02:59	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:b5:ee:aa:9f:a9:bb:86:86:d8:5d:7e:c7:71:cb:57:b5:27 Signature Algorithm: sha256W with-SHA256 30:44:02:20:0B:C6:C4:FE:93:69:60:A2:0A:7B:46:C6: B5:A6:B4:04:7D:14:BA:16:8F:07:FF:89:52:C2:07:57: FF:91:D9:BA:02:20:13:B5
2022-12-18 00:09:35	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	omovstab.gq
2022-12-18 00:03:14	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-98.w90-116.abo.wanadoo.fr
2022-12-18 00:12:16	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 15, u'threat_score': 35, u'compromised "Local\\SM0:7844:120:WilError_01"\n "Local\\ChromeProcessSingletonStartup!"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:7844:120:W Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Network\\1a8f52a0-4099-4402-b391-421fc08473ee.tmp]- [targetUID: 00000 7175f0cedd28.tmp]- [targetUID: 00000000-00007844]\n "870b1947-b37b-41dc-a12d-92436625da90.tmp" has type "UTF-8 Unicode text with very u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 2, u'description': u'Pattern mat [%TEMP%\\7844_1603751462\\product_page.js]- [targetUID: 00000000-00007844]\n Dropped file: "edge_driver.js" - Location: [%TEMP%\\7844 "C:\\Users\\HAPUBWS\\AppData\\Local\\Microsoft\\Edge\\User Data\\Default\\EdgePushStorageWithConnectTokens" (Indicator: "microsoft\\e
2022-12-18 00:13:04	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 4.3 Description: OpenVPN, when using a 64-bit block cipher, makes
2022-12-18 00:20:18	Netblock Membership	No	RIPE	0	0	3	0	None	81.88.48.0/20
2022-12-18 00:15:26	HTTP Status Code	No	Web Spider	0	0	2	0	None	None

2022-12-18 00:27:29	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [188.114.97.3]
2022-12-18 00:21:54	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-(
2022-12-18 00:04:28	Name Server (DNS NS Records)	No	DNS Raw Records	0	0	1	0	None	dns1.registrar-servers.com
2022-12-18 00:24:15	Malicious Internet Name	Yes	MetaDefender	0	1	1	0	None	avira.com [plague.fun]
2022-12-18 00:12:12	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 16, u'threat_score': 35, u'compromised 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'd Data\\14a38b17-41cf-42dd-9514-1efd2c164496.tmp]- [targetUID: 00000000-00004208]\n "shopping_iframe_driver.js" has type "ASCII text wi 9db8-fa52080a5706.tmp]- [targetUID: 00000000-00004208]\n "a9ec7364-a580-4497-9362-d7a9dd9d7694.tmp" has type "UTF-8 Unicode text with u'type': 8, u'description': u'Dropped file: "shopping_iframe_driver.js" - Location: [%TEMP%\\4208_838907974\\shopping_iframe_driver.j (console) x86-64 for MS Windows"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\WidevineCdm\\4.10.2557.0_platform_specific "%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Subresource Filter\\Unindexed Rules\\10.34.0.33\\LICENSE"\n Potential IP "188.114.96.3"
2022-12-18 00:40:14	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.9] https://www.virustotal.com/en/ip-address/188.114.96.9/information/
2022-12-18 00:09:00	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.1:443
2022-12-18 00:26:37	Physical Location	No	MetaDefender	0	0	2	0	None	Nice, France
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	4ad096fb-61a8-446f-be87-78e866d627f7.id.repl.co
2022-12-18 00:03:09	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.225
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	GP (Net ID: 00:01:24:F1:7F:54)
2022-12-18 00:23:00	Open TCP Port	No	SSL Certificate Analyzer	0	0	3	0	None	81.88.48.102:443
2022-12-18 00:07:17	HTTP Status Code	No	Web Spider	0	0	2	0	None	200
2022-12-18 00:21:44	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:12:51	Physical Location	No	ipapi.co	0	0	2	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2022-12-18 00:12:52	Physical Location	No	ipapi.co	0	0	2	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2022-12-18 00:07:19	Web Content Type	No	Web Spider	0	0	3	0	None	text/css; charset=UTF-8
2022-12-18 00:21:34	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-(
2022-12-18 00:19:06	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'25', u'country_tld': u'.it', u'ip': u'81.88.58.196', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2022-12-18 00:09:16	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'ssh', u'event_type': u'service', u'ip': u'20.226.56.97', u'vendor': u'', u'port': u'22', u'transport': {u'lat': -22.9035, u'lon': -47.0565}, u'country_name': u'Brazil', u'continent_name': u'South America', u'region_name': u'Sao Paulo'},
2022-12-18 00:09:38	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	00749061.cn.cdn.cloudflare.net
2022-12-18 00:33:43	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.188:443
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:07:21	Linked URL - Internal	No	Google	1	0	1	0	None	http://zerotwo-best-waifu.online/
2022-12-18 00:17:08	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 Organization Validation Secure Server CA

2022-12-18 00:14:47	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.160:8080
2022-12-18 00:20:56	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-O
2022-12-18 00:18:27	IP Address	No	DNS Resolver	13	0	2	0	None	81.88.58.196
2022-12-18 00:13:46	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	abuse@web.com
2022-12-18 00:18:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.6:80
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	vapor (Net ID: 00:02:2D:09:FC:69)
2022-12-18 00:10:04	Linked URL - Internal	No	URLScan.io	0	0	1	0	None	http://misogyny.wtf/grab/UsRjS959Rqm4sPG4
2022-12-18 00:05:23	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 20, u'threat_score': 100, u'compromise "Local\\SM0:5864:120:WilError_01"\n "Local\\SM0:5864:304:WilStaging_02"\n "Local\\InternetShortcutMutex"\n "Local\\SM0:5660:304:WilSt 42d6-4da2-b87c-cac737035349.tmp" has type "ASCII text with very long lines with no line terminators"- [targetUID: N/A]\n "41962708-51 "03cc95bd-1754-476e-b462-79536e7625ef.tmp" has type "UTF-8 Unicode text with very long lines with no line terminators"- Location: [%L "ASCII text with very long lines with no line terminators"- Location: [%TEMP%\\5660_724844775\\runtime.bundle.js]- [targetUID: 000000 [%TEMP%\\5660_1719137669\\edge_tracking_page_validator.js]- [targetUID: 00000000-00005660]\n Dropped file: "product_page.js" - Locati "bnpl_driver.js" - Location: [%TEMP%\\5660_724844775\\bnpl_driver.js]- [targetUID: 00000000-00005660]\n Dropped file: "edge_confirmat
2022-12-18 00:07:19	HTTP Headers	No	Web Spider	2	0	3	0	None	{"content-length": "998", "x-powered-by": "Express", "accept-ranges": "bytes", "keep-alive": "timeout=5", "last-modified": "Sun, 11 S
2022-12-18 00:16:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:26:05	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [104.21.19.243]
2022-12-18 00:09:16	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.3:443
2022-12-18 00:08:35	Raw Data from RIRs	No	LeakIX	0	0	1	0	None	{u'Services': None, u'Leaks': None}
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	House (Net ID: 00:02:2D:09:FC:0D)
2022-12-18 00:21:41	Netblock Membership	No	Censys	0	0	2	0	None	20.192.0.0/10
2022-12-18 00:08:45	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	stream.plague.fun
2022-12-18 00:06:22	Raw Data from RIRs	No	Hybrid Analysis	1	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "IsoScope_cd4_IESQMMUTEX_0_303"\n "Local\\VERMGMTBlockListFileMutex"\n "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "Local\\URLBLOCK_HA /resources/font-awesome/css/font-awesome.min.css HTTP/1.1\nAccept: text/css, */*\nReferer: https://f8a9d265-01cc-44cf-a7f6-04910a6d1c Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: f8a9d265-01cc-44cf-a7f6-04910a6c Alive\nCookie: PHPSESSID=11aac534407b1ee5b3606bd7bea8e35a" (Indicator: "mozilla/5.0 (")\n "GET /resources/css/commonsd7ac.css?2010202 04910a6d1dcb.id.repl.co/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-E deflate\nHost: f8a9d265-01cc-44cf-a7f6-04910a6d1dcb.id.repl.co\nDNT: 1\nConnection: Keep-Alive\nCookie: PHPSESSID=11aac534407b1ee5b36
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	onlinebankingpichinchaaccount.ecuador0.repl.co
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F1:C3:85)

2022-12-18 00:20:56	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3031::ac43:93e6:443
2022-12-18 00:09:35	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	laurasweeney.us
2022-12-18 00:04:56	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 64, u'compromised_ 000000000046}")\n "iexplore.exe" touched "CImeCommonAPI Class" (Path: "HKLM\\SOFTWARE\\CLASSES\\CLSID\\{17FB3711-DE14-477F-8B81-32A9C C000-000000000046}")\n "iexplore.exe" touched "CLSID_ConditionAttribute" (Path: "HKLM\\SOFTWARE\\CLASSES\\CLSID\\{18907F3B-9AFB-4F87- u'Antivirus vendors marked dropped file "urlblockindex_1_.bin" as clean (type is "data")'}, {u'category': u'General', u'origin': u'Ne "\\Sessions\\1\\BaseNamedObjects\\Local\\VERMGMTBlockListFileMutex"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_FILEMAPSWITCH Windows icon resource - 1 icon 32x32"\n "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has type "MS Windows icon resource - 1 ic 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
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:80
2022-12-18 00:04:28	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	eforward1.registrar-servers.com
2022-12-18 00:09:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.10:8080
2022-12-18 00:09:52	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	bomapunorthno.ga
2022-12-18 00:31:10	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.faith
2022-12-18 00:23:00	SSL Certificate - Issued to	No	SSL Certificate Analyzer	0	0	3	0	None	C=IT,ST=Firenze,O=Register S.p.A.,CN=*.amen.fr
2022-12-18 00:14:46	Internet Name - Unresolved	No	VirusTotal	0	0	1	0	None	wasp.plague.fun
2022-12-18 00:02:48	IP Address	No	Mnemonic PassiveDNS	83	0	1	0	None	104.21.28.240
2022-12-18 00:21:44	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:4700:3031::/48
2022-12-18 00:09:00	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.1:8080
2022-12-18 00:03:28	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3222.webapps.net
2022-12-18 00:03:08	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.198
2022-12-18 00:07:19	Web Content	No	Web Spider	0	0	3	0	None	.browser { margin: 1rem; padding: 0.8rem; cursor: pointer; border-radius: 15px; font-family: -apple-system, system-ui, BlinkMacSystem
2022-12-18 00:37:46	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.0] https://www.virustotal.com/en/ip-address/188.114.96.0/information/
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	a-zoom (Net ID: 00:01:38:D4:87:A3)
2022-12-18 00:30:49	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.app Registry Domain ID: 2CB67ED35-APP Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godadc PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Cou on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.101domain.com Name Server: ns2. restrict or deny your access to the Whois database, and may modify these terms at any time. Domain Name: plague.app Registry Domain I Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext to these terms and limitations of warranty. In particular, you agree not to use this data to allow, enable, or otherwise support the
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Apple Network 3668a9 (Net ID: 00:02:2D:00:C6:8F)
2022-12-18 00:26:05	Country	No	Country Name Extractor	0	0	6	0	None	Italy
2022-12-18 00:09:39	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.9:8443
2022-12-18	Malicious Internet	Yes	Cleanbrowsing.org	0	1	2	0	None	Blocked by Cleanbrowsing.org [www.zerotwo-best-waifu.online]

00:10:38	Name								
2022-12-18 00:13:15	Affiliate Description - Abstract	No	DuckDuckGo	0	0	2	0	None	Cloudflare, Inc. is an American content delivery network and DDoS mitigation company, founded in 2009. It primarily acts as a reverse
2022-12-18 00:21:54	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-(
2022-12-18 00:13:50	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	contact@whoisdefender.org
2022-12-18 00:21:20	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:03:10	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	1	0	None	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Organization Validation Secure Server CA
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:8880
2022-12-18 00:21:10	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [81.88.52.232] https://www.virustotal.com/en/ip-address/81.88.52.232/information/
2022-12-18 00:27:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.48.101:993
2022-12-18 00:25:52	Physical Location	No	MetaDefender	0	0	2	0	None	Medellin, Colombia
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet55FA (Net ID: 00:01:36:59:55:F8)
2022-12-18 00:09:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.0:80
2022-12-18 00:21:09	Netblock Membership	No	Censys	0	0	2	0	None	188.114.96.0/24
2022-12-18 00:21:51	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T20:48:45.183Z", "ip": "172.67.137.37", "location_updated_at": "2022-12-14T08:26:53.936631Z", "autonom "www.anomandaris.eu": {"record_type": "A", "resolved_at": "2022-11-30T14:44:35.292184349Z"}, "www.nocktech.com": {"record_type": "A", {"record_type": "A", "resolved_at": "2022-12-06T13:31:57.111320381Z"}, "ridddovencomp.cf": {"record_type": "A", "resolved_at": "2022- 30T16:44:46.486529899Z"}, "fasthighoubudho.gq": {"record_type": "A", "resolved_at": "2022-12-10T14:33:48.548055558Z"}, "cdn-5.mymorki 24T12:29:33.415758516Z"}, "www.topnotchrepair.com": {"record_type": "A", "resolved_at": "2022-12-08T14:09:26.614619667Z"}, "mostoreec "alicelesley.altervista.org": {"record_type": "CNAME", "resolved_at": "2022-12-14T17:17:49.475328681Z"}, "sudaryni.ru": {"record_type "resolved_at": "2022-12-13T12:16:56.526232800Z"}, "requests.dylansheffer.app": {"record_type": "A", "resolved_at": "2022-12-08T12:05:
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	b6ee708a-8bc5-45a6-b502-f1102c10886d.id.repl.co
2022-12-18 00:09:48	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	autodiscover.pungostrawberryfestival.info
2022-12-18 00:04:01	Physical Location	No	ipstack	0	0	2	0	None	United States
2022-12-18 00:03:35	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3239.webapps.net
2022-12-18 00:04:45	Raw Data from RIRs	No	Maltiverse	3	0	2	0	None	{u'last_updated': u'2017-02-17 00:00:00', u'classification': u'neutral', u'asn_country_code': u'US', u'creation_time': u'2021-03-04 1
2022-12-18 00:08:36	Netblock Membership	No	RIPE	3	0	2	0	None	81.88.48.0/20
2022-12-18 00:09:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.10:80
2022-12-18 00:21:51	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:04:24	Linked URL - Internal	No	Hybrid Analysis	1	0	1	0	None	http://20.224.2.213/
2022-12-18 00:26:49	Similar Domain - Whois	No	Whois	0	0	2	0	None	DOMAIN NAME: plague.pl registrant type: organization nameservers: ns0.wixdns.net. ns1.wixdns.net. created: 2019.07.26 20:05:17 last m
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	webpersonaspichincha1.webpichinch.repl.co

2022-12-18 00:03:10	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.235
2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://wasp.plague.fun/inject
2022-12-18 00:04:28	DNS SPF Record	No	DNS Raw Records	0	0	1	0	None	v=spf1 include:spf.efwd.registrar-servers.com ~all
2022-12-18 00:22:14	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-(
2022-12-18 00:02:47	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 0f:0e:0e:28:f1:c6:cb:2f:ce:67:1d:a6:c8:b8:7a:b2 Signature Algorithm: ecdsa-with-SH Constraints: critical CA:FALSE CT Precertificate Poison: critical NULL Signature Algorithm: ecdsa-with-SHA256 30:45:02:20:6f:73:02:9b
2022-12-18 00:16:26	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	sni.cloudflaressl.com
2022-12-18 00:24:06	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	support@lovelytab.com
2022-12-18 00:08:39	Physical Location	No	LeakIX	0	0	1	0	None	Campinas, Sao Paulo, Brazil
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	iz-wpa (Net ID: 00:01:8E:1A:64:A6)
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	q8k.qw653bv.repl.co
2022-12-18 00:02:39	IP Address	No	SpiderFoot UI	16	0	0	0	None	20.224.2.213
2022-12-18 00:09:22	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.6:443
2022-12-18 00:21:41	BGP AS Membership	No	Censys	0	0	2	0	None	8075
2022-12-18 00:22:29	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.net
2022-12-18 00:18:04	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.0:8443
2022-12-18 00:07:06	Web Content Type	No	Web Spider	0	0	2	0	None	text/html; charset=utf-8
2022-12-18 00:06:33	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.0:8443
2022-12-18 00:06:31	Company Name	No	Company Name Extractor	0	0	3	0	None	Cloudflare\, Inc.
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:2082
2022-12-18 00:04:01	Country	No	Country Name Extractor	0	0	2	0	None	United States
2022-12-18 00:29:09	Similar Domain - Whois	No	Whois	0	0	2	0	None	Domain name: plague.org.uk Data validation: Nominet was able to match the registrant's name and address against a 3rd party data sour
2022-12-18 00:04:11	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:04:38	Raw Data from RIRs	No	Maltiverse	0	0	2	0	None	{u'asn_registry': u'ripencc', u'country_code': u'US', u'classification': u'whitelist', u'asn_country_code': u'US', u'address': u'101 30 09:59:00', u'description': u'Anonymisation Services', u'last_seen': u'2022-03-10 11:59:00'}, {u'count': 1, u'source': u'Maltiverse
2022-12-18 00:10:49	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 configurati
2022-12-	Internet	No	DNS Resolver	0	0	2	0	None	atlas.plague.fun

18 00:08:45	Name - Unresolved								
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	wilson (Net ID: 00:02:2D:08:06:B3)
2022-12-18 00:06:04	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 16, u'threat_score': None, u'compromis 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'descr Data\\Default\\Cache\\Cache_Data\\f_00023e]- [targetUID: 00000000-00001204]\n "manifest.fingerprint" has type "ASCII text with no lir [targetUID: 00000000-00005232]\n "Last Browser" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Last Browser] u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 0, u'type': 2, u'description': u'Pattern match: "https://nac [%TEMP%\\5232_1843406595\\edge_tracking_page_validator.js]- [targetUID: 00000000-00005232]\n Dropped file: "shopping_iframe_driver.js 00000000-00005232-00000BE4-9206691908\n "C:\\Users\\HAPUBWS\\AppData\\Local\\Microsoft\\Edge\\User Data\\Default\\EdgePushStorageWith
2022-12-18 00:13:15	Affiliate Description - Category	No	DuckDuckGo	0	0	2	0	None	Freedom of speech in the United States
2022-12-18 00:02:44	Linked URL - Internal	No	grep.app	1	0	1	0	None	https://atlas.plague.fun/register&
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:80
2022-12-18 00:03:31	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3229.webapps.net
2022-12-18 00:24:58	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.187
2022-12-18 00:21:10	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)
2022-12-18 00:05:58	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	stream.plague.fun
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	denis (Net ID: 00:01:46:02:C4:4C)
2022-12-18 00:09:44	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	amabintio.cf
2022-12-18 00:06:35	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 16, u'threat_score': None, u'compromis u'name': u'Contacts server', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'r 3007000"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\load_statistics.db-wal]- [targetUID: 00000000-00007412]\n ' Data\\Default\\e693b8a0-e037-472a-9e02-ee8a1e572700.tmp]- [targetUID: 00000000-00007412]\n "edge_driver.js" has type "UTF-8 Unicode t Notifications\\LOG]- [targetUID: 00000000-00007412]\n "21f69060-82d1-4e71-9964-fc9ef288e479.tmp" has type "UTF-8 Unicode text with ve u'description': u'0/90 Antivirus vendors marked sample as malicious (0% detection rate)'}, {u'category': u'Unusual Characteristics', u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-1', u'name': u'Drops executable files', u'attck_id_wi
2022-12-18 00:25:39	Physical Location	No	MetaDefender	0	0	2	0	None	Medellin, Colombia
2022-12-18 00:19:03	Physical Location	No	ipapi.co	1	0	3	0	None	Florence, Tuscany, 52, Italy, IT
2022-12-18 00:03:30	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3227.webapps.net
2022-12-18 00:17:21	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [104.21.28.240] https://www.virustotal.com/en/ip-address/104.21.28.240/information/
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	Spotify (Category: music) https://open.spotify.com/user/rasputain
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:2053
2022-12-18 00:02:45	SSL Certificate - Issued to	No	CertSpotter	0	0	1	0	None	CN=*.misogyny.wtf
2022-12-18 00:06:02	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	registrar-servers.com
2022-12-	Open TCP	No	LeakIX	0	0	2	0	None	

18 00:08:54	Port								172.67.147.230:443
2022-12-18 00:18:28	Affiliate - Internet Name	No	DNS Resolver	1	0	2	0	None	webmail-fr.setupdns.net
2022-12-18 00:04:28	Email Gateway (DNS MX Records)	No	DNS Raw Records	0	0	1	0	None	eforward3.registrar-servers.com
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	vlidainfobanc.winuserfonbanco.repl.co
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	ecuadopichi.ecuado30499f.repl.co
2022-12-18 00:03:08	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:11:01	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: plague.ai Registry Domain ID: 908327_nic_ai Registry WHOIS Server: whois.nic.ai Creation Date: 2020-02-25T16:54:28.932Z BillingCity: Reykjavik BillingState/Province: Capital Region BillingPostal Code: 101 BillingCountry: IS BillingPhone: +354.4212434 Bi +1.6613102107 Registry RegistrantID: SnEsi-ZeMmq RegistrantName: Redacted for Privacy RegistrantOrganization: Privacy service provide Name Server: ns2.dan.com DNSSEC: unsigned >>> Last update of WHOIS database: 2022-12-17T14:55:15.937Z <<< For more information on Who
2022-12-18 00:05:45	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u' "IsoScope_cec_IESQMMUTEX_0_331"'}, {u'category': u'General', u'origin': u'Binary File', u'identifier': u'binary-16', u'name': u'Drops u'binary-37', u'name': u'Drops files inside appdata directory', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'cape datablocks 0x1 compression"'}, {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'na [%APPDATA%\\Microsoft\\Windows\\Cookies\\F9DXFO4E.txt]- [targetUID: 00000000-00003308]\n "search__0633EE93-D776-472f-A0FF-E1416B8B2E3 u'threat_level': 0, u'type': 2, u'description': u'Pattern match: "https://lightsalmonstickyopenlook.eberech.repl.co/#andrew.kwan%40ta "http://lightsalmonstickyopenlook.eberech.repl.co" as malicious (8% detection rate)\n 7/91 reputation engines marked "https://lightsa
2022-12-18 00:11:07	Similar Domain - Whois	No	Whois	3	0	2	0	None	%% %% This is the AFNIC Whois server. %% %% complete date format: YYYY-MM-DDThh:mm:ssZ %% %% Rights restricted by copyright. %% See h registrar: EURODNS S.A. changed: 2015-09-24T11:47:25Z anonymous: NO obsoleted: NO eppstatus: associated eppstatus: active eligstatus:
2022-12-18 00:12:37	Physical Location	No	ipapi.co	1	0	2	0	None	Kansas City, Missouri, MO, United States, US
2022-12-18 00:03:30	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3226.webapps.net
2022-12-18 00:09:53	Malicious IP on Same Subnet	Yes	abuse.ch	0	0	2	0	None	abuse.ch SSL Blacklist (IP) [4.224.0.0/12] https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
2022-12-18 00:03:08	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	hook.plague.fun
2022-12-18 00:25:36	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-178.w90-116.abo.wanadoo.fr
2022-12-18 00:04:22	Raw Data from RIRs	No	Hybrid Analysis	0	0	1	0	None	{u'count': 1, u'search_terms': [{u'id': u'host', u'value': u'20.224.2.213'}], u'result': [{u'environment_id': 160, u'job_id': u'63825
2022-12-18 00:02:39	Internal SpiderFoot Root event	No	SpiderFoot UI	15	0	0	0	None	plague.fun,misogyny.wtf,rasputain.fr,zerotwo-best-waifu.online,137.117.157.128,20.195.209.219,4.228.83.86,40.113.112.131,51.103.210.2
2022-12-18 00:21:54	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-O
2022-12-18 00:03:12	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	api.plague.fun
2022-12-18 00:07:18	HTTP Status Code	No	Web Spider	0	0	3	0	None	200
2022-12-18 00:08:39	Raw Data from RIRs	No	LeakIX	0	0	1	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'4.228.83.86', u'vendor': u'', u'port': u'80', u'transport': {u'region_iso_code': u'BR-SP', u'country_iso_code': u'BR', u'city_name': u'Campinas', u'location': {u'lat': -22.9035, u'lon': -47.056 {u'content-length': u'50', u'server': u'Werkzeug/2.2.2 Python/3.10.0'}, u'length': 0, u'favicon_hash': u'', u'root': u''}, u'tags': [
2022-12-18 00:06:52	Malicious IP Address	Yes	Internet Storm Center	0	1	2	0	None	Internet Storm Center [188.114.96.0] https://isc.sans.edu/api/ip/188.114.96.0

2022-12-18 00:21:37	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["68"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Keep_Alive": "DISPLAY_UTF8", "X_Powered_By": "DISPLAY_UTF
2022-12-18 00:21:17	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-O
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:06:00	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	registrar-servers.com
2022-12-18 00:06:58	Malicious IP Address	Yes	Internet Storm Center	0	1	2	0	None	Internet Storm Center [188.114.97.1] https://isc.sans.edu/api/ip/188.114.97.1
2022-12-18 00:03:17	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-106.w90-116.abo.wanadoo.fr
2022-12-18 00:16:04	Malicious IP Address	Yes	VirusTotal	0	1	1	0	None	VirusTotal [20.195.209.219] https://www.virustotal.com/en/ip-address/20.195.209.219/information/
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date"
2022-12-18 00:06:31	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.147.230:443
2022-12-18 00:21:20	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date"
2022-12-18 00:21:13	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:
2022-12-18 00:04:11	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	sni.cloudflaressl.com
2022-12-18 00:21:13	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-O
2022-12-18 00:16:57	Web Content	No	Web Spider	3	0	2	0	None	<!DOCTYPE html> <html> <head> <meta http-equiv="content-type" content="text/html; charset=utf-8;" /> <meta http-equiv="content-langua
2022-12-18 00:04:00	Country	No	Country Name Extractor	0	0	2	0	None	United States
2022-12-18 00:14:46	Linked URL - Internal	No	Web Spider	0	0	2	0	None	https://rasputain.fr/
2022-12-18 00:06:06	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:15:47	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	4	0	None	keep-alive: timeout=5
2022-12-18 00:32:33	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.154:443
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpeedStream (Net ID: 00:01:24:F0:B4:05)
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:27	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3037::6815:13f3:443
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:2082
2022-12-18 00:09:11	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.190.129:8443
2022-12-18 00:18:23	Affiliate - Domain Name	No	DNS Resolver	0	0	3	0	None	securemail.pro
2022-12-18 00:27:08	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.ro

2022-12-18 00:25:32	Physical Location	No	MetaDefender	0	0	2	0	None	Medellin, Colombia
2022-12-18 00:16:59	Web Content	No	Web Spider	1	0	4	0	None	@import url("/css/vendor/bootstrap/bootstrap.min.css"); @import url("/css/register/base_buttons.css"); @import url("/css/register/for 15px; color:#444; height: 30px; outline: none; transition-duration: 0.2s; transition-timing-function: cubic-bezier(0.4, 0, 0.2, 1);] group.btn-group input[type="radio"]:checked + label span{ background-color:#449CFA; } .choice-group.btn-group input[type="radio"] + l margin-bottom: 0;*/ /*min-height: 100%; *//* Fallback for vh unit */ /*min-height: 100vh;*/ /* You might also want to use 'height' pr dotted #ccc; display: inline-block; margin: 30px 15px 0; padding: 20px 0 0; width: 95%; } .footer h4 { font-size: 13px; } .footer p { position: relative; } .promo{ float: left; width:100% } .choice-group.btn-group a { width: 100%; max-width: 100%; display: inline; }
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:21:17	Netblock Membership	No	Censys	0	0	2	0	None	188.114.96.0/24
2022-12-18 00:18:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.17:443
2022-12-18 00:30:51	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.bar
2022-12-18 00:09:29	Open TCP Port	No	LeakIX	0	0	2	0	None	81.88.52.232:80
2022-12-18 00:08:22	Physical Location	No	Fraudguard	0	0	1	0	None	Brazil, Sao Paulo, Campinas
2022-12-18 00:13:30	Internet Name	No	DNS Brute-forcer	6	1	1	0	None	mail.zerotwo-best-waifu.online
2022-12-18 00:09:14	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.19.243:8443
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:09:15	Open TCP Port	No	LeakIX	0	0	2	0	None	20.226.83.185:80
2022-12-18 00:23:32	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	webmail-fr.setupdns.net. 900 IN CNAME webmail-fr.securemail.pro.
2022-12-18 00:03:11	Affiliate - Domain Name	No	DNS Resolver	2	0	3	0	None	wanadoo.fr
2022-12-18 00:18:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.8:8080
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:09:19	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.137.37:443
2022-12-18 00:27:29	Physical Location	No	MetaDefender	0	0	2	0	None	Medellin, Colombia
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	bancolombiaeravistuala.sucusalvirtual.repl.co
2022-12-18 00:06:54	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'c u'"687141682008705833.16848724.repl.co"\n "nam12.safelinks.protection.outlook.com"\n "seeklogo.com"\n "www.easygameitems.com"\n "x1.c "IsoScope_fd4_ConnHashTable<4052>_HashTable_Mutex"\n "Local\\VERMGMTBlockListFileMutex"\n "Local\\URLBLOCK_HASHFILESWITCH_MUTEX"\n "L u'description': u'"57C8EDB95DF3F0AD4EE2DC2B8CFD4157" has type "Microsoft Cabinet archive data 4817 bytes 1 file"\n "77EC63BDA74BD0D0E "77EC63BDA74BD0D0E0426DC8F8008506" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\77EC63BDA74E "5A957D6E16B7CF49932C9515784473F1" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\5A957D6E16E url=https%3A%2F%2F687141682008705833.16848724.repl.co%2F&data=05%7C01%7C%7C8424604cfc5e4768653f08daad5eff12%7C84df9e7fe9f640afb435aaa
2022-12-18 00:09:35	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	late-recipe-06ac.phonene.workers.dev
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:25:07	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	81.88.58.186
2022-12-18 00:09:37	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.3:443

2022-12-18 00:07:49	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:2c:cd:9b:50:65:02:e8:a9:66:93:11:97:33:8f:e3:ed:9b Signature Algorithm: sha256W SHA256 30:45:02:21:00:C3:25:CA:E0:91:C9:7B:9B:32:99:32: 0F:57:E2:A5:48:D4:29:C0:95:B6:AC:62:47:D9:B4:27: 82:7B:81:DD:35:02:20:04:E1:4
2022-12-18 00:16:36	Physical Location	No	numverify	0	0	3	0	None	FR
2022-12-18 00:41:23	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.13] https://www.virustotal.com/en/ip-address/188.114.96.13/information/
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	LF-X1U.00014A10EF0C (Net ID: 00:01:4A:10:EF:0C)
2022-12-18 00:20:59	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:8080
2022-12-18 00:10:04	Physical Location	No	URLScan.io	0	0	1	0	None	FR
2022-12-18 00:18:44	Malicious IP on Same Subnet	Yes	Emerging Threats	0	0	2	0	None	emergingthreats.net [20.192.0.0/10] https://rules.emergingthreats.net/blockrules/compromised-ips.txt
2022-12-18 00:13:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	domainabuse@tucows.com
2022-12-18 00:19:17	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [u'banker', u'emotet'], u'crowdstrike_ai': None, u'total_processes': 7, u'threat_score' }\n}\nvar d = o.replace("nm.c({", "");\nvar D = "year fuck foundation familiar radio association technique affair finish";\nvar xn7 = priority environmental brother thank stand";\n }\n}\nvar sHVH = "b+By";\nvar gWh = "conversation pour team table link he requirement' fix accident evening past quality rest formal joy cross once comment smile law dear";\nvar LS0 = "UU8g-5;r";\nvar w0Y = "aQZbj:zsE7S1 "");\nfor (var YM = 2563; YM < 588; $i += 669) {\n for (var jV = 2526; jV < 159; $i += 145) {\n var FcRm$lc = "only charity rai 5419840;\nvar RRWYR = "NP2[K)Ol*J>Uz8r?V.OYW6bGYdBb6T";\nvar DhSlzk = fO4.replace("cu", "");\nvar jWm = ">08%AFogTwb#]tIC2Stt~@ "WGWB[(QxV@Y,$F=0;}9yTa@RJ{-U";\nvar N06rEQAE = TnSKC4v + d;\nfor (var u60a = 1552; u60a < 537; $i += 743) {\n var aK3h = 2358301;
2022-12-18 00:03:08	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	atlas.plague.fun
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:8880
2022-12-18 00:21:44	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T21:38:21.633Z", "ip": "2606:4700:3031::6815:7b3", "location_updated_at": "2022-12-15T10:39:11.585922Z "pghbusinessplus.com": {"record_type": "AAAA", "resolved_at": "2022-12-03T13:54:45.868033682Z"}, "cpcalendars.nocktech.com": {"record {"record_type": "CNAME", "resolved_at": "2022-12-07T13:48:57.083633204Z"}, "lafatipitin.buzz": {"record_type": "AAAA", "resolved_at": "resolved_at": "2022-12-15T14:53:07.974813782Z"}, "hotel-behringer.de": {"record_type": "AAAA", "resolved_at": "2022-12-14T22:23:17.1 "www.fvbowling.com.ve.cdn.cloudflare.net": {"record_type": "AAAA", "resolved_at": "2022-12-01T15:43:49.524130454Z"}, "rjoutdoorsoluti {"record_type": "AAAA", "resolved_at": "2022-11-16T17:08:14.361545226Z"}, "cortiolamtapersres.ml": {"record_type": "AAAA", "resolved_ 14T15:20:56.567076509Z"}, "pl.ukrainianwomen.date": {"record_type": "AAAA", "resolved_at": "2022-12-06T14:50:18.281969258Z"}, "moodle
2022-12-18 00:08:52	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.28.240:8080
2022-12-18 00:03:01	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.97
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	101 (Net ID: 00:01:03:7B:E0:44)
2022-12-18 00:09:24	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.7:8080
2022-12-18 00:03:08	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.195
2022-12-18 00:12:04	Country	No	Country Name Extractor	0	0	3	0	None	United States
2022-12-18 00:11:08	Similar Domain - Whois	No	Whois	3	0	2	0	None	Domain Name: PLAGUE.COM Registry Domain ID: 19383017_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namebright.com Registrar URL: http ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information abo Registrar URL: http://www.NameBright.com Updated Date: 2021-06-09T00:00:00.000Z Creation Date: 2000-02-08T11:36:34.000Z Registrar Reg State/Province: G2 Tech Postal Code: 6440 Tech Country: NZ Tech Phone: +1.9138710454 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Ema

2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://wasp.plague.fun/inject/MTJ8Vp5aynR51YMM
2022-12-18 00:31:12	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@porkbun.com
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:2096
2022-12-18 00:18:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.9:8080
2022-12-18 00:02:50	IP Address	No	Mnemonic PassiveDNS	57	0	1	0	None	104.21.7.179
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	2WIRE522 (Net ID: 00:01:E6:93:CB:2D)
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	niftyoblongautomatedinformationsystem.login879.repl.co
2022-12-18 00:21:02	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:16:53	Affiliate - Company Name	No	Company Name Extractor	0	0	4	0	None	NameCheap, Inc.
2022-12-18 00:03:06	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.185
2022-12-18 00:04:45	Malicious IP Address	Yes	Maltiverse	0	1	2	0	None	Maltiverse [104.21.19.243]
2022-12-18 00:09:52	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	blog.ic-agency.com
2022-12-18 00:08:38	Physical Location	No	LeakIX	0	0	1	0	None	Campinas, Sao Paulo, Brazil
2022-12-18 00:11:20	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	obf.plague.fun
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:2053
2022-12-18 00:21:20	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:02:43	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:d0:d1:a1:cc:7c:20:ed:eb:01:fc:85:dd:45:cc:e5:1b:da Signature Algorithm: sha256W with-SHA256 30:45:02:21:00:A9:DD:3E:19:3D:08:47:5F:9B:B1:90: AB:C2:AD:E2:91:05:EF:EF:95:99:23:9E:12:BB:18:C5: F2:98:2C:7F:FF:02:20:30
2022-12-18 00:03:05	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.179
2022-12-18 00:04:09	Raw Data from RIRs	No	Hybrid Analysis	0	0	1	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised u'"\\Sessions\\1\\BaseNamedObjects\\IsoScope_b40_IESQMMUTEX_0_519"\n "Local\\InternetShortcutMutex"\n "{5312EE61-79E3-4A24-BFE1-132B8 u'relevance': 3, u'threat_level': 0, u'type': 8, u'description': u'Dropped file: "5DCLXO04.txt" - Location: [%APPDATA%\\Microsoft\\Wi has type "HTML document ASCII text with CRLF line terminators"- [targetUID: N/A]\n "en-US.4" has type "data"- Location: [%LOCALAPPDAT 2, u'description': u'Pattern match: "http://misogyny.wtf:2020/copy"\n Pattern match: "http://misogyny.wtf"'}, {u'category': u'Network u'malicious', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 2, u'type': 12, u'description': u'No specific Control', u'informative_identifiers_count': 0, u'suspicious_identifiers_count': 0}], u'certificates': [], u'hosts': [u'20.226.83.185'
2022-12-18 00:21:02	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:03	Web Server	No	Web Server Identifier	0	0	4	0	None	Werkzeug/2.2.2 Python/3.9.11
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:443
2022-12-	Raw Data	No	ipapi.co	0	0	1	0	None	

18 00:11:56	from RIRs								{u'region_code': u'SP', u'country_tld': u'.br', u'ip': u'4.228.83.86', u'currency_name': u'Real', u'currency': u'BRL', u'country_popu
2022-12-18 00:20:46	Physical Location	No	Censys	0	0	1	0	None	Amsterdam, North Holland, 1012, Netherlands, Europe
2022-12-18 00:22:08	Malicious Internet Name	Yes	Cleanbrowsing.org	0	1	2	0	None	Blocked by Cleanbrowsing.org [ftp.zerotwo-best-waifu.online]
2022-12-18 00:28:44	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.tv
2022-12-18 00:32:27	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.wtf Registry Domain ID: 91b300be317945ac9a02c110d39076e9-DONUTS Registrar WHOIS Server: whois.donuts.co Registrar Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query t Identity Digital does not guarantee its accuracy. Users accessing the Identity Digital Whois service agree to use the data only for l to contact the registrant, please refer to the Whois records available through the registrar URL listed above. Access to non-public d Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar o Server: ns-cloud-e1.googledomains.com Name Server: ns-cloud-e2.googledomains.com Name Server: ns-cloud-e3.googledomains.com Name Serv downtime during production or OT&E maintenance periods. Queries to the Whois services are throttled. If too many queries are receivec
2022-12-18 00:12:06	Country	No	Country Name Extractor	0	0	3	0	None	United States
2022-12-18 00:04:10	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	188.114.96.0:443
2022-12-18 00:09:51	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	blinracinil.tk
2022-12-18 00:04:10	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3
2022-12-18 00:13:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.128:443
2022-12-18 00:13:51	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@godaddy.com
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:2095
2022-12-18 00:21:30	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T22:57:29.991Z", "ip": "172.67.190.129", "location_updated_at": "2022-12-11T04:34:39.903276Z", "autonc {"record_type": "A", "resolved_at": "2022-10-13T09:23:32.675728636Z"}, "abruspowolfcmomel.cf": {"record_type": "A", "resolved_at": "2 12-09T14:11:32.965062841Z"}, "cpanel.northedgearchitecture.co.uk": {"record_type": "A", "resolved_at": "2022-12-09T16:47:00.725482235 "www.dogsciencesays.com": {"record_type": "A", "resolved_at": "2022-12-06T13:34:34.004464956Z"}, "www.hogroastcirencester.com": {"rec "2022-12-10T12:09:48.597886439Z"}, "ebkingbet.com": {"record_type": "A", "resolved_at": "2022-12-17T13:16:29.923192379Z"}, "6v7truste "ws.alfons.education": {"record_type": "A", "resolved_at": "2022-11-25T14:46:03.860725031Z"}, "storytel.us": {"record_type": "A", "re vocations-ok.live": {"record_type": "A", "resolved_at": "2022-12-07T15:43:19.629791588Z"}, "jitedeciqibib.rest": {"record_type": "A",
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet2EE2 (Net ID: 00:01:36:5B:2E:E0)
2022-12-18 00:06:20	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "Local\\!BrowserEmulation!SharedMemory!Mutex"\n "Local\\VERMGMTBlockListFileMutex"\n "\\Sessions\\1\\BaseNamedObjects\\UpdatingNewTab u'origin': u'Binary File', u'identifier': u'binary-5', u'name': u'Drops cabinet archive files', u'attck_id_wiki': None, u'threat_leve [%APPDATA%\\Microsoft\\Windows\\Cookies\\SLFH63TP.txt]- [targetUID: 00000000-00002856]\n Dropped file: "OQUWGK48.txt" - Location: [%A compression"- Location: [%TEMP%\\Cab2781.tmp]- [targetUID: 00000000-00002856]\n "~DFCF87F3A035D51E0C.TMP" has type "data"- Location: u'Network Related', u'origin': u'String', u'identifier': u'string-102', u'name': u'Decrypted SSL network traffic', u'attck_id_wiki': u'interesting': False, u'error_type': None, u'state': u'SUCCESS', u'entrypoint': None, u'mitre_attcks': [], u'certificates': [], u'hc
2022-12-18 00:02:39	Internet Name	No	SpiderFoot UI	49	0	0	0	None	zerotwo-best-waifu.online
2022-12-18 00:02:47	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2022-12-18 00:06:31	Company Name	No	Company Name Extractor	4	0	2	0	None	Cloudflare\, Inc.
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	2WIRE623 (Net ID: 00:00:85:F5:03:9F)
2022-12-18 00:19:14	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [u'miner'], u'crowdstrike_ai': None, u'total_processes': 10, u'threat_score': 100, u'cc "\\Sessions\\1\\BaseNamedObjects\\Global\\3a886eb8-fe40-4d0a-b78b-9e0bcb683fb7"'}, {u'category': u'General', u'origin': u'Registry Ac 00002280)\n Spawned process "netsh.exe" with commandline "advfirewall firewall add rule name="Host-process for services of ..." (UID: {645FF040-5081-101B-9F08-00AA002F954E}\\SHELLFOLDER")\n "<Input Sample>.exe" touched "Control Panel" (Path: "HKCU\\CLSID\\{26EE0668-A (Path: "HKCU\\CLSID\\{8FD8B88D-30E1-4F25-AC2B-553D3D65F0EA}\\SHELLFOLDER")\n "<Input Sample>.exe" touched "CLSID_SearchHome" (Path: "

									Target', u'identifier': u'target-67', u'name': u'Process launched with changed environment', u'attck_id_wiki': None, u'threat_level_h "cmd.exe" with commandline "/C move /Y "%TEMP%\\srhdkgl.exe" %WINDIR%\\system32\\aweovprv\\" (UID: 00026065-00004064)\n Spawned proce
2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://wasp.plague.fun/inject/TJlP9P7aJ8QTzB98
2022-12-18 00:11:55	Raw Data from RIRs	No	ipapi.co	0	0	1	0	None	{u'region_code': u'SP', u'country_tld': u'.br', u'ip': u'20.195.209.219', u'currency_name': u'Real', u'currency': u'BRL', u'country_p
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	lessbancodaviviendadaviplatacogreater.ebanking.repl.co
2022-12-18 00:03:13	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-96.w90-116.abo.wanadoo.fr
2022-12-18 00:10:05	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	https://zerotwo-best-waifu.online/
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:12:34	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'cour
2022-12-18 00:18:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.10:8443
2022-12-18 00:20:46	Netblock Membership	No	Censys	0	0	1	0	None	40.112.0.0/13
2022-12-18 00:09:36	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	qauhixyp.ga
2022-12-18 00:21:27	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T20:22:45.965Z", "ip": "2606:4700:3037::6815:13f3", "location_updated_at": "2022-12-16T19:03:06.188736 25T17:18:30.899764295Z"}, "rouzzz.tk": {"record_type": "AAAA", "resolved_at": "2022-11-27T16:33:19.875741780Z"}, "croqdoudou68.fr": { "torri.pl": {"record_type": "AAAA", "resolved_at": "2022-12-11T08:23:49.046212456Z"}, "athsnydam.tk": {"record_type": "AAAA", "resolv online-st0cktrading-esgo-ok.live": {"record_type": "AAAA", "resolved_at": "2022-12-04T15:28:45.315201663Z"}, "squarerxylawthoulich.tk "resolved_at": "2022-12-14T15:51:47.264561473Z"}, "www.nflfootballjerseys.us.org": {"record_type": "AAAA", "resolved_at": "2022-11-26 {"record_type": "AAAA", "resolved_at": "2022-11-21T13:46:57.180736459Z"}, "www.thespruces.us": {"record_type": "AAAA", "resolved_at": {"record_type": "AAAA", "resolved_at": "2022-11-11T13:12:29.864284296Z"}, "trx.video": {"record_type": "AAAA", "resolved_at": "2022-1
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F0:17:4A)
2022-12-18 00:03:27	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	195.204.149.34.bc.googleusercontent.com
2022-12-18 00:21:09	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:
2022-12-18 00:08:54	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.147.230:80
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	05vb65df.qw653bv.repl.co
2022-12-18 00:12:10	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 16, u'threat_score': 35, u'compromised 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'd Data\\14a38b17-41cf-42dd-9514-1efd2c164496.tmp]- [targetUID: 00000000-00004208]\n "shopping_iframe_driver.js" has type "ASCII text wi 9db8-fa52080a5706.tmp]- [targetUID: 00000000-00004208]\n "a9ec7364-a580-4497-9362-d7a9dd9d7694.tmp" has type "UTF-8 Unicode text with u'type': 8, u'description': u'Dropped file: "shopping_iframe_driver.js" - Location: [%TEMP%\\4208_838907974\\shopping_iframe_driver.j (console) x86-64 for MS Windows"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\WidevineCdm\\4.10.2557.0_platform_specific "%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Subresource Filter\\Unindexed Rules\\10.34.0.33\\LICENSE"\n Potential IP "188.114.96.3"
2022-12-18 00:12:11	Physical Location	No	ipapi.co	0	0	2	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	7717 7361 (Net ID: 00:00:C5:FC:FE:34)
2022-12-18 00:28:40	Physical Location	No	MetaDefender	0	0	3	0	None	Firenze, Italy
2022-12-18 00:18:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.11:8443
2022-12-	SSL	No	Certificate	1	0	1	0	None	

18 00:02:57	Certificate - Raw Data		Transparency						Certificate: Data: Version: 3 (0x2) Serial Number: 04:d0:d1:a1:cc:7c:20:ed:eb:01:fc:85:dd:45:cc:e5:1b:da Signature Algorithm: sha256W 7d:95:91:4d:9a:d7:92:5a:20:5f:df:3a:f7:70:07:52:af:26: e5:44:cf:29:99:36:a2:f4:f0:92:fa:35:dd:ae:62:10:ad:8d: 9e:95:1d:8d:12:db:7d:2a
2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F2:6F:6D)
2022-12-18 00:18:23	IP Address	No	DNS Resolver	6	0	2	0	None	195.110.124.246
2022-12-18 00:14:36	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 configurati
2022-12-18 00:21:37	Software Used	Yes	Censys	0	0	2	0	None	Express
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	lichess (Category: gaming) https://lichess.org/@/rasputain
2022-12-18 00:21:34	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-O
2022-12-18 00:25:41	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-187.w90-116.abo.wanadoo.fr
2022-12-18 00:13:35	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	noc@cloudflare.com
2022-12-18 00:07:17	Linked URL - Internal	No	Web Spider	4	0	2	0	None	http://misogyny.wtf:2020/css/index.css
2022-12-18 00:21:11	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)
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:31:07	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	support@sav.com
2022-12-18 00:18:44	Malicious IP on Same Subnet	Yes	Emerging Threats	0	0	2	0	None	emergingthreats.net [40.112.0.0/13] https://rules.emergingthreats.net/blockrules/compromised-ips.txt
2022-12-18 00:05:12	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:43:a4:7d:29:1f:15:0e:6b:ac:86:e4:4b:c0:be:69:71:a9 Signature Algorithm: sha256W 80:be:82:e8:96:f8:df:13:0f:ca:15:85:8c:8d:ca:d0:c7:67: 5f:86:6d:5d:8e:88:a2:b2:15:b1:05:8e:c8:b9:11:6d:8f:45: eb:c2:e1:17:34:0a:fb:7f
2022-12-18 00:02:44	Raw Data from RIRs	No	grep.app	0	0	1	0	None	{u'repo': {u'raw': u'billythegoat356/Atlas'}, u'total_matches': {u'raw': u'1'}, u'content': {u'snippet': u'<table class="highlight-ta
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	35ba3c6b-b09c-4896-9bf5-4c911dbcf9a0.id.repl.co
2022-12-18 00:09:15	Physical Location	No	LeakIX	0	0	2	0	None	Campinas, Sao Paulo, Brazil
2022-12-18 00:02:43	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2022-12-18 00:03:26	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	186.204.149.34.bc.googleusercontent.com
2022-12-18 00:18:46	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.20:80
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date"
2022-12-18 00:04:49	Similar Domain	Yes	Tool - DNSTwist	1	0	1	0	None	misogyn.y.wtf
2022-12-18 00:04:11	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18	Affiliate - Email	No	E-Mail Address Extractor	0	0	3	0	None	staff@eurodns.com

00:13:48	Address								
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:36:05	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.237] https://www.virustotal.com/en/ip-address/81.88.52.237/information/
2022-12-18 00:16:32	Raw Data from RIRs	No	numverify	0	0	3	0	None	{u'international_format': u'+492283296859', u'local_format': u'02283296859', u'number': u'492283296859', u'valid': True, u'line_type'
2022-12-18 00:24:57	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.182
2022-12-18 00:27:12	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.58.196:25
2022-12-18 00:14:31	Physical Location	No	ipstack	0	0	2	0	None	Colombia
2022-12-18 00:03:10	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	1	0	None	webapps.net
2022-12-18 00:07:13	Raw Data from RIRs	No	Certificate Transparency	1	0	1	0	None	[{u'not_after': u'2023-01-26T16:20:04', u'not_before': u'2022-10-28T16:20:05', u'issuer_ca_id': 183267, u'name_value': u'rasputain.fr
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	vapor (Net ID: 00:02:2D:09:FC:69)
2022-12-18 00:12:01	Raw Data from RIRs	No	ipapi.co	0	0	1	0	None	{u'region_code': u'NH', u'country_tld': u'.nl', u'ip': u'20.224.2.213', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2022-12-18 00:09:37	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.3:8443
2022-12-18 00:09:53	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	borramasciahuva.ml
2022-12-18 00:09:37	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	web3apima.cf
2022-12-18 00:20:56	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: -
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	2093-banco-personal-clien-3393.209938.repl.co
2022-12-18 00:03:06	Internet Name	No	DNS Resolver	0	0	2	0	None	misogyny.wtf
2022-12-18 00:31:43	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.nyc
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	appdaviplataco.linkbanking.repl.co
2022-12-18 00:12:33	Physical Location	No	ipapi.co	1	0	2	0	None	London, England, ENG, United Kingdom, GB
2022-12-18 00:05:37	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised u'description': u'"GET / HTTP/1.1\nAccept: text/html, application/xhtml+xml, */*\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Wi https://bancodeoccidente.portalpersonas1.repl.co/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:1 */*;q=0.5\nReferer: https://bancodeoccidente.portalpersonas1.repl.co/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6. */*;q=0.5\nReferer: https://bancodeoccidente.portalpersonas1.repl.co/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6. */*\nReferer: https://bancodeoccidente.portalpersonas1.repl.co/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Tri "user-agent: ")\n "GET /firefox-color.png HTTP/1.1\nAccept: image/png, image/svg+xml, image/*;q=0.8, */*;q=0.5\nReferer: https://banc
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:06:09	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 16, u'threat_score': 35, u'compromised "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:1900:304:WilStaging_02"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\ChromeProcessSingleto Log version 3007000"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\load_statistics.db-wal]- [targetUID: 00000000-0 Data\\Default\\Cache\\Cache_Data\\f_00023d]- [targetUID: 00000000-00005256]\n "7cce5ccc-bfea-42d5-b504-84d1d9cc49b0.tmp" has type "UT with very long lines with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Network\\b76bccfc-f81 [%TEMP%\\1900_909108262\\edge_checkout_page_validator.js]- [targetUID: 00000000-00001900]\n Dropped file: "shoppingfre.js" - Location data") in Source: 00000000-00001900-00000BE4-927066661\n "C:\\Users\\HAPUBWS\\AppData\\Local\\Microsoft\\Edge\\User Data\\Crashpad\\r
2022-12-18	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-O

00:21:30									
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	re.autecosa.repl.co
2022-12-18 00:13:35	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@cloudflare.com
2022-12-18 00:03:52	Similar Domain	Yes	Similar Domain Finder	0	0	1	0	None	zerotwo-best-waifu.online
2022-12-18 00:25:34	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-174.w90-116.abo.wanadoo.fr
2022-12-18 00:03:06	Internet Name	No	DNS Resolver	0	0	2	0	None	misogyny.wtf
2022-12-18 00:27:44	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	domainabuse@tucows.com
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	S-lan (Net ID: 00:01:24:F1:91:41)
2022-12-18 00:13:35	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	rir@cloudflare.com
2022-12-18 00:09:50	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	benimbahis64.com
2022-12-18 00:21:06	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-(
2022-12-18 00:22:14	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: -
2022-12-18 00:20:43	Internet Name	No	DNS Resolver	0	0	3	0	None	webmail.zerotwo-best-waifu.online
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:22:11	Netblock Membership	No	Censys	0	0	2	0	None	81.88.48.0/20
2022-12-18 00:07:05	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise {u'category': u'General', u'origin': u'Created Mutant', u'identifier': u'mutant-0', u'name': u'Creates mutants', u'attck_id_wiki': No archive data 61712 bytes 1 file"\n "57C8EDB95DF3F0AD4EE2DC2B8CFD4157" has type "Microsoft Cabinet archive data 4817 bytes 1 file"\n ' 00000000-00003668]\n "~DF7A8E4CFBAC14A516.TMP" has type "data"- Location: [%TEMP%\\~DF7A8E4CFBAC14A516.TMP]- [targetUID: 00000000-000 [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB606228BC7A711E]- [targ "HTTP/1.1 200 OK\nDate: Fri, 22 Jul 2022 01:56:26 GMT\nServer: Apache\nX-Powered-By: PHP/7.3.33\nUpgrade: h2,h2c\nConnection: Upgrade <xVd/9s$4R;}Q[Eh&_u;H$bGsYGTYYmrD9UE$$fC92%KkRoThJhj2!+|G3~svcNJ3g87<!"*S"7pskapMe"X`aj&!jyc8$?n| NW?b1KdfMpg3\'tSxs\n_{N>E^F\\2{tR_E
2022-12-18 00:13:45	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@godaddy.com
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:09:F8:70)
2022-12-18 00:16:59	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	55 2nd PMO (Net ID: 00:01:21:10:85:60)
2022-12-18 00:16:59	HTTP Status Code	No	Web Spider	0	0	4	0	None	200
2022-12-18 00:08:34	Netblock Membership	No	RIPE	1	0	2	0	None	34.149.0.0/16
2022-12-18 00:05:04	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 40, u'compromised_ "\\Sessions\\1\\BaseNamedObjects\\{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "Local\\InternetShortcutMutex"\n "IsoScope_e58_ConnHashTa

									"iexplore.exe" with commandline "SCODEF:3672 CREDAT:275457 /prefetch:2" (UID: 00066381-00001384)'}, {u'category': u'General', u'origi u'origin': u'String', u'identifier': u'string-7', u'name': u'Contains PDB pathways', u'attck_id_wiki': None, u'threat_level_human': u {u'category': u'General', u'origin': u'Binary File', u'identifier': u'binary-16', u'name': u'Drops files marked as clean', u'attck_id (part of module "IEFRAME.DLL")\n "iexplore.exe" wrote bytes "a035e46e" to virtual address "0x748C139C" (part of module "UXTHEME.DLL") u'type': 8, u'description': u'"77EC63BDA74BD0D0E0426DC8F8008506" has type "Microsoft Cabinet archive data 58446 bytes 1 file"\n "CabF
2022-12-18 00:07:17	HTTP Status Code	No	Web Spider	0	0	2	0	None	403
2022-12-18 00:02:50	IPv6 Address	No	Mnemonic PassiveDNS	13	0	1	0	None	2606:4700:3032::ac43:8925
2022-12-18 00:21:30	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-O
2022-12-18 00:03:25	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	183.204.149.34.bc.googleusercontent.com
2022-12-18 00:05:21	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'104.21.7.179'}], u'result': [{u'environment_id': 160, u'job_id': u'634fe
2022-12-18 00:09:33	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.27.242:8443
2022-12-18 00:04:12	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:08:aa:47:53:40:59:b8:a3:96:dc:96:87:a9:7a:35:d6:08 Signature Algorithm: ecdsa-w 00:d1:f2:c2:c9:76:cf:0c:5f:07:03:d2:2c:94:c4:a4:70:f1: 03:d1:8f:78:8a:05:22:da:d2:44:5e:4f:72:4f:1d:c1:78:0e: 9f:81:c9:b6:22:66:b7:7a
2022-12-18 00:08:27	Netblock Membership	No	RIPE	0	0	2	0	None	104.21.16.0/20
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:8080
2022-12-18 00:13:36	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	rir@cloudflare.com
2022-12-18 00:05:44	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u' "\\Sessions\\1\\BaseNamedObjects\\IsoScope_608_IE_EarlyTabStart_0xc2c_Mutex"\n "\\Sessions\\1\\BaseNamedObjects\\IsoScope_608_ConnHas u'"34.149.204.188:443"\n "104.18.10.207:443"\n "142.251.211.234:443"\n "69.16.175.42:443"\n "104.17.24.14:443"\n "142.250.217.106:443 setup 62932 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"\n "77EC63BDA74BD0D0E0426DC8F8008506" has ty [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 00000000-00002524]\n "BJIL
									{u'category': u'Network Related', u'origin': u'String', u'identifier': u'string-3', u'name': u'Found potential URL in binary/memory', detection rate)\n 7/91 reputation engines marked "https://lightsalmonstickyopenlook.eberech.repl.co" as malicious (7% detection rate)
2022-12-18 00:18:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.10:443
2022-12-18 00:12:29	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'172.67.137.37', u'currency_name': u'Dollar', u'currency': u'CAD', u'country_
2022-12-18 00:21:20	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conn
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	a-zoom (Net ID: 00:01:38:D4:87:A3)
2022-12-18 00:21:58	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:
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNet8FBA (Net ID: 00:01:36:5C:8F:B8)
2022-12-18 00:02:44	Internet Name - Unresolved	No	CertSpotter	0	0	1	0	None	hook.plague.fun
2022-12-18 00:20:52	Netblock Membership	No	Censys	0	0	1	0	None	20.192.0.0/10
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:21:54	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-O
2022-12-18 00:09:42	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.15:443
2022-12-18 00:13:46	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	abuse@namecheap.com

2022-12-18 00:21:44	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3031::6815:7b3:443
2022-12-18 00:13:15	Affiliate Description - Category	No	DuckDuckGo	0	0	2	0	None	Reverse proxy
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	redwood (Net ID: 00:01:38:85:C1:F8)
2022-12-18 00:06:39	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.es
2022-12-18 00:22:21	Similar Domain - Whois	No	Whois	2	0	2	0	None	Domain Name: PLAGUE.ME Registry Domain ID: D425500000338876015-AGRS Registrar WHOIS Server: whois.namecheap.com Registrar URL: www.na facsimile of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing custo by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region F
2022-12-18 00:21:13	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-O
2022-12-18 00:03:05	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	atlas.plague.fun
2022-12-18 00:09:44	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	ambidextrousthoughts.com
2022-12-18 00:38:53	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.4] https://www.virustotal.com/en/ip-address/188.114.96.4/information/
2022-12-18 00:03:05	IP Address	No	DNS Resolver	0	0	1	0	None	81.88.52.232
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:2052
2022-12-18 00:04:31	Affiliate - Internet Name - Unresolved	No	DNS Raw Records	0	0	1	0	None	spf.webapps.net
2022-12-18 00:22:14	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:2052
2022-12-18 00:03:12	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:43:e4:fc:51:db:21:42:a6:26:a1:af:57:d7:7c:1f:09:d4 Signature Algorithm: ecdsa-w with-SHA256 30:45:02:20:52:60:7D:D5:E5:D5:CA:63:59:6C:4E:65: 2B:95:7D:B8:79:E9:9C:B0:1E:EA:1B:00:44:16:69:68: A8:6F:8E:69:02:21:00:BE
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:443
2022-12-18 00:03:21	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-110.w90-116.abo.wanadoo.fr
2022-12-18 00:19:18	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [104.21.19.243] https://www.virustotal.com/en/ip-address/104.21.19.243/information/
2022-12-18 00:03:35	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3241.webapps.net
2022-12-18 00:24:58	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.185
2022-12-18 00:04:31	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	ns2.amenworld.com
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F2:68:C6)

2022-12-18 00:13:15	Affiliate Description - Category	No	DuckDuckGo	0	0	2	0	None	Internet security
2022-12-18 00:18:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.5:8080
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:21:13	Physical Location	No	Censys	0	0	2	0	None	Amsterdam, North Holland, 1012, Netherlands, Europe
2022-12-18 00:20:59	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:09:00	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'188.114.96.1', u'vendor': u'', u'port': u'443', u'transport u'country_iso_code': u'NL', u'city_name': u'Amsterdam', u'location': {u'lat': 52.3759, u'lon': 4.8975}, u'country_name': u'Netherlanc u'raw': None, u'password': u'', u'noauth': False, u'key': u''}, u'software': {u'modules': None, u'version': u'', u'os': u'', u'name': u'continent_name': u'Europe', u'region_name': u'North Holland'}, u'host': u'test5-pointg.nc-testdomain2.club', u'summary': u'Date: Tu u'6d1f2e7c9ee98731fedbc44a39cb147fd61faf135869985633f6d7099edc3d89', u'leak': {u'dataset': {u'files': 0, u'rows': 0, u'ransom_notes': charset=UTF-8\r\nTransfer-Encoding: chunked\r\nConnection: close\r\nX-Frame-Options: SAMEORIGIN\r\nCross-Origin-Embedder-Policy: requ 0}, u'type': u'', u'severity': u'', u'stage': u''}, u'event_pipeline': [u'CertStream', u'l9scan', u'tcpid', u'HttpPlugin'], u'http':
2022-12-18 00:31:35	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.ltd
2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:07:18	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'104.21.27.242'}], u'result': [{u'environment_id': 160, u'job_id': u'6398
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom1330 (Net ID: 00:01:38:92:E5:07)
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:04:00	Country	No	Country Name Extractor	0	0	2	0	None	France
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	flamboyantmicrostructs.allgominsprovin.repl.co
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2096
2022-12-18 00:04:30	DNS TXT Record	No	DNS Raw Records	0	0	1	0	None	v=spf1 include:spf.webapps.net ~all
2022-12-18 00:24:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.174
2022-12-18 00:14:05	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 protoc
2022-12-18 00:39:03	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	misogyny.com.au
2022-12-18 00:03:04	IP Address	No	DNS Resolver	14	0	1	0	None	104.21.27.242
2022-12-18 00:10:05	Physical Location	No	URLScan.io	0	0	1	0	None	IT
2022-12-18 00:04:02	Physical Location	No	ipstack	0	0	2	0	None	France
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	Chess.com (Category: gaming) https://www.chess.com/member/rasputain
2022-12-18 00:21:09	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:21:13	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-(
2022-12-18	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	pichinhsac.repl.co

00:16:46									
2022-12-18 00:20:22	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [104.21.7.179] https://www.virustotal.com/en/ip-address/104.21.7.179/information/
2022-12-18 00:13:27	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	7b20cf325f4f4ba4bc3a96b338b107cd.protect@withheldforprivacy.com
2022-12-18 00:20:42	Netblock Membership	No	Censys	0	0	1	0	None	4.224.0.0/12
2022-12-18 00:09:50	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	belssurpzysgasif.tk
2022-12-18 00:02:39	Domain Name	No	SpiderFoot UI	12	0	0	0	None	zerotwo-best-waifu.online
2022-12-18 00:04:01	Country	No	Country Name Extractor	0	0	4	0	None	France
2022-12-18 00:20:31	Raw Data from RIRs	No	LeakIX	0	0	3	0	None	{u'Services': None, u'Leaks': None}
2022-12-18 00:13:41	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	gestionndd@francetelecom.biz
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:09:43	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.3:443
2022-12-18 00:06:06	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	atlas.plague.fun
2022-12-18 00:09:42	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.15:80
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:2086
2022-12-18 00:06:29	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 15, u'threat_score': 35, u'compromised u'capec_id': None, u'attck_id': u'T1071.004', u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"http-api.livecoinwa u'Dropped files', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': "settings.dat" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Crashpad\\settings.dat]- [targetUID: 00000000- bdfac46e5306.tmp" has type "ASCII text with very long lines with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\Us Heuristic match: "tesla.event22.repl.co"\n Pattern match: "www.livecoinwatch.com"\n Heuristic match: "1t;ps_//\'tesla.e`_ent_2.repl.c 1756017086\n "C:\\Users\\HAPUBWS\\AppData\\Local\\Microsoft\\Edge\\User Data\\Crashpad\\reports" (Indicator: "microsoft\\edge\\user c
2022-12-18 00:06:51	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.137.37:8443
2022-12-18 00:21:27	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:10:49	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 4.3 Description: OpenVPN, when using a 64-bit block cipher, makes
2022-12-18 00:07:18	HTTP Headers	No	Web Spider	1	0	3	0	None	{"date": "Sun, 18 Dec 2022 00:07:18 GMT", "content-length": "207", "content-type": "text/html; charset=utf-8", "connection": "close",
2022-12-18 00:07:21	Raw Data from RIRs	No	Google	0	0	1	0	None	{'webSearchUrl': u'https://www.google.com/search?q=site:misogyny.wtf&aq=t&oe=utf-8&client=firefox-a&ie=utf-8&rls=org.mozilla%3Aen-US%
2022-12-18 00:11:02	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: PLAGUE.CC Registry Domain ID: 178127471_DOMAIN_CC-VRSN Registrar WHOIS Server: whois.dynadot.com Registrar URL: http://w information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. Veri Expiration Date: 2023-07-10T00:19:13.0Z Registrar: DYNADOT LLC Registrar IANA ID: 472 Registrar Abuse Contact Email: abuse@dynadot.co 00:23:38 -0700 <<<
2022-12-18 00:10:04	BGP AS Membership	No	URLScan.io	0	0	1	0	None	13335
2022-12-18 00:09:50	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 configurati
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec

2022-12-18 00:13:48	Web Content Language	No	Language Detector	0	0	4	0	None	English
2022-12-18 00:04:04	Web Server	No	Tool - WhatWeb	0	0	1	0	None	cloudflare
2022-12-18 00:20:56	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:21:17	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:
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:01:24:F2:E2:35)
2022-12-18 00:21:54	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:04:28	Name Server (DNS NS Records)	No	DNS Raw Records	0	0	1	0	None	dns2.registrar-servers.com
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:80
2022-12-18 00:09:37	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.3:80
2022-12-18 00:09:20	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.5:8443
2022-12-18 00:22:07	Netblock Membership	No	Censys	0	0	2	0	None	34.149.0.0/16
2022-12-18 00:06:50	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "IsoScope_ac8_ConnHashTable<2760>_HashTable_Mutex"\n "Local\\ZonesCacheCounterMutex"\n "Local\\!BrowserEmulation!SharedMemory!Mutex"\ u'identifier': u'binary-37', u'name': u'Drops files inside appdata directory', u'attck_id_wiki': None, u'threat_level_human': u'infor [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442]- [targe "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\265C0DEB29181DD1891051371C5F863A_14F2E352CCFE495001982FF Related', u'origin': u'String', u'identifier': u'string-3', u'name': u'Found potential URL in binary/memory', u'attck_id_wiki': None, u'https://pro77argenti3er.prpb839vvinciar.repl.co/index1.html', u'submission_id': u'6349c14052d83759c2363e21', u'created_at': u'2022-
2022-12-18 00:11:03	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 currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with th reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access t Registrant Country: US Registrant Phone: DATA REDACTED Registrant Phone Ext: DATA REDACTED Registrant Fax: DATA REDACTED Registrant F Server: ns4.cloudflare.com Name Server: ns5.cloudflare.com Name Server: ns6.cloudflare.com Name Server: ns7.cloudflare.com DNSSEC: si
2022-12-18 00:15:03	Malicious Internet Name	Yes	VirusTotal	0	1	1	0	None	VirusTotal [misogyny.wtf] https://www.virustotal.com/en/domain/misogyny.wtf/information/
2022-12-18 00:02:47	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	089070 (Net ID: 00:02:2D:08:90:70)
2022-12-18 00:21:06	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-O
2022-12-18 00:08:59	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.0:80
2022-12-18 00:13:34	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 protoc
2022-12-18 00:39:43	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.7] https://www.virustotal.com/en/ip-address/188.114.96.7/information/
2022-12-18 00:03:08	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.197
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WLAN (Net ID: 00:01:24:F1:C3:85)
2022-12-18 00:09:38	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.13:8080
2022-12-18	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra

00:21:02									
2022-12-18 00:21:02	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:03:11	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.239
2022-12-18 00:04:28	Raw DNS Records	No	DNS Raw Records	0	0	1	0	None	misogyny.wtf. 1800 IN NS dns1.registrar-servers.com. misogyny.wtf. 1800 IN NS dns2.registrar-servers.com.
2022-12-18 00:08:56	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.0:8443
2022-12-18 00:09:31	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.169.215:80
2022-12-18 00:16:26	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-SH X509v3 Basic Constraints: critical CA:FALSE CT Precertificate SCTs: Signed Certificate Timestamp: Version : v1 (0x0) Log ID : E8:3E:D 30:45:02:21:00:d8:35:e0:5c:fe:c9:39:b4:06:5a:95:36:1c: 73:f4:85:1c:c5:6e:6b:ef:48:76:d6:7f:a3:fe:55:ed:82:7f: c5:02:20:7f:8c:86:3a:6f
2022-12-18 00:06:40	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 15, u'threat_score': 100, u server', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'thre b0d1-3dcfd7392a15.tmp" has type "ASCII text with very long lines with no line terminators"- [targetUID: N/A]\n "LOG" has type "ASCII u'type': 2, u'description': u'"C:\\Users\\HAPUBWS\\AppData\\Local\\Microsoft\\Edge\\User Data\\Crashpad" (Indicator: "microsoft\\edge "microsoft\\edge\\user data") in Source: 00000000-00004600-00000BE4-218136205986\n "C:\\Users\\HAPUBWS\\AppData\\Local\\Microsoft\\Ed "%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Subresource Filter\\Indexed Rules\\35\\10.34.0.28"\n Potential IP "10.34.0.28" found in u'threat_level_human': u'malicious', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 2, u'type': 12, u'descr
2022-12-18 00:19:05	Physical Location	No	ipapi.co	0	0	3	0	None	Florence, Tuscany, 52, Italy, IT
2022-12-18 00:09:40	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	abtebepon.tk
2022-12-18 00:22:28	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.128:80
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetA41A (Net ID: 00:01:36:57:A4:18)
2022-12-18 00:21:20	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:
2022-12-18 00:35:49	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.236] https://www.virustotal.com/en/ip-address/81.88.52.236/information/
2022-12-18 00:09:16	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.3:8443
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	6562 7451 (Net ID: 00:00:C5:D7:2F:EC)
2022-12-18 00:10:03	Physical Location	No	URLScan.io	0	0	1	0	None	US
2022-12-18 00:18:06	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.1:8443
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:443
2022-12-18 00:08:40	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:25:38	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-182.w90-116.abo.wanadoo.fr
2022-12-18 00:20:39	Netblock Membership	No	Censys	0	0	1	0	None	20.192.0.0/10
2022-12-18 00:21:13	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-O
2022-12-18 00:09:43	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	alert.auroramediagroup.xyz

2022-12-18 00:21:27	Netblock IPv6 Membership	No	Censys	0	0	2	0	None	2606:4700:3037::/48
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	default (Net ID: 00:01:24:F0:65:67)
2022-12-18 00:12:31	URL (Purely Static)	No	Page Information	0	0	4	0	None	http://misogyny.wtf/parser
2022-12-18 00:03:12	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	api.plague.fun
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	TEO Network Enterprise (Net ID: 00:01:24:F0:B7:E1)
2022-12-18 00:21:20	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:09:20	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.5:443
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	BJNPSETUP (Net ID: 00:00:85:F4:1C:9A)
2022-12-18 00:21:58	Open TCP Port	No	Censys	0	0	2	0	None	2a06:98c1:3120::1:80
2022-12-18 00:04:02	Physical Location	No	ipstack	0	0	2	0	None	United States
2022-12-18 00:04:04	Web Server	No	Tool - WhatWeb	0	0	1	0	None	Werkzeug/2.2.2 Python/3.9.11
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:2095
2022-12-18 00:03:35	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:20:36	Physical Location	No	Censys	1	0	1	0	None	Amsterdam, North Holland, 1012, Netherlands, Europe
2022-12-18 00:23:00	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	3	0	None	amen.fr
2022-12-18 00:31:03	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.cloud
2022-12-18 00:04:38	Username	No	Account Finder	2	0	1	0	None	zerotwo-best-waifu
2022-12-18 00:02:39	Domain Name	No	SpiderFoot UI	16	0	0	0	None	rasputain.fr
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:2096
2022-12-18 00:21:13	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:07:00	Malicious IP Address	Yes	Internet Storm Center	0	1	2	0	None	Internet Storm Center [34.149.204.188] https://isc.sans.edu/api/ip/34.149.204.188
2022-12-18 00:18:21	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.8:443
2022-12-18 00:25:35	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-176.w90-116.abo.wanadoo.fr
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:02:47	Raw Data from RIRs	No	CertSpotter	1	0	1	0	None	[{u'pubkey_sha256': u'f842b5fd7b48b773eae9aa6f5314b0dbd70cc31a085c84b95ffafa8db9b6d4c9', u'revoked': False, u'not_after': u'2023-01-1 u'acf2ac151f50c231c00eaa4065d9974d19858788bd3a15e1c66a77b225be0e48', u'type': u'precert'}, u'dns_names': [u'*.rasputain.fr', u'rasput u'MIIEUzCCAzugAwIBAgISAyzNm1BlAuipZpMRlzOP4+2bMA0GCSqGSIb3DQEBCwUAMDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQDEwJ u'2f150a3178bc7623ed48e9070b57caf428cdd366e99a151e4ae16ba6fa363cad', u'type': u'cert'}, u'dns_names': [u'rasputain.fr'], u'tbs_sha256

2022-12-18 00:09:20	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.5:8080
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SurfandSip Wavelan (Net ID: 00:02:2D:01:79:94)
2022-12-18 00:12:05	Country	No	Country Name Extractor	0	0	4	0	None	United States
2022-12-18 00:18:10	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [188.114.97.0] https://www.virustotal.com/en/ip-address/188.114.97.0/information/
2022-12-18 00:13:34	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 4.3 Description: OpenVPN, when using a 64-bit block cipher, makes
2022-12-18 00:21:44	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: -
2022-12-18 00:25:41	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-188.w90-116.abo.wanadoo.fr
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	beigekhakiprocedurallanguage--pichinncha3ec.repl.co
2022-12-18 00:21:37	Software Used	Yes	Censys	0	0	2	0	None	python 3.9.11
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	pichinhsac--pichinhsac.repl.co
2022-12-18 00:05:13	Linked URL - Internal	No	Hybrid Analysis	0	0	2	0	None	http://misogyny.wtf/inject/UsRjS959Rqm4sPG4
2022-12-18 00:25:44	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	cloudioazure.register.it
2022-12-18 00:20:29	Raw Data from RIRs	No	LeakIX	0	0	3	0	None	{u'Services': None, u'Leaks': None}
2022-12-18 00:21:20	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-(
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	SpeedStream (Net ID: 00:01:24:F0:82:16)
2022-12-18 00:14:14	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.144:8080
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:2086
2022-12-18 00:22:11	BGP AS Membership	No	Censys	0	0	2	0	None	39729
2022-12-18 00:09:11	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'172.67.190.129', u'vendor': u'', u'port': u'80', u'transpor u'', u'location': {u'lat': 37.751, u'lon': -97.822}, u'country_name': u'United States', u'continent_name': u'North America', u'regior u'infected': False, u'collections': 0, u'size': 0}, u'type': u'', u'severity': u'', u'stage': u''}, u'event_pipeline': [u'CertStream' {"success_fraction":0,"report_to":"cf-nel","max_age":604800}\r\nServer: cloudflare\r\nCF-RAY: 764581ed1a4f7320-LHR\r\nalt-svc: h3=":4 u'0001-01-01T00:00:00Z'}, u'enabled': False, u'detected': False, u'version': u''}, u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'noauth': False, u'key': u''}, u'software': {u'modules': None, u'version': u'', u'os': u'', u'name': u'cloudflare', u'fingerprint': u'Date: Thu, 03 Nov 2022 06:38:27 GMT\r\nContent-Type: text/html\r\nTransfer-Encoding: chunked\r\nConnection: close\r\nLast-Modified:
2022-12-18 00:02:39	Internet Name	No	SpiderFoot UI	25	0	0	0	None	rasputain.fr
2022-12-18 00:12:05	Physical Location	No	ipapi.co	0	0	2	0	None	Newark, New Jersey, NJ, United States, US
2022-12-18 00:08:38	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2022-12-18 00:21:47	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:27:36	Malicious IP Address	Yes	MetaDefender	0	0	2	0	None	webroot.com [188.114.96.9]

2022-12-18 00:11:04	Affiliate - Domain Whois	No	Whois	4	0	3	0	None	Domain Name: AMENWORLD.COM Registry Domain ID: 15262498_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.networksolutions.com Registrar database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a http://networksolutions.com Updated Date: 2022-11-26T05:03:33Z Creation Date: 1999-12-14T23:19:10Z Registrar Registration Expiration Masking Enabled Tech City: Statutory Masking Enabled Tech State/Province: Statutory Masking Enabled Tech Postal Code: Statutory Maski related to a domain name registration record. Networksolutions.com makes this information available "as is," and does not guarantee i
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:08:42	Physical Location	No	LeakIX	0	0	1	0	None	Zurich, Zurich, Switzerland
2022-12-18 00:56:40	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	misogyny.net
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ToddNet (Net ID: 00:01:24:F2:5E:43)
2022-12-18 00:12:03	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'NJ', u'country_tld': u'.us', u'ip': u'2606:4700:3031::ac43:93e6', u'currency_name': u'Dollar', u'currency': u'USD'
2022-12-18 00:07:18	Web Content	No	Web Spider	2	0	3	0	None	<!doctype html> <html lang=en> <title>404 Not Found</title> <h1>Not Found</h1> <p>The requested URL was not found on the server. If y
2022-12-18 00:05:51	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 16, u'threat_score': None, u'compromis u'relevance': 3, u'threat_level': 0, u'type': 4, u'description': u'"\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:2268:120:WilError_01' type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%TEMP%\\2268_478418729_platform_specific\\win_x64\\widevi "77EC63BDA74BD0D0E0426DC8F8008506" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\77EC63BDA74 with no line terminators"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\e93703ec-1b1f-4cd8-ac7e-72ecaace237e.tmp]- [targetU u'suspicious', u'capec_id': None, u'attck_id': None, u'relevance': 5, u'threat_level': 1, u'type': 8, u'description': u'Dropped file: u'identifier': u'binary-1', u'name': u'Drops executable files', u'attck_id_wiki': None, u'threat_level_human': u'suspicious', u'capec
2022-12-18 00:21:47	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:08:39	Open TCP Port	No	LeakIX	0	0	1	0	None	4.228.83.86:80
2022-12-18 00:02:45	SSL Certificate Expiring	Yes	CertSpotter	0	0	1	0	None	2022-12-19 20:09:19
2022-12-18 00:02:48	IP Address	No	Mnemonic PassiveDNS	80	0	1	0	None	188.114.97.0
2022-12-18 00:07:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 77, u'compromised_ "iexplore.exe" touched "WebBrowserHandler Proxy" (Path: "HKCU\\CLSID\\{3CB169B3-17D9-4E47-8B93-2878998F69A2}\\INPROCHANDLER32")\n "ie "iexplore.exe" touched "PSOAInterface" (Path: "HKCU\\CLSID\\{00020424-0000-0000-C000-000000000046}\\INPROCSERVER32")'}, {u'category': "IsoScope_fa8_IESQMMUTEX_0_303"\n "UpdatingNewTabPageData"\n "Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "Local\\!BrowserEmulation!SharedMemor "CAF4703619713E3F18D8A9D5D88D6288_A7725538C46DE2D0088EE44974E2CEBA" has type "data"\n "07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2 u'CAPEC-647', u'attck_id': u'T1012', u'relevance': 10, u'threat_level': 0, u'type': 3, u'description': u'"iexplore.exe" (Path: "HKLM\ u'Detected Suricata Alert', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u're
2022-12-18 00:31:41	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.network
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	linksys (Net ID: 00:01:24:F2:17:BC)
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:12:06	Country	No	Country Name Extractor	0	1	2	0	None	Brazil
2022-12-18 00:09:20	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.5:80
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:80
2022-12-18 00:09:42	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	ads-a-digitalmarketingmasters-ok.live
2022-12-18 00:18:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.13:443
2022-12-18 00:21:17	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-O

2022-12-18 00:02:48	Domain Name	No	grep.app	0	0	1	0	None	zerotwo-best-waifu.online
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:2053
2022-12-18 00:03:02	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.98
2022-12-18 00:22:14	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T23:50:56.796Z", "ip": "172.67.169.215", "location_updated_at": "2022-12-14T08:17:27.851700Z", "autonc {"record_type": "A", "resolved_at": "2022-12-01T12:29:30.322141335Z"}, "image.smarthomebulb.store": {"record_type": "A", "resolved_at "2022-12-02T12:33:43.052698342Z"}, "jump.bobbyho.me": {"record_type": "A", "resolved_at": "2022-12-07T15:44:38.282317480Z"}, "reroti. 11T15:16:50.972553558Z"}, "onlinecasinoadvies.nl": {"record_type": "A", "resolved_at": "2022-12-05T16:40:40.439003453Z"}, "rssbridge. "betterairminneapolis.com": {"record_type": "A", "resolved_at": "2022-12-14T13:14:01.259553748Z"}, "www.paige-elizabeth.com": {"recor 23T16:35:56.486968016Z"}, "fulltenthecomp.gq": {"record_type": "A", "resolved_at": "2022-12-16T14:42:09.346022216Z"}, "thailandlotter "resolved_at": "2022-11-23T17:12:44.076081908Z"}, "budekub.buzz": {"record_type": "A", "resolved_at": "2022-10-12T12:27:50.220553138Z
2022-12-18 00:23:30	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	ftp.zerotwo-best-waifu.online. 900 IN CNAME zerotwo-best-waifu.online.
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date"
2022-12-18 00:21:02	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date"
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	MarvellAP8x (Net ID: 00:01:36:16:7E:FB)
2022-12-18 00:09:32	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	cracroksnamequacis.tk
2022-12-18 00:23:29	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	autoconfig.zerotwo-best-waifu.online. 900 IN CNAME tb-fr.securemail.pro.
2022-12-18 00:08:38	Raw Data from RIRs	No	LeakIX	0	0	1	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'20.195.209.219', u'vendor': u'', u'port': u'80', u'transpor u'', u'geoip': {u'region_iso_code': u'BR-SP', u'country_iso_code': u'BR', u'city_name': u'Campinas', u'location': {u'lat': -22.9035, u'type': u'', u'severity': u'', u'stage': u''}, u'event_pipeline': [u'l9scan', u'tcpid', u'HttpPlugin'], u'http': {u'status': 0, u'ti u'service', u'ip': u'20.195.209.219', u'vendor': u'', u'port': u'80', u'transport': [u'tcp', u'http'], u'event_source': u'l9explore', u'BR-SP', u'country_iso_code': u'BR', u'city_name': u'Campinas', u'location': {u'lat': -22.9035, u'lon': -47.0565}, u'country_name':
2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:13:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.128:8443
2022-12-18 00:21:23	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:02:44	Internet Name - Unresolved	No	CertSpotter	0	0	1	0	None	api.plague.fun
2022-12-18 00:08:44	Raw Data from RIRs	No	LeakIX	0	0	1	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'20.224.2.213', u'vendor': u'', u'port': u'80', u'transport' {u'region_iso_code': u'NL-NH', u'country_iso_code': u'NL', u'city_name': u'Amsterdam', u'location': {u'lat': 52.3759, u'lon': 4.8975} {u'content-length': u'94', u'server': u'Werkzeug/2.0.2 Python/3.9.13'}, u'length': 0, u'favicon_hash': u'', u'root': u''}, u'tags': [u'software': {u'modules': [{u'version': u'3.9.13', u'name': u'Python', u'fingerprint': u''}], u'version': u'2.2.2', u'os': u'', u'nam text/html; charset=utf-8\r\nContent-Length: 94\r\nConnection: close\r\n\r\nRoses are red Violets are blue Wasp is happy
2022-12-18 00:24:58	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.190
2022-12-18 00:02:44	Raw Data from RIRs	No	grep.app	0	0	1	0	None	{u'repo': {u'raw': u'infobloxopen/threat-intelligence'}, u'total_matches': {u'raw': u'1'}, u'content': {u'snippet': u'<table class="h
2022-12-18 00:09:46	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	apparthotel-montana.com
2022-12-18 00:09:22	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.6:80
2022-12-18 00:21:06	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-C
2022-12-18 00:23:00	Co-Hosted Site - Domain Name	No	SSL Certificate Analyzer	0	0	3	0	None	amen.fr
2022-12-18 00:36:54	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.240] https://www.virustotal.com/en/ip-address/81.88.52.240/information/

2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	471cc080-4495-49c9-8c80-bdc32d109730.id.repl.co
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	#LG@Vo1P*Service& (Net ID: 00:01:36:57:A4:17)
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	pannet-24 (Net ID: 00:01:8E:DA:59:C4)
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2052
2022-12-18 00:08:12	Netblock Membership	No	RIPE	4	0	1	0	None	4.224.0.0/12
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ToddNet (Net ID: 00:01:24:F2:5E:43)
2022-12-18 00:08:59	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.0:8443
2022-12-18 00:21:44	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:80
2022-12-18 00:21:58	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:13:15	Search Engines Web Content	No	DuckDuckGo	0	0	2	0	None	{ "Abstract" : "Cloudflare, Inc. is an American content delivery network and DDoS mitigation company, founded in 2009. It primarily a "label" : "Operating income", "sort_order" : "1001", "value" : "US$ \u2212127.7 million (2021)", "wiki_order" : 3 }, { "data_type" : type" : "item", "id" : "Q19967801", "numeric-id" : 19967801 }, "wiki_order" : "207" }], "meta" : [{ "data_type" : "string", "label" Francisco Bay Area" }], "Results" : [{ "FirstURL" : "https://www.cloudflare.com/", "Icon" : { "Height" : 16, "URL" : "/i/cloudflare
2022-12-18 00:21:20	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:
2022-12-18 00:20:05	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [172.67.137.37] https://www.virustotal.com/en/ip-address/172.67.137.37/information/
2022-12-18 00:13:49	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	support@namebright.com
2022-12-18 00:03:27	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	194.204.149.34.bc.googleusercontent.com
2022-12-18 00:05:53	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': u'Windows Gui', u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 9, u'threat_score': 100, u'c (Path: "HKCU\\SOFTWARE\\MICROSOFT\\SYSTEMCERTIFICATES\\CA\\CERTIFICATES\\5AEAEE3F7F2A9449CEBAFEEC68FDD184F20124A7"; Key: "BLOB")\n "E "VirtualProtect" (Indicator: "VirtualProtect")\n "VirtualFree" (Indicator: "VirtualFree")\n "GetFullPathNameW" (Indicator: "GetFullPa u'relevance': 3, u'threat_level': 0, u'type': 9, u'description': u'Spawned process "ElevenClock.Installer.tmp" with commandline "/SL5 u'https://attack.mitre.org/techniques/T1059/003', u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': u'T1059.003' [ebp - 0x34], eax,movdword ptr [ebp - 0x2c], eax,movdword ptr [ebp - 0x28], eax,movdword ptr [ebp - 0x14], eax,moveax, 0x4b14b8,call0 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
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:8080
2022-12-18 00:11:26	Legal Entity Identifier	No	GLEIF	0	0	3	0	None	5493007DY18BGNLDWU14
2022-12-18 00:22:07	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 404 Not Found Replit-Cluster: global Date: <REDACTED> Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Via:
2022-12-18 00:06:42	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.190.129:443
2022-12-18 00:18:25	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.10:8080
2022-12-18 00:22:14	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-O
2022-12-18 00:10:03	Raw Data from RIRs	No	URLScan.io	2	0	1	0	None	[{u'sort': [1668435861696, u'5c215008-1899-4aaa-8f55-bc69632d1bbe'], u'task': {u'domain': u'plague.fun', u'uuid': u'5c215008-1899-4aa u'https://urlscan.io/screenshots/932845e7-6f04-44ea-ba43-55e59845ee6d.png', u'result': u'https://urlscan.io/api/v1/result/932845e7-6f u'result': u'https://urlscan.io/api/v1/result/123e1e1c-97d3-4aac-974d-4d17eba3d22c/', u'_id': u'123e1e1c-97d3-4aac-974d-4d17eba3d22c'

									10-20T13:03:35.083Z', u'apexDomain': u'plague.fun', u'method': u'manual'}, u'stats': {u'uniqIPs': 3, u'uniqCountries': 2, u'encodedDa {u'mimeType': u'text/html', u'status': u'200', u'domain': u'wasp.plague.fun', u'url': u'http://wasp.plague.fun/inject/TJlP9P7aJ8QTzB9 u'http://wasp.plague.fun/inject/MTJ8Vp5aynR51YMM', u'visibility': u'public', u'time': u'2022-10-18T01:17:33.313Z', u'apexDomain': u'p u'text/html', u'status': u'200', u'domain': u'wasp.plague.fun', u'url': u'http://wasp.plague.fun/inject/PDS1ays5XQVjXMk3', u'ip': u'5
2022-12-18 00:09:27	Open TCP Port	No	LeakIX	0	0	2	0	None	34.149.204.188:80
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	chaturbate (Category: XXXPORNXXX) https://chaturbate.com/rasputain/
2022-12-18 00:03:28	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3223.webapps.net
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	REL (Net ID: 00:02:2D:02:35:63)
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:03:10:83)
2022-12-18 00:09:37	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	unifybarometer.top
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:09:32	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	calsawaltare.ml
2022-12-18 00:12:29	Physical Location	No	ipapi.co	0	0	2	0	None	Toronto, Ontario, ON, Canada, CA
2022-12-18 00:33:43	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.188:5060
2022-12-18 00:03:36	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:d8:e8:f9:6e:af:5c:60:20:62:8a:c9:01:2c:b1:dd:b1:ef Signature Algorithm: sha256W X509v3 Authority Key Identifier: keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1 Authority Information Access: OCSP
2022-12-18 00:34:10	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.229] https://www.virustotal.com/en/ip-address/81.88.52.229/information/
2022-12-18 00:28:01	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.su
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:8080
2022-12-18 00:14:47	Internet Name - Unresolved	No	VirusTotal	0	0	1	0	None	www.plague.fun
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	55294762-91a3-4ac7-93f9-c44ef8b9aead.id.repl.co
2022-12-18 00:20:23	Physical Location	No	Fraudguard	0	0	3	0	None	France, Alpes-Maritimes, Cannes
2022-12-18 00:11:10	Similar Domain - Whois	No	Whois	0	0	2	0	None	Domain: plague.gg Domain Status: Active Transfer Prohibited by Registrar Registrant: Redacted for privacy Registrar: NameCheap, Inc (
2022-12-18 00:18:19	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.7:8443
2022-12-18 00:21:51	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:20:44	Malicious IP on Same Subnet	Yes	CINS Army List	0	0	2	0	None	cinsscore.com [40.112.0.0/13] http://cinsscore.com/list/ci-badguys.txt
2022-12-18 00:18:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.4:443
2022-12-18 00:11:12	Similar Domain - Whois	No	Whois	0	0	2	0	None	********** * Please note that the following result could be a subgroup of
2022-12-18 00:08:54	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.147.230:8443
2022-12-18 00:10:05	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	https://zerotwo-best-waifu.online/778112985743251/wap/dsc_injection

2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	Snapchat Stories (Category: social) https://story.snapchat.com/s/rasputain
2022-12-18 00:18:24	Internet Name	No	DNS Resolver	0	0	2	0	None	zerotwo-best-waifu.online
2022-12-18 00:08:24	Netblock Membership	No	RIPE	73	0	2	0	None	188.114.97.0/24
2022-12-18 00:21:54	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-(
2022-12-18 00:09:40	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	a-snag-us-bathroom-remodel.fyi
2022-12-18 00:16:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:04:30	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	mail-fr.securemail.pro
2022-12-18 00:31:49	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.press
2022-12-18 00:32:43	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.224] https://www.virustotal.com/en/ip-address/81.88.52.224/information/
2022-12-18 00:06:42	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.190.129:8443
2022-12-18 00:11:30	Physical Address	No	GLEIF	0	0	3	0	None	10500 NE 8TH ST, STE 750, BELLEVUE, US-WA, US, 98004
2022-12-18 00:06:37	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:d6:9e:d2:88:e9:c1:89:74:28:65:2d:6e:88:09:50:9f:4f Signature Algorithm: ecdsa-w : ecdsa-with-SHA256 30:45:02:20:4A:E4:98:06:90:A2:26:39:BD:A3:6A:4D: A5:7D:F1:92:76:73:72:56:74:3A:35:52:D7:FB:31:D9: 74:05:08:1E:02:
2022-12-18 00:21:37	BGP AS Membership	No	Censys	0	0	2	0	None	8075
2022-12-18 00:08:23	Physical Location	No	Fraudguard	0	0	1	0	None	Netherlands, North Holland, Amsterdam
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	iz-wpa (Net ID: 00:01:8E:1A:64:A6)
2022-12-18 00:08:40	Malicious IP on Same Subnet	Yes	CleanTalk Spam List	0	0	2	0	None	CleanTalk Spam List [20.192.0.0/10] https://iplists.firehol.org/files/cleantalk_7d.ipset
2022-12-18 00:09:18	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.4:443
2022-12-18 00:31:45	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.onl
2022-12-18 00:11:10	Similar Domain - Whois	No	Whois	0	0	2	0	None	domain.....: plague.fi status.....: Registered created.....: 27.2.2015 16:06:53 expires.....: 27.2.2025
2022-12-18 00:32:06	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.site
2022-12-18 00:31:38	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@godaddy.com
2022-12-18 00:36:22	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.238] https://www.virustotal.com/en/ip-address/81.88.52.238/information/
2022-12-18 00:08:45	IP Address	No	DNS Resolver	0	0	2	0	None	81.88.52.232
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	interbanca.alertaficohsa.repl.co
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:2083
2022-12-18 00:09:21	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.7.179:8443

2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:2086
2022-12-18 00:07:07	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 70, u'compromised_ u'origin': u'Binary File', u'identifier': u'binary-16', u'name': u'Drops files marked as clean', u'attck_id_wiki': None, u'threat_lev "MSAA AccPropServices" (Path: "HKCU\\CLSID\\{B5F8350B-0548-48B1-A6EE-88BD00B4A5E7}\\TREATAS")\n "iexplore.exe" touched "Task Bar Comm "Microsoft Url History Service" (Path: "HKCU\\CLSID\\{3C374A40-BAE4-11CF-BF7D-00AA006946EE}\\PROGID")'}, {u'category': u'General', u' type "data"\n "search_2_.json" has type "ASCII text with no line terminators"\n "~DFF4882BA6F87F7023.TMP" has type "data"\n "80237EE4 u'https://attack.mitre.org/techniques/T1012', u'threat_level_human': u'informative', u'capec_id': u'CAPEC-647', u'attck_id': u'T1012' 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
2022-12-18 00:13:50	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namebright.com
2022-12-18 00:21:09	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:
2022-12-18 00:21:27	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: -
2022-12-18 00:13:51	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@ovh.net
2022-12-18 00:08:54	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'172.67.147.230', u'vendor': u'', u'port': u'80', u'transpor 37.751, u'lon': -97.822}, u'country_name': u'United States', u'continent_name': u'North America', u'region_name': u''}, u'host': u'17 u'length': 0, u'favicon_hash': u'', u'root': u''}, u'tags': [], u'ssl': {u'cypher_suite': u'', u'jarm': u'', u'certificate': {u'domai u'event_type': u'service', u'ip': u'172.67.147.230', u'vendor': u'', u'port': u'80', u'transport': [u'tcp', u'http'], u'event_source' u'location': {u'lat': 37.751, u'lon': -97.822}, u'country_name': u'United States', u'continent_name': u'North America', u'region_name u'leak': {u'dataset': {u'files': 0, u'rows': 0, u'ransom_notes': None, u'infected': False, u'collections': 0, u'size': 0}, u'type': u s=oP1mq%2BnndrAFwQ84uK3P2QUttnvIR52MsUJJ1FJDAjip3XbhcZAH98A9ipie2K6qHOJn0bR2DiDGv2ahYNM%2FwZ36H0xX45v7yLAaZ8G%2BCfbqyNt1KHq7Xnk2HxUle
2022-12-18 00:12:05	Country	No	Country Name Extractor	0	0	5	0	None	France
2022-12-18 00:27:12	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.58.196:465
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:8880
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:2053
2022-12-18 00:16:36	Raw Data from RIRs	No	numverify	0	0	3	0	None	{u'international_format': u'+33170702110', u'local_format': u'170702110', u'number': u'33170702110', u'valid': True, u'line_type': u'
2022-12-18 00:21:41	Physical Location	No	Censys	0	0	2	0	None	Campinas, Sao Paulo, Brazil, South America
2022-12-18 00:16:53	Affiliate - Company Name	No	Company Name Extractor	0	0	4	0	None	NAMECHEAP INC
2022-12-18 00:28:27	Physical Location	No	MetaDefender	0	0	3	0	None	Firenze, Italy
2022-12-18 00:03:08	Affiliate - IP Address	No	DNS Look-aside	5	0	2	0	None	81.88.52.222
2022-12-18 00:32:18	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	westabuse@gmail.com
2022-12-18 00:09:42	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	adler-shop.ch
2022-12-18 00:02:45	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=*.misogyny.wtf
2022-12-18 00:25:33	Affiliate - Domain Name	No	DNS Resolver	0	0	3	0	None	securemail.pro
2022-12-18 00:12:19	Phone Number	No	Phone Number Extractor	3	0	2	0	None	+3544212434

2022-12-18 00:05:08	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised "\\Sessions\\1\\BaseNamedObjects\\Local\\!BrowserEmulation!SharedMemory!Mutex"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\VERMGMTBloc [targetUID: 00000000-00003048]\n Dropped file: "XXQS23FV.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\XXQS23FV.txt]- [ta type "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "~DF23DB81915CF93D1F.TMP" has type "data"- Lo 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'desc trusted Antivirus engine', u'attck_id_wiki': None, u'threat_level_human': u'malicious', u'capec_id': None, u'attck_id': None, u'relev Transfer', u'informative_identifiers': [], u'tactic': u'Command and Control', u'informative_identifiers_count': 1, u'suspicious_ident
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	myLGNetFBC6 (Net ID: 00:01:36:5A:FB:C4)
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WaveLAN Network (Net ID: 00:02:2D:03:8E:D3)
2022-12-18 00:15:06	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	confirrr.confir45.repl.co
2022-12-18 00:04:01	Physical Location	No	ipstack	0	0	2	0	None	United States
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:8443
2022-12-18 00:24:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.173
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	55 2nd PMO (Net ID: 00:01:21:10:61:00)
2022-12-18 00:08:01	Raw Data from RIRs	No	Certificate Transparency	1	0	1	0	None	[{u'not_after': u'2022-09-18T23:59:59', u'not_before': u'2022-06-20T00:00:00', u'issuer_ca_id': 158800, u'name_value': u'www.zerotwo-
2022-12-18 00:05:20	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise u'Monitored Target', u'identifier': u'target-67', u'name': u'Process launched with changed environment', u'attck_id_wiki': None, u'th "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_FILEMAPSWITCH_MUTEX_3736"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_HASHF "i.ytimg.com"'}, {u'category': u'General', u'origin': u'Monitored Target', u'identifier': u'target-25', u'name': u'Spawns new process "401c7ef5fe070000" to virtual address "0xFBBAF378" (part of module "UXTHEME.DLL")\n "iexplore.exe" wrote bytes "401c7ef5fe070000" to bytes "406882f5fe070000" to virtual address "0xF47C3DD8" (part of module "IEFRAME.DLL")\n "iexplore.exe" wrote bytes "500780f5fe07000 1024x683 frames 3"\n "3Q6HX9B0.txt" has type "ASCII text"\n "B398B80134F72209547439DB21AB308D_CCF564BE5A3C924B17DDEBDEB5236E12" has t
2022-12-18 00:09:47	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	autodiscover.algoritmoexpert.com.br
2022-12-18 00:13:44	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	5	0	None	z22lglbqyskvzwym@registerprivateregistration.com
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:09	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:
2022-12-18 00:04:01	Physical Location	No	ipstack	0	0	2	0	None	Colombia
2022-12-18 00:03:01	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:50:42:ff:9a:7a:0a:ec:db:51:55:79:18:dd:8f:ed:52:b0 Signature Algorithm: sha256W Identifier: keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6 Authority Information Access: OCSP - URI:http://r3.o.le
2022-12-18 00:13:07	Internet Name	No	DNS Brute-forcer	1	1	1	0	None	mc.rasputain.fr
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	3a141a26-3f99-4729-a07d-d79506a1ed3c.id.repl.co
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	perswebpichincha-com--webpich.repl.co
2022-12-18 00:03:27	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	197.204.149.34.bc.googleusercontent.com

2022-12-18 00:09:14	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'104.21.19.243', u'vendor': u'', u'port': u'80', u'transport u'', u'location': {u'lat': 0, u'lon': 0}, u'country_name': u'', u'continent_name': u'', u'region_name': u''}, u'host': u'getinbox.tec u'size': 0}, u'type': u'', u'severity': u'', u'stage': u''}, u'event_pipeline': [u'CertStream', u'l9scan', u'tcpid', u'HttpPlugin'], 764581e64a75c45e-EWR\r\nalt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400\r\n\nPage title: JokerLiveStream - Sport Streams Widget' u'8aaf468feab8927fb681839bf712954133a918608eaf8046d1fb3b5c96d9afc3', u'key_algo': u'ECDSA', u'not_before': u'2022-11-03T12:36:21Z'}, u'104.16.0.0/13'}, u'service': {u'credentials': {u'username': u'', u'raw': None, u'password': u'', u'noauth': False, u'key': u''}, u' u'', u'city_name': u'', u'location': {u'lat': 0, u'lon': 0}, u'country_name': u'', u'continent_name': u'', u'region_name': u''}, u'hc
2022-12-18 00:05:32	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 16, u'threat_score': None, u'origin': u'Binary File', u'identifier': u'binary-16', u'name': u'Drops files marked as clean', u'attck_id_wiki': None, u'threat_lev u'description': u'"widevinecdm.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\\(x8 Location: [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\77EC63BDA74BD0D0E0426DC8F8008506]- [targetUID: 00000000-0000485 801b-7f2295bdfcdd.tmp]- [targetUID: 00000000-00004856]\n "Indexing in Progress" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft inside temp directory', u'attck_id_wiki': None, u'threat_level_human': u'suspicious', u'capec_id': None, u'attck_id': None, u'relevar {u'category': u'Installation/Persistence', u'origin': u'API Call', u'identifier': u'api-43', u'name': u'Writes a PE file header to di
2022-12-18 00:08:38	BGP AS Membership	No	RIPE	0	0	2	0	None	8075
2022-12-18 00:04:38	Username	No	Account Finder	26	0	1	0	None	rasputain
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	cc80f5ce-556e-4359-822e-61d4178e4d8d.id.repl.co
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	atencionparati.edavivienda.repl.co
2022-12-18 00:24:05	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	hmac-sha2-256-etm@openssh.com
2022-12-18 00:24:59	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.193
2022-12-18 00:09:37	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'https', u'event_type': u'service', u'ip': u'188.114.96.3', u'vendor': u'', u'port': u'443', u'transpor u'', u'ssh': {u'motd': u'', u'version': 0, u'banner': u'', u'fingerprint': u''}, u'reverse': u'', u'geoip': {u'region_iso_code': u'NU u'key': u''}, u'software': {u'modules': None, u'version': u'', u'os': u'', u'name': u'cloudflare', u'fingerprint': u''}}, u'event_fir u'shanerimmer.com', u'summary': u'Date: Fri, 04 Nov 2022 13:58:58 GMT\r\nContent-Type: text/html; charset=UTF-8\r\nTransfer-Encoding: u'severity': u'', u'stage': u''}, u'event_pipeline': [u'CertStream', u'l9scan', u'tcpid', u'HttpPlugin'], u'http': {u'status': 0, u't nel","max_age":604800}\r\nServer: cloudflare\r\nCF-RAY: 764dde00cae790d6-FRA\r\nalt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400\ u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'banner': u'', u'fingerprint': u''}, u'reverse': u'', u'geoip': {u'region_iso_coc
2022-12-18 00:09:46	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.17:80
2022-12-18 00:08:39	Netblock Membership	No	RIPE	0	0	2	0	None	188.114.96.0/24
2022-12-18 00:31:07	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse-contact@sav.com
2022-12-18 00:06:05	Affiliate - Domain Name	No	DNS Resolver	2	0	2	0	None	amenworld.com
2022-12-18 00:09:38	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	3974639.com.cdn.cloudflare.net
2022-12-18 00:03:12	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	api.plague.fun
2022-12-18 00:14:36	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-6329 https://nvd.nist.gov/vuln/detail/CVE-2016-6329 Score: 4.3 Description: OpenVPN, when using a 64-bit block cipher, makes
2022-12-18 00:04:28	Name Server (DNS NS Records)	No	DNS Raw Records	0	0	1	0	None	garrett.ns.cloudflare.com
2022-12-18 00:28:45	Similar Domain - Whois	No	Whois	0	0	2	0	None	No match for "PLAGUE.TV". >>> Last update of WHOIS database: 2022-12-18T00:28:31Z <<< NOTICE: The expiration date displayed in this r Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automa
2022-12-18 00:07:49	Co-Hosted Site	No	Certificate Transparency	0	0	1	0	None	sni.cloudflaressl.com

2022-12-18 00:18:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.6:8443
2022-12-18 00:06:35	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.0:8443
2022-12-18 00:03:10	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	1	0	None	webapps.net
2022-12-18 00:07:21	Raw Data from RIRs	No	Google	0	0	1	0	None	{'webSearchUrl': u'https://www.google.com/search?q=site:zerotwo-best-waifu.online&aq=t&oe=utf-8&client=firefox-a&ie=utf-8&rls=org.moz
2022-12-18 00:13:26	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	domainabuse@tucows.com
2022-12-18 00:11:51	Malicious IP on Same Subnet	Yes	Greensnow	0	0	3	0	None	greensnow.co [81.88.48.0/20] https://blocklist.greensnow.co/greensnow.txt
2022-12-18 00:03:27	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	193.204.149.34.bc.googleusercontent.com
2022-12-18 00:25:37	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-180.w90-116.abo.wanadoo.fr
2022-12-18 00:21:23	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3032::ac43:be81:443
2022-12-18 00:16:53	Affiliate - Company Name	No	Company Name Extractor	0	0	4	0	None	Network Solutions, LLC
2022-12-18 00:21:09	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-(
2022-12-18 00:05:57	Account on External Site	No	Account Finder	0	0	2	0	None	Internet Archive User Search (Category: misc) https://archive.org/search.php?query=zerotwo-best-waifu
2022-12-18 00:25:45	Physical Location	No	MetaDefender	0	0	2	0	None	Medellin, Colombia
2022-12-18 00:31:34	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	domainabuse@tucows.com
2022-12-18 00:06:33	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "Local\\ZonesLockedCacheCounterMutex"\n "IsoScope_d54_IE_EarlyTabStart_0xe14_Mutex"\n "\\Sessions\\1\\BaseNamedObjects\\IsoScope_d54_ en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: transparentde compression"\n "CabC48F.tmp" has type "Microsoft Cabinet archive data Windows 2000/XP setup 62919 bytes 1 file at 0x2c +A "authroot.s [%LOCALAPPDATA%\\Microsoft\\Windows\\Temporary Internet Files\\Content.IE5\\37NU00GP\\8J27H8AQ.htm]- [targetUID: 00000000-00004004]\n Windows 2000/XP setup 62919 bytes 1 file at 0x2c +A "authroot.stl" number 1 6 datablocks 0x1 compression"- Location: [%TEMP%\\CabC48F "https://transparentdelightfulpolyhedron.davi9875.repl.co"\n Heuristic match: "transparentdelightfulpolyhedron.davi9875.repl.co"\n Pa
2022-12-18 00:14:05	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 5.0 Description: The DES and Triple DES ciphers, as used in the T
2022-12-18 00:09:37	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	webmail.delfin.ee
2022-12-18 00:04:11	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	188.114.97.1:443
2022-12-18 00:08:44	Open TCP Port	No	Pulsedive	0	0	2	0	None	104.21.19.243:8443
2022-12-18 00:05:41	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise 1\nConnection: Keep-Alive" (Indicator: "mozilla/5.0 (")\n "GET /archvs/icons8-eye-48.png HTTP/1.1\nAccept: image/png, image/svg+xml, "GET /archvs/library(2).css HTTP/1.1\nAccept: text/css, */*\nReferer: https://wellgroomedhuskyelement.bancathn.repl.co/\nAccept-Langu https://wellgroomedhuskyelement.bancathn.repl.co/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:1 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' Antivirus vendors marked dropped file "TarC1A2.tmp" as clean (type is "data")'}, {u'category': u'General', u'origin': u'Network Traff datablocks 0x1 compression"\n "CabC1A1.tmp" has type "Microsoft Cabinet archive data Windows 2000/XP setup 62932 bytes 1 file at 0x2c
2022-12-	Linked URL	No	URLScan.io	1	0	1	0	None	https://misogyny.wtf/inject/UsRjS959Rqm4sPG4

18 00:10:04	- Internal								
2022-12-18 00:21:58	Open TCP Port	No	Censys	0	0	2	0	None	2a06:98c1:3120::1:443
2022-12-18 00:09:39	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	3d-shine.cn
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	grownediblehardrive.verific2022.repl.co
2022-12-18 00:09:51	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	bkqpv.tw.cdn.cloudflare.net
2022-12-18 00:08:44	Internet Name	No	DNS Resolver	0	0	2	0	None	www.zerotwo-best-waifu.online
2022-12-18 00:04:47	Malicious IP Address	Yes	Maltiverse	0	1	2	0	None	Maltiverse [104.21.7.179]
2022-12-18 00:22:07	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Connection": "DISPLAY_UTF8"}, "Connection": ["close"]}
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	salplramtreamyclawzsolpail.sismteam.repl.co
2022-12-18 00:05:37	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	atlas.plague.fun
2022-12-18 00:11:58	Physical Location	No	ipapi.co	0	0	1	0	None	Amsterdam, North Holland, NH, Netherlands, NL
2022-12-18 00:10:05	Raw Data from RIRs	No	URLScan.io	0	0	1	0	None	[{u'sort': [1667590315361, u'1188e2e2-af8b-40c6-8583-2e87bde49a9c'], u'task': {u'domain': u'zerotwo-best-waifu.online', u'uuid': u'11 u'public', u'time': u'2022-11-04T19:31:53.479Z', u'apexDomain': u'zerotwo-best-waifu.online', u'method': u'api'}, u'stats': {u'uniqIP u'https://urlscan.io/screenshots/4d43e7bb-aad6-442f-85fa-4a3686ab7773.png', u'result': u'https://urlscan.io/api/v1/result/4d43e7bb-aa u'zerotwo-best-waifu.online', u'asn': u'AS39729', u'title': u'Site saisi par la BL2C - Police Judiciaire de Paris - Police Nationale u'REGISTER-AS, IT', u'server': u'Apache', u'tlsIssuer': u'ZeroSSL RSA Domain Secure Site CA', u'tlsValidDays': 90, u'country': u'IT', b92f-82ebdad6b3d7', u'url': u'http://zerotwo-best-waifu.online', u'visibility': u'public', u'time': u'2022-08-18T12:13:21.082Z', u'ap u'https://urlscan.io/screenshots/79d42a6e-f145-4347-84ef-337994702af8.png', u'result': u'https://urlscan.io/api/v1/result/79d42a6e-f1
2022-12-18 00:06:45	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [u'phishing'], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u' u'identifier': u'network-0', u'name': u'Contacts domains', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id' clean (type is "data")'}, {u'category': u'General', u'origin': u'Network Traffic', u'identifier': u'network-51', u'name': u'Queries D [%APPDATA%\\Microsoft\\Windows\\Cookies\\P8ZQMMQV.txt]- [targetUID: 00000000-00003108]\n Dropped file: "K3EBOBED.txt" - Location: [%A "MZYDYQ5Q.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\MZYDYQ5Q.txt]- [targetUID: 00000000-00003108]\n Dropped file: "LC superintendencia_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUID: N/A]\n "2_042_nearme_1_.svg" has type "SVG Scalab u'"leAppAdjuster=g.MobileAppAdjuster,t.iFrameAnchors=y.iFrameAnchors,t.hideInMobile=w.hideInMobile,t.youtubeParams=k.youtubeParams},,
2022-12-18 00:11:07	Similar Domain - Whois	No	Whois	2	0	2	0	None	%% %% This is the AFNIC Whois server. %% %% complete date format: YYYY-MM-DDThh:mm:ssZ %% %% Rights restricted by copyright. %% See h
2022-12-18 00:14:14	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.144:443
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	infoworld (Net ID: 00:02:2D:04:D1:DB)
2022-12-18 00:17:38	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [172.67.147.230] https://www.virustotal.com/en/ip-address/172.67.147.230/information/
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:8443
2022-12-18 00:22:14	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-O
2022-12-18 00:18:23	Affiliate - Internet Name	No	DNS Resolver	1	0	2	0	None	tb-fr.securemail.pro
2022-12-18 00:26:05	Country	No	Country Name Extractor	0	1	6	0	None	United Kingdom
2022-12-18 00:23:30	Internet Name	No	DNS Raw Records	0	0	2	0	None	zerotwo-best-waifu.online
2022-12-18 00:09:16	Open TCP Port	No	LeakIX	0	0	2	0	None	20.226.56.97:22
2022-12-	Co-Hosted	No	HackerTarget	0	0	2	0	None	

18 00:09:36	Site								thumderec.ml
2022-12-18 00:16:52	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Font Awesome
2022-12-18 00:18:26	Affiliate - Internet Name	No	DNS Resolver	0	0	2	0	None	mail-fr.securemail.pro
2022-12-18 00:04:28	Name Server (DNS NS Records)	No	DNS Raw Records	0	0	1	0	None	ns1.amenworld.com
2022-12-18 00:18:13	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.4:8080
2022-12-18 00:13:34	Vulnerability - CVE Medium	Yes	Tool - testssl.sh	0	1	2	0	None	CVE-2016-2183 https://nvd.nist.gov/vuln/detail/CVE-2016-2183 Score: 5.0 Description: The DES and Triple DES ciphers, as used in the T
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	knowingeffectiveresource.bancoprovinar.repl.co
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	cbd4ff9b-b43e-44db-b460-6a779468fac5.id.repl.co
2022-12-18 00:12:23	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'SP', u'country_tld': u'.br', u'ip': u'20.226.83.185', u'currency_name': u'Real', u'currency': u'BRL', u'country_po
2022-12-18 00:16:52	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	jQuery
2022-12-18 00:09:16	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.3:80
2022-12-18 00:21:02	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conn
2022-12-18 00:10:04	Web Server	No	URLScan.io	0	0	1	0	None	cloudflare
2022-12-18 00:09:39	Physical Location	No	LeakIX	0	0	2	0	None	Amsterdam, North Holland, Netherlands
2022-12-18 00:25:42	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-191.w90-116.abo.wanadoo.fr
2022-12-18 00:08:38	BGP AS Membership	No	RIPE	0	0	2	0	None	3356
2022-12-18 00:20:52	Physical Location	No	Censys	0	0	1	0	None	Amsterdam, North Holland, 1012, Netherlands, Europe
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conn
2022-12-18 00:14:32	Country	No	Country Name Extractor	0	0	3	0	None	United States
2022-12-18 00:12:24	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'compromised_ "IsoScope_c84_IE_EarlyTabStart_0xe68_Mutex"\n "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\Zon u'description': u'"urlblockindex_1_.bin" has type "data"- [targetUID: N/A]\n "RecoveryStore._5FC32A7B-771D-11ED-B8BD-0800278A77A4_.da "data"- Location: [%TEMP%\\~DFABD3E3197957479F.TMP]- [targetUID: 00000000-00003204]\n "EWM02H3X.txt" has type "ASCII text"- Location: u'threat_level': 1, u'type': 2, u'description': u'Potential IP "188.114.97.3" found in string "https://188.114.97.3/"\n Potential IP u'https://188.114.97.3/', u'submission_id': u'63922bb58f5d337c6c22e8a0', u'created_at': u'2022-12-08T18:23:49+00:00', u'filename': No u'Network Traffic', u'identifier': u'network-1', u'name': u'Contacts server', u'attck_id_wiki': None, u'threat_level_human': u'inform
2022-12-18 00:07:15	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 6, u'threat_score': 100, u'compromised section named ".tls"\n "obs-nvenc-test.exe" has an writable section named ".data"\n "decklink.dll" has an writable section named ".da "HKLM\\SOFTWARE\\Classes\\WOW6432Node\\CLSID\\{A3FCE0F5-3493-419F-958A-ABA1250EC20B}" >nul 2>&1"\n "reg query "HKLM\\SOFTWARE\\Classe edx,movrsi, rcx,cmpedx, 1,jne0x180003585,call0x180003904,movr8, rdi,movedx, ebx,movrcx, rsi,movrbx, qword ptr [rsp + 0x30],movrsi, qw edx,movrsi, rcx,cmpedx, 1,jne0x18043bba1,call0x18043bd60,movr8, rdi,movedx, ebx,movrcx, rsi,movrbx, qword ptr [rsp + 0x30],movrsi, qw 0x28,jmp0x140001794,int3,int3,pushrbx,subrsp, 0x20,movrbx, rcx,xorecx, ecx,callqword ptr [rip + 0xf793],movrcx, rbx,callqword ptr [ri 1,je0x6db01370,addrsp, 0x48,jmp0x6db01200,nop,movqword ptr [rsp + 0x38], r8,movdword ptr [rsp + 0x34], edx,movqword ptr [rsp + 0x28],
2022-12-18 00:12:31	URL (Purely Static)	No	Page Information	0	0	2	0	None	http://misogyny.wtf
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:8443
2022-12-18 00:09:12	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.1:8080

2022-12-18 00:41:02	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: MISOGYNY.COM Registry Domain ID: 1499316_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http:/ database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domair these terms at any time. The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars. Domain Name: misogyny.com Regis Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Ac registrar. By submitting an inquiry, you agree to these terms and limitations of warranty. In particular, you agree not to use this c
2022-12-18 00:17:36	Physical Coordinates	No	OpenStreetMap	91	0	4	0	None	37.7803446,-122.3906132
2022-12-18 00:03:05	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	api.plague.fun
2022-12-18 00:11:53	Raw Data from RIRs	No	ipapi.co	0	0	1	0	None	{u'region_code': u'NH', u'country_tld': u'.nl', u'ip': u'137.117.157.128', u'currency_name': u'Euro', u'currency': u'EUR', u'country_
2022-12-18 00:04:39	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 0, u'threat_score': None, u'compromise u'malicious', u'minor_os_version': None, u'domains': [], u'extracted_files': [], u'type_short': []}, {u'subsystem': None, u'classific "HKLM\\SOFTWARE\\CLASSES\\WOW6432NODE\\CLSID\\{A47979D2-C419-11D9-A5B4-001185AD2B89}\\PROGID")\n "iexplore.exe" touched "Cor MIME Fil "HKCU\\CLSID\\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\\TREATAS")\n "IEXPLORE.EXE" touched "ShellWindows" (Path: "HKCU\\CLSID\\{9BA0597 "142.250.190.131:80"\n "142.250.191.130:443"\n "142.250.190.34:443"\n "172.217.4.66:443"\n "87.250.251.119:443"\n "172.217.4.193:443' 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, "data"\n "GYVCAIAD.txt" has type "ASCII text"\n "zrt_lookup_1_.htm" has type "HTML document ASCII text with very long lines"\n "6BADA
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ENHLG (Net ID: 00:01:36:5B:37:00)
2022-12-18 00:03:26	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	190.204.149.34.bc.googleusercontent.com
2022-12-18 00:03:03	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.106
2022-12-18 00:28:21	Physical Location	No	MetaDefender	0	0	3	0	None	Nice, France
2022-12-18 00:23:19	Country	No	Country Name Extractor	0	1	2	0	None	Brazil
2022-12-18 00:09:38	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	10424580.cn.cdn.cloudflare.net
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	logitecgameuser (Net ID: 00:01:8E:15:D4:A7)
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:2086
2022-12-18 00:02:44	Raw Data from RIRs	No	grep.app	0	0	1	0	None	{u'repo': {u'raw': u'billythegoat356/billythegoat356.github.io'}, u'total_matches': {u'raw': u'1'}, u'content': {u'snippet': u'<table
2022-12-18 00:13:44	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	a5abd1a233e74bff97a58d905b501db2.protect@withheldforprivacy.com
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WaveLAN Network VHome2B (Net ID: 00:02:2D:03:03:11)
2022-12-18 00:24:59	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.191
2022-12-18 00:05:16	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 2, u'search_terms': [{u'id': u'host', u'value': u'172.67.137.37'}], u'result': [{u'environment_id': 120, u'job_id': u'6297
2022-12-18 00:25:44	Affiliate - Domain Name	No	DNS Resolver	2	0	5	0	None	register.it
2022-12-18	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'

00:21:20									
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:8080
2022-12-18 00:13:45	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@dynadot.com
2022-12-18 00:09:50	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	beeorganic.us
2022-12-18 00:21:13	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:
2022-12-18 00:02:50	IP Address	No	Mnemonic PassiveDNS	60	0	1	0	None	172.67.137.37
2022-12-18 00:04:25	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	{u'count': 5, u'search_terms': [{u'id': u'host', u'value': u'104.21.28.240'}], u'result': [{u'environment_id': 160, u'job_id': u'638b None, u'av_detect': u'0', u'environment_description': u'Windows 7 32 bit', u'threat_score': 87, u'verdict': u'malicious', u'submit_na
2022-12-18 00:10:49	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 protoc
2022-12-18 00:04:02	Physical Location	No	ipstack	0	0	2	0	None	Italy
2022-12-18 00:14:32	Country	No	Country Name Extractor	0	0	3	0	None	France
2022-12-18 00:08:38	Netblock Membership	No	RIPE	1	0	2	0	None	172.67.160.0/20
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:2053
2022-12-18 00:18:40	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.17:80
2022-12-18 00:18:42	Raw Data from RIRs	No	Tool - WAFW00F	1	0	2	0	None	[{"url": "https://webmail.zerotwo-best-waifu.online", "firewall": "None", "detected": false, "manufacturer": "None"}]
2022-12-18 00:13:35	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	rir@cloudflare.com
2022-12-18 00:13:43	Internet Name	No	DNS Brute-forcer	6	1	1	0	None	smtp.zerotwo-best-waifu.online
2022-12-18 00:02:43	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=api.plague.fun
2022-12-18 00:16:26	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
2022-12-18 00:10:04	Physical Location	No	URLScan.io	0	0	1	0	None	BR
2022-12-18 00:23:33	Affiliate - Internet Name	No	DNS Raw Records	1	0	2	0	None	webmail-fr.securemail.pro
2022-12-18 00:16:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	sni.cloudflaressl.com
2022-12-18 00:07:17	Linked URL - Internal	No	Web Spider	4	0	2	0	None	http://misogyny.wtf:2020/css/parser.css
2022-12-18 00:24:05	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	curve25519-sha256@libssh.org
2022-12-18 00:18:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.13:8443
2022-12-18 00:09:46	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.17:8080

2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	ArmorGames (Category: gaming) https://armorgames.com/user/rasputain
2022-12-18 00:02:43	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=R3
2022-12-18 00:21:20	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:02:45	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Let's Encrypt,CN=E1
2022-12-18 00:09:36	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.12:8080
2022-12-18 00:12:46	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'NJ', u'country_tld': u'.us', u'ip': u'2606:4700:3035::6815:1bf2', u'currency_name': u'Dollar', u'currency': u'USD'
2022-12-18 00:09:14	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.2:8443
2022-12-18 00:06:16	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\ZonesCacheCounterMutex"' u'name': u'Drops cabinet archive files', u'attck_id_wiki': None, u'threat_level_human': u'informative', u'capec_id': None, u'attck_id u'threat_level': 0, u'type': 8, u'description': u'"plg1_1_.svg" has type "SVG Scalable Vector Graphics image"- [targetUID: N/A]\n "ur 0800271A9FF3_.dat" has type "Composite Document File V2 Document Cannot read section info"- [targetUID: N/A]\n "dberr.txt" has type ' 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'desc u'total_network_connections': 1, u'av_detect': 50, u'machine_learning_models': [], u'total_signatures': 9, u'image_base': None, u'err
2022-12-18 00:03:32	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3231.webapps.net
2022-12-18 00:12:06	Country	No	Country Name Extractor	0	1	2	0	None	Netherlands
2022-12-18 00:16:33	Raw Data from RIRs	No	numverify	0	0	3	0	None	{u'international_format': u'+14259744689', u'local_format': u'4259744689', u'number': u'14259744689', u'valid': True, u'line_type': u
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:2095
2022-12-18 00:06:57	Open TCP Port	No	Pulsedive	0	0	2	0	None	34.149.204.188:443
2022-12-18 00:09:22	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.6:8080
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	Rock Chalk (Net ID: 00:01:95:08:D8:04)
2022-12-18 00:05:58	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	api.plague.fun
2022-12-18 00:04:30	Raw DNS Records	No	DNS Raw Records	0	0	1	0	None	zerotwo-best-waifu.online. 900 IN MX 10 mail-fr.securemail.pro.
2022-12-18 00:04:00	Country	No	Country Name Extractor	0	1	2	0	None	Iceland
2022-12-18 00:08:38	Netblock Membership	No	RIPE	0	0	2	0	None	104.21.16.0/20
2022-12-18 00:12:31	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'104.21.7.179', u'currency_name': u'Dollar', u'currency': u'CAD', u'country_p
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	043320 (Net ID: 00:02:2D:04:33:20)
2022-12-18 00:13:44	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namecheap.com

2022-12-18 00:03:06	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	atlas.plague.fun
2022-12-18 00:03:05	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	hook.plague.fun
2022-12-18 00:06:37	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.1:443
2022-12-18 00:47:06	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.35] https://www.virustotal.com/en/ip-address/188.114.96.35/information/
2022-12-18 00:21:34	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	tricolrsasar.tricolorprueba.repl.co
2022-12-18 00:20:46	BGP AS Membership	No	Censys	0	0	1	0	None	8075
2022-12-18 00:04:11	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
2022-12-18 00:06:01	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:d6:9e:d2:88:e9:c1:89:74:28:65:2d:6e:88:09:50:9f:4f Signature Algorithm: ecdsa-w 30:11:d1:8b:02:89:a9:55:4e:fa:1e:63:01:dd:1c:92:d3:03: 99:e5:5f:ad:f4:fb:2f:0f:19:cc:c1:31:98:97:36:b1:c3:97: 96:91:aa:01:42:36:42:ec
2022-12-18 00:22:07	Open TCP Port	No	Censys	0	0	2	0	None	34.149.204.188:8099
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:80
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	verifiquy.macrond.repl.co
2022-12-18 00:16:26	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	WestEd (Net ID: 00:02:2D:05:7E:93)
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2095
2022-12-18 00:11:00	Affiliate - Domain Whois	No	Whois	4	0	4	0	None	Domain Name: WEBAPPS.NET Registry Domain ID: 98172701_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.register.it Registrar URL: http:/ purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does no Creation Date: 2011-01-25T00:00:00Z Registrar Registration Expiration Date: 2023-05-21T00:00:00Z Registrar: REGISTER S.P.A. Registrar http://wdprs.internic.net/ >>> Last update of whois database: 2022-12-18T00:11:00Z <<< For more information on Whois status codes, pl
2022-12-18 00:16:57	Linked URL - Internal	No	Web Spider	0	0	2	0	None	http://webmail.zerotwo-best-waifu.online
2022-12-18 00:21:13	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:08:27	Netblock Membership	No	RIPE	0	0	2	0	None	20.192.0.0/10
2022-12-18 00:09:18	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.4:80
2022-12-18 00:15:47	Non-Standard HTTP Header	No	Strange Header Identifier	0	0	3	0	None	keep-alive: timeout=5
2022-12-18 00:05:56	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.cc
2022-12-18 00:03:31	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3228.webapps.net
2022-12-18 00:04:27	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 28, u'threat_score': 52, u'compromised FPS_BROWSER_USER_PROFILE_STRING="Default", FPS_BROWSER_APP_PROFILE_STRING="Internet Explorer""\n Process "msedge.exe" (UID: 00000000- "192.0.77.37:443"\n "192.0.77.2:443"\n "192.0.76.3:443"\n "142.251.214.136:443"\n "104.18.225.52:443"\n "68.183.31.14:443"\n "172.67. commandline "--single-argument https://pivigames.blog/" (UID: 00000000-00007776)\n Spawned process "msedge.exe" with commandline "--t "msedge.exe" with commandline "--type=renderer --disable-client-side-phishing-detection --displ ..." (UID: 00000000-00007412), Spawne u'relevance': 3, u'threat_level': 0, u'type': 9, u'description': u'Spawned process "msedge.exe" with commandline "--single-argument h disable-client-side-phishing-detection --displ ..." (UID: 00000000-00006872), Spawned process "msedge.exe" with commandline "--type=r

2022-12-18 00:14:47	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.160:443
2022-12-18 00:08:26	Physical Location	No	Fraudguard	0	0	2	0	None	France, Alpes-Maritimes, Cannes
2022-12-18 00:03:03	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.102
2022-12-18 00:02:52	Domain Registrar	No	Whois	0	0	1	0	None	NAMECHEAP INC
2022-12-18 00:21:51	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-(
2022-12-18 00:19:06	Physical Location	No	ipstack	0	0	3	0	None	Italy
2022-12-18 00:03:25	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	184.204.149.34.bc.googleusercontent.com
2022-12-18 00:09:44	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	altravavuceled.ml
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:2087
2022-12-18 00:27:36	Physical Location	No	MetaDefender	0	0	2	0	None	Medellin, Colombia
2022-12-18 00:21:30	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: -
2022-12-18 00:08:33	Raw Data from RIRs	No	LeakIX	0	0	1	0	None	{u'Services': None, u'Leaks': None}
2022-12-18 00:13:34	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 configurati
2022-12-18 00:21:51	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-(
2022-12-18 00:21:17	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-(
2022-12-18 00:16:27	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:2052
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	583f728d-a0bf-4d32-a6ac-4790f3b2b608.id.repl.co
2022-12-18 00:21:37	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T18:22:57.283Z", "ip": "20.226.83.185", "location_updated_at": "2022-12-05T09:58:11.048726Z", "autonom ["sha256:393fdcc8946ba766b2d3c64d6c60f600e141f5f1b49bdf34ca6636cc3741f99c", "sha1:09a15540b06ce16164e40ae17c66e477bf1401de"], "status {"_encoding": {"User_Agent": "DISPLAY_UTF8", "Accept": "DISPLAY_UTF8"}, "User_Agent": ["Mozilla/5.0 (compatible; CensysInspect/1.1; + "banner_hashes": ["sha256:faf3963d2a83a2de210a1e48e54b1bb2b90d8595c09e807aa56e17d64fda353a"], "source_ip": "167.248.133.63", "extende "DISPLAY_HEX"}, "leaf_data": {"pubkey_algorithm": "RSA", "public_key": {"key_algorithm": "RSA", "rsa": {"_encoding": {"modulus": "DIS "14d14d16d14d14d08c14d14d14d14d", "tls_extensions_sha256": "fd9c9d14e4f4f67f94f0359f8b28f532", "observed_at": "2022-12-10T14:48:44.55 ["*/*"]}, "method": "GET", "uri": "http://20.226.83.185:5050/"}, "response": {"body": "root page", "_encoding": {"body": "DISPLAY_UTF
2022-12-18 00:05:38	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	stream.plague.fun
2022-12-18 00:08:13	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 41:cf:04:f8:c0:f2:7b:cd:70:73:3f:d3:40:5f:a0:ad Signature Algorithm: sha384WithRSA critical CA:FALSE X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication X509v3 Certificate Policies c0:01:cb:36:53:03:f6:58:2d:9b:58:bd:4c:21:48:8b:7f:cc: 71:3b:54:d0:9f:7a:b6:bc:fe:37:93:67:af:18:58:c0:de:bb: df:39:f6:f3:13:81:d7:f6
2022-12-18 00:18:04	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.0:80
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	perswebpichincha-com.webpich.repl.co
2022-12-18 00:14:32	Country	No	Country Name Extractor	0	1	3	0	None	United Kingdom
2022-12-18 00:03:04	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	90.116.166.109

2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	ecuapichin.repl.co
2022-12-18 00:02:43	SSL Certificate - Issued to	No	CertSpotter	1	0	1	0	None	CN=*.plague.fun
2022-12-18 00:06:58	Malicious IP Address	Yes	Internet Storm Center	0	1	2	0	None	Internet Storm Center [188.114.97.0] https://isc.sans.edu/api/ip/188.114.97.0
2022-12-18 00:13:34	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@cloudflare.com
2022-12-18 00:05:00	SSL Certificate - Raw Data	No	Certificate Transparency	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:f8:40:07:a9:2a:29:fa:95:e2:5f:ea:f2:e9:75:79:57:8e Signature Algorithm: sha256w with-SHA256 30:44:02:20:61:29:22:AC:4F:7C:30:86:DB:CB:A5:62: 1A:74:E6:F0:17:04:90:2B:D9:04:A5:D2:DA:A2:8A:F3: A8:7C:6C:79:02:20:6F:4C
2022-12-18 00:24:55	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.175
2022-12-18 00:06:31	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.147.230:8080
2022-12-18 00:21:23	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:22:11	Physical Location	No	Censys	0	0	2	0	None	Italy, Europe
2022-12-18 00:09:49	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	avfree.me
2022-12-18 00:21:17	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:04:02	Physical Location	No	ipstack	0	0	2	0	None	United States
2022-12-18 00:21:23	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:21:47	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:06:37	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.1:8443
2022-12-18 00:10:03	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://wasp.plague.fun
2022-12-18 00:09:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.8:8080
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	new.laposadadelch.repl.co
2022-12-18 00:21:47	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: -
2022-12-18 00:08:23	Physical Location	No	Fraudguard	0	0	1	0	None	Switzerland, Zurich, Zurich
2022-12-18 00:38:20	Malicious IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [188.114.96.2] https://www.virustotal.com/en/ip-address/188.114.96.2/information/
2022-12-18 00:09:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.9:8443
2022-12-18 00:21:30	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-O
2022-12-18 00:23:19	Country	No	Country Name Extractor	0	1	2	0	None	Netherlands
2022-12-18 00:18:29	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.12:80
2022-12-18 00:19:24	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'81.88.58.196'}], u'result': [{u'environment_id': 100, u'job_id': u'58c13
2022-12-18 00:20:39	BGP AS Membership	No	Censys	0	0	1	0	None	8075

2022-12-18 00:06:11	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 16, u'threat_score': 35, u'compromised "Local\\SM0:7556:304:WilStaging_02"\n "Local\\ChromeProcessSingletonStartup!"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:7556:304 00000000-00007556]\n "a8df4246-6074-4dd8-ab45-c3b99ff35d09.tmp" has type "UTF-8 Unicode text with very long lines with no line termin [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Ad Blocking\\9533cb2f-21ec-4c23-9e8a-a151e5751c36.tmp]- [targetUID: 00000000-00007556]\n script files inside temp directory', u'attck_id_wiki': None, u'threat_level_human': u'suspicious', u'capec_id': None, u'attck_id': No 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'de 00000000-00007556-00000BE4-283951284235\n "C:\\Users\\HAPUBWS\\AppData\\Local\\Microsoft\\Edge\\User Data\\Subresource Filter\\Uninde
2022-12-18 00:03:10	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.233
2022-12-18 00:26:05	Country	No	Country Name Extractor	0	0	6	0	None	United States
2022-12-18 00:04:01	Physical Location	No	ipstack	0	0	2	0	None	Brazil
2022-12-18 00:20:42	Open TCP Port	No	LeakIX	0	0	3	0	None	81.88.48.102:80
2022-12-18 00:16:27	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	personasvietualiempre.virtualsi.repl.co
2022-12-18 00:03:10	Open TCP Port	No	SSL Certificate Analyzer	0	0	1	0	None	zerotwo-best-waifu.online:443
2022-12-18 00:06:40	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.1:443
2022-12-18 00:21:09	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:
2022-12-18 00:22:14	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-O
2022-12-18 00:02:44	Raw Data from RIRs	No	grep.app	0	0	1	0	None	{u'repo': {u'raw': u'billythegoat356/Hyperion'}, u'total_matches': {u'raw': u'1'}, u'content': {u'snippet': u'<table class="highlight
2022-12-18 00:25:39	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-185.w90-116.abo.wanadoo.fr
2022-12-18 00:21:34	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-O
2022-12-18 00:10:05	Linked URL - Internal	No	URLScan.io	1	0	1	0	None	http://zerotwo-best-waifu.online
2022-12-18 00:21:30	BGP AS Membership	No	Censys	0	0	2	0	None	13335
2022-12-18 00:09:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.10:443
2022-12-18 00:04:37	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 28, u'threat_score': 52, u'compromised FPS_BROWSER_USER_PROFILE_STRING="Default", FPS_BROWSER_APP_PROFILE_STRING="Internet Explorer""\n Process "msedge.exe" (UID: 00000000- "192.0.77.37:443"\n "192.0.77.2:443"\n "192.0.76.3:443"\n "142.251.214.136:443"\n "104.18.225.52:443"\n "68.183.31.14:443"\n "172.67. commandline "--single-argument https://pivigames.blog/" (UID: 00000000-00007776)\n Spawned process "msedge.exe" with commandline "--t "msedge.exe" with commandline "--type=renderer --disable-client-side-phishing-detection --displ ..." (UID: 00000000-00007412), Spawne u'relevance': 3, u'threat_level': 0, u'type': 9, u'description': u'Spawned process "msedge.exe" with commandline "--single-argument h disable-client-side-phishing-detection --displ ..." (UID: 00000000-00006872), Spawned process "msedge.exe" with commandline "--type=r
2022-12-18 00:04:10	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:28:20	Web Framework	No	Web Framework Identifier	0	0	3	0	None	jQuery
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date"
2022-12-18 00:05:37	Internet Name - Unresolved	No	Certificate Transparency	0	0	1	0	None	api.plague.fun
2022-12-18 00:03:08	Affiliate - IP Address	No	DNS Look-aside	1	0	2	0	None	34.149.204.193
2022-12-18 00:06:49	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 39:2f:d3:a5:c8:f5:ab:d1:13:70:69:a5:1d:f6:ba:07 Signature Algorithm: sha256WithRSA keyid:D5:FC:9E:0D:DF:1E:CA:DD:08:97:97:6E:2B:C5:5F:C5:2B:F5:EC:B8 Authority Information Access: OCSP - URI:http://ocsp.pki.goog/s/gts

2022-12-18 00:18:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.6:443
2022-12-18 00:03:16	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-103.w90-116.abo.wanadoo.fr
2022-12-18 00:19:06	Physical Location	No	ipstack	0	0	3	0	None	France
2022-12-18 00:06:13	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.co
2022-12-18 00:11:02	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.ca Registry Domain ID: 73359129-CIRA Registrar WHOIS Server: whois.ca.fury.ca Registrar URL: https://www.namechea Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please ask the Regis ns709.websitewelcome.com Name Server: ns710.websitewelcome.com DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: htt Registrant Email: Please ask the Registrar of Record identified in this output for information on how to contact the Registrant, Admi REDACTED FOR PRIVACY Billing City: REDACTED FOR PRIVACY Billing State/Province: REDACTED FOR PRIVACY Billing Postal Code: REDACTED FO
2022-12-18 00:23:33	Affiliate - Internet Name	No	DNS Raw Records	1	0	2	0	None	webmail-fr.setupdns.net
2022-12-18 00:13:51	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@ascio.com
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date"
2022-12-18 00:27:45	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	plague.org@contactprivacy.com
2022-12-18 00:09:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.11:8080
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	Mastodon-API (Category: social) https://mastodon.social/api/v2/search?q=rasputain
2022-12-18 00:03:22	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-111.w90-116.abo.wanadoo.fr
2022-12-18 00:21:23	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-O
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	wilson (Net ID: 00:02:2D:08:06:B3)
2022-12-18 00:09:40	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	accreditedhomegoodsonline.com
2022-12-18 00:06:55	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_HASHFILESWITCH_MUTEX"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_DOWNLOAD_ u'type': 8, u'description': u'Antivirus vendors marked dropped file "urlblockindex_1_.bin" as clean (type is "data")\n Antivirus vend u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_id_wiki': None, u'threat_level_human': u'informative', V2 Document Cannot read section info"- [targetUID: N/A]\n "~DF42CE4BD4D83F4862.TMP" has type "data"- Location: [%TEMP%\\~DF42CE4BD4D8 [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\MetaData\\7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776]- [targ Trident/7.0; rv:11.0) like Gecko\nAccept-Encoding: gzip, deflate\nHost: pichincha-serc.pichinchasc.repl.co\nDNT: 1\nConnection: Keep-
2022-12-18 00:04:07	Raw Data from RIRs	No	Hybrid Analysis	0	0	1	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised None, u'attck_id': u'T1071.001', u'relevance': 1, u'threat_level': 0, u'type': 2, u'description': u'"GET /W2gQQnU.png HTTP/1.1\nAccep "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\ZonesCacheCounterMutex"\ {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_ "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Internet Explorer\\DomainSuggestions\\en-US.4]- [targetUID: 00000000-00001500]\n "image HTTP/1.1\nAccept: */*\nAccept-Encoding: gzip, deflate\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nHos XW5oyMLA0~WHL#F4m[)MDw*dIm\nAt\nv1FAQQN7B9R~Xa|zo&kF+xCkCAzX;xS(A^Hku10:0#V%-/]W614IrQ^;"21Z@vZ%rO*-;b0nHv&Fm/ix,w1;JH\ndgnbI,/dAt<Vm
2022-12-18 00:05:00	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 69, u'compromised_ u'"\\Sessions\\1\\BaseNamedObjects\\IsoScope_704_IESQMMUTEX_0_519"\n "Local\\InternetShortcutMutex"\n "{66D0969A-1E86-44CF-B4EC-3806D u'description': u'"iexplore.exe" touched "Cor MIME Filter, CorFltr, CorFltr 1" (Path: "HKLM\\SOFTWARE\\CLASSES\\CLSID\\{1E66F26B-79EE "HKLM\\SOFTWARE\\CLASSES\\CLSID\\{00000106-0000-0010-8000-00AA006D2EA4}\\IMPLEMENTED CATEGORIES\\{00021493-0000-0000-C000-00000000004 {0000031A-0000-0000-C000-000000000046}\\IMPLEMENTED CATEGORIES\\{00021493-0000-0000-C000-000000000046}")\n "iexplore.exe" touched "DC 080027DFF835_.dat" has type "Composite Document File V2 Document Cannot read section info"\n "80237EE4964FC9C409AAF55BF996A292_D46D6F {u'category': u'Network Related', u'origin': u'String', u'identifier': u'string-3', u'name': u'Found potential URL in binary/memory',
2022-12-18	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.181

00:24:57									
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:16:57	HTTP Status Code	No	Web Spider	0	0	2	0	None	200
2022-12-18 00:21:17	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:
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	Steam (Category: gaming) https://steamcommunity.com/id/rasputain
2022-12-18 00:34:59	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.233] https://www.virustotal.com/en/ip-address/81.88.52.233/information/
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:8080
2022-12-18 00:03:33	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lhcp3235.webapps.net
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	Discogs (Category: music) https://www.discogs.com/user/rasputain
2022-12-18 00:27:12	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.ru
2022-12-18 00:09:31	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.169.215:8443
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:2095
2022-12-18 00:18:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.3:8080
2022-12-18 00:04:12	Linked URL - Internal	No	Hybrid Analysis	4	0	1	0	None	http://misogyny.wtf/grab/UsRjS959Rqm4sPG4
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	bbvacxx.repl.co
2022-12-18 00:21:06	Open TCP Port	No	Censys	0	0	2	0	None	172.67.147.230:2052
2022-12-18 00:17:08	Open TCP Port	No	SSL Certificate Analyzer	0	0	2	0	None	webmail.zerotwo-best-waifu.online:443
2022-12-18 00:18:23	IP Address	No	DNS Resolver	28	0	2	0	None	90.116.149.183
2022-12-18 00:12:05	Country	No	Country Name Extractor	0	1	4	0	None	Iceland
2022-12-18 00:33:43	Open TCP Port	No	Pulsedive	0	1	4	0	None	195.110.124.188:3389
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	provin894.hot93.repl.co
2022-12-18 00:21:13	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-18T00:20:43.126Z", "ip": "188.114.97.0", "location_updated_at": "2022-12-13T14:54:31.302828Z", "autonomo "koopervaringen.nl": {"record_type": "A", "resolved_at": "2022-10-13T17:36:35.577740211Z"}, "koopreacties.nl": {"record_type": "A", " 22T17:21:21.386128784Z"}, "lillakurorten.se": {"record_type": "A", "resolved_at": "2022-11-26T17:01:26.024528346Z"}, "wanbetalerslijs "resolved_at": "2022-12-09T12:12:48.971521181Z"}, "gunjehetmij.nl": {"record_type": "A", "resolved_at": "2022-11-22T17:20:37.41450941 "2022-12-08T12:26:19.009964762Z"}, "www.directlinks.nl": {"record_type": "A", "resolved_at": "2022-11-13T16:07:49.735746547Z"}, "twee "carrosserievag.be", "hanalytic.co.uk", "speurder-tips.nl", "welmakkelijker.nl", "www.directlinks.nl", "tweedehandsnu.nl", "girls4def oldie\" lang=\"en-US\"> <![endif]-->\n<!--[if IE 8]> <html class=\"no-js ie8 oldie\" lang=\"en-US\"> <![endif]-->\n<!--[if gt IE 8]><!
2022-12-18 00:21:17	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T22:41:02.660Z", "ip": "188.114.96.1", "location_updated_at": "2022-12-14T06:51:22.751367Z", "autonomo "resolved_at": "2022-10-15T13:31:47.102980654Z"}, "wolny.poker": {"record_type": "A", "resolved_at": "2022-10-23T17:07:04.797789596Z" 13T12:32:37.254071978Z"}, "test1-pointg.nc-testdomain2.club": {"record_type": "A", "resolved_at": "2022-12-05T12:32:16.018654402Z"}, "sign.moeking.me": {"record_type": "A", "resolved_at": "2022-09-28T16:39:39.465293148Z"}, "mail.lskala.com": {"record_type": "A", "re {"record_type": "A", "resolved_at": "2022-10-24T13:34:44.275517531Z"}, "mail.mardinscarf.com": {"record_type": "A", "resolved_at": "2 "939394.xyz", "edu.rabinia.com", "ritta.app", "ftp.baharelm.ir", "landing.makingprojec.com", "test5-pointg.nc-testdomain2.club", "pas [endif]-->\n<!--[if gt IE 8]><!--> <html class=\"no-js\" lang=\"en-US\"> <!--<![endif]-->\n<head>\n<title>Direct IP access not allowe
2022-12-	Malicious	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.234] https://www.virustotal.com/en/ip-address/81.88.52.234/information/

18 00:35:15	Affiliate IP Address								
2022-12-18 00:18:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.3:443
2022-12-18 00:18:08	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.2:443
2022-12-18 00:05:11	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised u'"\\Sessions\\1\\BaseNamedObjects\\IsoScope_b40_IESQMMUTEX_0_519"\n "Local\\InternetShortcutMutex"\n "{5312EE61-79E3-4A24-BFE1-132B8 u'relevance': 3, u'threat_level': 0, u'type': 8, u'description': u'Dropped file: "5DCLXO04.txt" - Location: [%APPDATA%\\Microsoft\\Wi has type "HTML document ASCII text with CRLF line terminators"- [targetUID: N/A]\n "en-US.4" has type "data"- Location: [%LOCALAPPDAT 2, u'description': u'Pattern match: "http://misogyny.wtf:2020/copy"\n Pattern match: "http://misogyny.wtf"'}, {u'category': u'Network u'malicious', u'capec_id': None, u'attck_id': None, u'relevance': 10, u'threat_level': 2, u'type': 12, u'description': u'No specific Control', u'informative_identifiers_count': 0, u'suspicious_identifiers_count': 0}], u'certificates': [], u'hosts': [u'20.226.83.185'
2022-12-18 00:25:45	Affiliate - Internet Name	No	DNS Resolver	1	0	4	0	None	ns.dominiando.us
2022-12-18 00:08:20	Netblock Membership	No	RIPE	1	0	2	0	None	172.67.144.0/20
2022-12-18 00:18:35	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.15:8443
2022-12-18 00:08:38	BGP AS Membership	No	RIPE	0	0	3	0	None	13335
2022-12-18 00:06:32	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 18, u'threat_score': None, u'compromis u'"\\Sessions\\1\\BaseNamedObjects\\Local\\SM0:7944:120:WilError_01"\n "Local\\SM0:8064:120:WilError_01"\n "Local\\SM0:8064:304:WilSt filesystem (MS-DOS OS/2 NT) original size modulo 2^32 14962921"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Default\\Cach [targetUID: N/A]\n "settings.dat" has type "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Edge\\User Data\\Crashpad\\settings.dat]- [t Data\\Default\\Code Cache\\js\\960087930daf924a_0]- [targetUID: 00000000-00007944]\n "11fcebfcf933fb1a_0" has type "data"- [targetUID u'suspicious', u'capec_id': None, u'attck_id': None, u'relevance': 5, u'threat_level': 1, u'type': 2, u'description': u'"C:\\Users\\H Data\\Default\\IndexedDB\\https_rolly-vortex.nugeshinia.repl.co_0.indexeddb.leveld" (Indicator: "microsoft\\edge\\user data") in Sour
2022-12-18 00:21:17	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.1:443
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:80
2022-12-18 00:08:33	Netblock Membership	No	RIPE	2	0	2	0	None	90.116.0.0/16
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	InterSolar (Net ID: 00:00:00:00:83:B5)
2022-12-18 00:18:31	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.13:8080
2022-12-18 00:06:49	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise u'origin': u'Network Traffic', u'identifier': u'network-0', u'name': u'Contacts domains', u'attck_id_wiki': None, u'threat_level_huma "ocsp.sca1b.amazontrust.com"\n "scontent-ord5-1.xx.fbcdn.net"\n "tr.snapchat.com"\n "video.nick313.repl.co"'}, {u'category': u'Genera [%APPDATA%\\Microsoft\\Windows\\Cookies\\LZ1YVEKK.txt]- [targetUID: 00000000-00003720]\n Dropped file: "EG03EPAK.txt" - Location: [%A "PJCSE9PV.txt" - Location: [%APPDATA%\\Microsoft\\Windows\\Cookies\\PJCSE9PV.txt]- [targetUID: 00000000-00003868]\n Dropped file: "PC "B039FEA45CB4CC4BBACFC013C7C55604_005284E085E122BD76B51F33745F7753" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptr [%LOCALAPPDATA%\\ow\\Microsoft\\CryptnetUrlCache\\Content\\6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442]- [targe
2022-12-18 00:26:24	Physical Location	No	MetaDefender	0	0	2	0	None	San Francisco, United States
2022-12-18 00:21:34	Open TCP Port	No	Censys	0	0	2	0	None	104.21.19.243:8880
2022-12-18 00:03:12	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	avaliabproviline.tio9865.repl.co
2022-12-18 00:20:56	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3031::ac43:93e6:80
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	jh00qe63.qw653bv.repl.co
2022-12-18 00:03:06	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	atlas.plague.fun

2022-12-18 00:21:37	Open TCP Port Banner	No	Censys	0	0	2	0	None	HTTP/1.1 200 OK X-Powered-By: Express Access-Control-Allow-Origin: * Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	usablewarpedusers.577dhooo.repl.co
2022-12-18 00:22:14	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:54	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date"
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	wordywealthycleaninstall.donverif0654.repl.co
2022-12-18 00:03:08	Affiliate - IP Address	No	DNS Look-aside	6	0	2	0	None	81.88.52.223
2022-12-18 00:32:21	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.148:80
2022-12-18 00:09:37	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	tyasochyhigh.ml
2022-12-18 00:12:19	Phone Number	No	Phone Number Extractor	3	0	2	0	None	+14259744689
2022-12-18 00:03:06	Internet Name	No	DNS Resolver	0	0	2	0	None	rasputain.fr
2022-12-18 00:27:03	Physical Location	No	MetaDefender	0	0	2	0	None	San Jose, United States
2022-12-18 00:22:04	BGP AS Membership	No	Censys	0	0	2	0	None	3215
2022-12-18 00:09:00	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.96.1:8443
2022-12-18 00:21:17	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-O
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:2052
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	tumblr (Category: images) https://rasputain.tumblr.com
2022-12-18 00:32:23	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.wtf
2022-12-18 00:16:59	HTTP Headers	No	Web Spider	0	0	4	0	None	{"content-length": "8698", "accept-ranges": "bytes", "last-modified": "Fri, 12 Feb 2021 14:43:40 GMT", "connection": "keep-alive", "e
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	vapor (Net ID: 00:02:2D:09:FB:FD)
2022-12-18 00:33:53	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.228] https://www.virustotal.com/en/ip-address/81.88.52.228/information/
2022-12-18 00:08:52	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.28.240:80
2022-12-18 00:20:52	Raw Data from RIRs	No	Censys	0	0	1	0	None	{"last_updated_at": "2022-12-18T00:13:55.162Z", "ip": "20.224.2.213", "location_updated_at": "2022-12-18T00:20:49.758804Z", "autonomo
2022-12-18 00:02:48	IPv6 Address	No	Mnemonic PassiveDNS	13	0	1	0	None	2606:4700:3037::6815:13f3
2022-12-18 00:21:47	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3032::ac43:8925:80
2022-12-18 00:08:43	Internet Name	No	DNS Resolver	0	0	2	0	None	www.zerotwo-best-waifu.online

2022-12-18 00:19:48	Malicious IP Address	Yes	VirusTotal	0	0	2	0	None	VirusTotal [20.226.56.97] https://www.virustotal.com/en/ip-address/20.226.56.97/information/
2022-12-18 00:18:27	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.11:80
2022-12-18 00:09:11	Physical Location	No	LeakIX	0	0	2	0	None	United States
2022-12-18 00:08:59	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'188.114.97.0', u'vendor': u'', u'port': u'443', u'transport u'country_iso_code': u'NL', u'city_name': u'Amsterdam', u'location': {u'lat': 52.3759, u'lon': 4.8975}, u'country_name': u'Netherlanc u'password': u'', u'noauth': False, u'key': u''}, u'software': {u'modules': None, u'version': u'', u'os': u'', u'name': u'cloudflare' u'North Holland'}, u'host': u'misibrowser.ga', u'summary': u'Date: Sun, 30 Oct 2022 13:50:04 GMT\r\nContent-Type: text/plain; charset u'6d1f2e7c9ee98731ce17441d7885c1ca501c58ace273eaf3d72dd424bf85c783', u'leak': {u'dataset': {u'files': 0, u'rows': 0, u'ransom_notes': close\r\nx-frame-options: SAMEORIGIN\r\nreferrer-policy: same-origin\r\nCache-Control: private, max-age=0, no-store, no-cache, must-r u'event_pipeline': [u'CertStream', u'l9scan', u'tcpid', u'HttpPlugin'], u'http': {u'status': 0, u'title': u'301 Moved Permanently', u
2022-12-18 00:09:52	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	blocuncrunducvelchna.gq
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ENHLG (Net ID: 00:01:36:5B:37:00)
2022-12-18 00:19:08	Raw Data from RIRs	No	ipapi.co	0	0	3	0	None	{u'region_code': u'52', u'country_tld': u'.it', u'ip': u'81.88.48.102', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2022-12-18 00:09:36	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.12:8443
2022-12-18 00:03:57	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	plague.ai
2022-12-18 00:21:37	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["9"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "X_Powered_By": "DISPLAY_UTF8", "Access_Control_Allow_Heade
2022-12-18 00:21:02	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-(
2022-12-18 00:27:10	Open TCP Port	No	Pulsedive	0	0	3	0	None	81.88.48.101:25
2022-12-18 00:12:31	URL (Purely Static)	No	Page Information	0	0	3	0	None	http://misogyny.wtf:2020/copy
2022-12-18 00:21:03	Web Technology	No	Web Server Identifier	0	0	3	0	None	Express
2022-12-18 00:03:09	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.231
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:2083
2022-12-18 00:11:50	Malicious Internet Name	Yes	CloudFlare Malware DNS	0	1	2	0	None	Blocked by CloudFlare DNS [www.zerotwo-best-waifu.online]
2022-12-18 00:09:54	Hosting Provider	No	Hosting Provider Identifier	0	1	1	0	None	Microsoft Azure: http://www.windowsazure.com/en-us/
2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	register.it: http://we.register.it/
2022-12-18 00:14:46	Malicious Internet Name	Yes	VirusTotal	0	1	1	0	None	VirusTotal [plague.fun] https://www.virustotal.com/en/domain/plague.fun/information/
2022-12-18 00:04:12	Linked URL - Internal	No	Hybrid Analysis	8	0	1	0	None	http://misogyny.wtf:2020/parser
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	ProCare-Guest (Net ID: 00:01:21:1C:30:F0)
2022-12-18 00:06:33	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.96.0:443
2022-12-18 00:13:36	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	rir@cloudflare.com
2022-12-18 00:21:03	Web Server	No	Web Server Identifier	0	0	2	0	None	Werkzeug/2.2.2 Python/3.9.11

2022-12-18 00:28:20	Web Framework	No	Web Framework Identifier	0	0	5	0	None	jQuery
2022-12-18 00:02:45	SSL Certificate - Issued by	No	CertSpotter	0	0	1	0	None	C=US,O=Google Trust Services LLC,CN=GTS CA 1P5
2022-12-18 00:02:47	SSL Certificate - Issued to	No	CertSpotter	0	0	1	0	None	CN=rasputain.fr
2022-12-18 00:09:48	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	autodiscover.sectraexpress.com
2022-12-18 00:21:51	Open TCP Port	No	Censys	0	0	2	0	None	172.67.137.37:2087
2022-12-18 00:16:55	Malicious Internet Name	Yes	CloudFlare Malware DNS	0	1	2	0	None	Blocked by CloudFlare DNS [smtp.zerotwo-best-waifu.online]
2022-12-18 00:16:27	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-SH X509v3 Basic Constraints: critical CA:FALSE CT Precertificate SCTs: Signed Certificate Timestamp: Version : v1 (0x0) Log ID : E8:3E:D 30:45:02:21:00:d8:35:e0:5c:fe:c9:39:b4:06:5a:95:36:1c: 73:f4:85:1c:c5:6e:6b:ef:48:76:d6:7f:a3:fe:55:ed:82:7f: c5:02:20:7f:8c:86:3a:6f
2022-12-18 00:21:20	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.1:2096
2022-12-18 00:12:05	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'NJ', u'country_tld': u'.us', u'ip': u'2606:4700:3033::6815:1cf0', u'currency_name': u'Dollar', u'currency': u'USD'
2022-12-18 00:02:43	SSL Certificate - Issued to	No	CertSpotter	0	0	1	0	None	CN=*.plague.fun
2022-12-18 00:25:39	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [188.114.97.0]
2022-12-18 00:24:57	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.180
2022-12-18 00:06:06	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	plague.fun
2022-12-18 00:21:06	Physical Location	No	Censys	0	0	2	0	None	United States, North America
2022-12-18 00:02:45	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: f4:f0:fa:2f:ab:28:c3:7d:0e:b0:02:5f:9f:06:b1:0c Signature Algorithm: sha256WithRSA keyid:D5:FC:9E:0D:DF:1E:CA:DD:08:97:97:6E:2B:C5:5F:C5:2B:F5:EC:B8 Authority Information Access: OCSP - URI:http://ocsp.pki.goog/s/gts
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	410HowardStudios (Net ID: 00:02:2D:00:25:63)
2022-12-18 00:14:05	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 configurati
2022-12-18 00:14:16	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:2096
2022-12-18 00:33:37	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.227] https://www.virustotal.com/en/ip-address/81.88.52.227/information/
2022-12-18 00:13:35	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	noc@cloudflare.com
2022-12-18 00:40:42	Similar Domain	Yes	TLD Searcher	1	0	1	0	None	misogyny.ca
2022-12-18 00:18:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.5:443
2022-12-18 00:08:30	Raw Data from RIRs	No	LeakIX	5	0	1	0	None	{u'Services': [{u'protocol': u'https', u'event_type': u'service', u'ip': u'188.114.96.3', u'vendor': u'', u'port': u'443', u'transpor u'TLSv1.3'}, u'mac': u'', u'ssh': {u'motd': u'', u'version': 0, u'banner': u'', u'fingerprint': u''}, u'reverse': u'', u'geoip': {u'r u'188.114.97.9', u'vendor': u'', u'port': u'443', u'transport': [u'tcp', u'tls', u'http'], u'event_source': u'HttpPlugin', u'network' u'banner': u'', u'fingerprint': u''}, u'reverse': u'', u'geoip': {u'region_iso_code': u'NL-NH', u'country_iso_code': u'NL', u'city_na u'2a06:98c1:3120:0:0:0:0:0/46'}, u'service': {u'credentials': {u'username': u'', u'raw': None, u'password': u'', u'noauth': False, u'

									chunked\r\nConnection: close\r\nCache-Control: max-age=3600\r\nExpires: Sun, 30 Oct 2022 20:20:51 GMT\r\nLocation: https://plague.fur u'', u'header': {u'server': u'cloudflare'}, u'length': 0, u'favicon_hash': u'', u'root': u''}, u'tags': [], u'ssl': {u'cypher_suite':
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	" (Cloaked) (Net ID: 00:01:36:59:CB:CF)
2022-12-18 00:16:27	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3
2022-12-18 00:09:34	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	enarag.za.com
2022-12-18 00:09:38	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.13:80
2022-12-18 00:23:00	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	3	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 5a:c8:d1:a7:f1:1c:c3:42:65:4b:ca:e7:c0:d9:70:ae Signature Algorithm: sha256WithRSA Usage: critical Digital Signature, Key Encipherment X509v3 Basic Constraints: critical CA:FALSE X509v3 Extended Key Usage: TLS Web Se E2:ED:A3:9D:81:F5:32:9A:05:0D:99:08:F4:E7:FD:A1: 4D:D8:BF:DF:4B:AA:82 Signed Certificate Timestamp: Version : v1 (0x0) Log ID : E8:3E
2022-12-18 00:02:48	IPv6 Address	No	Mnemonic PassiveDNS	13	0	1	0	None	2606:4700:3031::ac43:93e6
2022-12-18 00:04:47	Raw Data from RIRs	No	Maltiverse	3	0	2	0	None	{u'asn_registry': u'arin', u'country_code': u'US', u'classification': u'whitelist', u'asn_country_code': u'US', u'is_open_proxy': Fal
2022-12-18 00:17:08	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	2	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 5a:c8:d1:a7:f1:1c:c3:42:65:4b:ca:e7:c0:d9:70:ae Signature Algorithm: sha256WithRSA Usage: critical Digital Signature, Key Encipherment X509v3 Basic Constraints: critical CA:FALSE X509v3 Extended Key Usage: TLS Web Se E2:ED:A3:9D:81:F5:32:9A:05:0D:99:08:F4:E7:FD:A1: 4D:D8:BF:DF:4B:AA:82 Signed Certificate Timestamp: Version : v1 (0x0) Log ID : E8:3E
2022-12-18 00:09:24	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.7:443
2022-12-18 00:21:09	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T23:35:15.006Z", "ip": "188.114.96.0", "location_updated_at": "2022-12-14T07:30:02.870325Z", "autonomo "bj.klizi.cn": {"record_type": "CNAME", "resolved_at": "2022-12-14T08:35:45.163449865Z"}, "koopreacties.nl": {"record_type": "A", "re "www.joinapp.top": {"record_type": "A", "resolved_at": "2022-10-13T18:09:04.767251163Z"}, "wanbetalerslijst.nl": {"record_type": "A", 16T16:39:23.885828265Z"}, "troubleswith.nl": {"record_type": "A", "resolved_at": "2022-10-29T16:52:06.147706433Z"}, "gunjehetmij.nl": "2022-11-23T20:19:59.951708942Z"}, "markplaatstips.nl": {"record_type": "A", "resolved_at": "2022-11-10T16:21:23.839281327Z"}, "girls "mail.dumpjedureverzekering.nl", "verdubbelalles.nl", "enforcepages.online", "www.koopreacties.nl", "watchland.nl", "www.speurder-tip {"_encoding": {"User_Agent": "DISPLAY_UTF8", "Accept": "DISPLAY_UTF8"}, "User_Agent": ["Mozilla/5.0 (compatible; CensysInspect/1.1;
2022-12-18 00:06:31	Company Name	No	Company Name Extractor	0	0	2	0	None	NAMECHEAP INC
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:16:53	Company Name	No	Company Name Extractor	0	0	3	0	None	Cloudflare\, Inc.
2022-12-18 00:09:55	Hosting Provider	No	Hosting Provider Identifier	0	0	2	0	None	Cloudflare Inc: https://www.cloudflare.com/
2022-12-18 00:11:08	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: plague.co Registry Domain ID: D4A395B67AB204CFAABA57C93F6BB05A4-NSR Registrar WHOIS Server: whois.godaddy.com Registrar PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: RE Last update of WHOIS database: 2022-12-18T00:11:07Z <<< For more information on Whois status codes, please visit https://icann.org/ep portion thereof, is not allowed without .CO Internet's prior written permission. .CO Internet reserves the right to modify or change Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.c 2155 E Warner Rd Tech City: Tempe Tech State/Province: Arizona Tech Postal Code: 85284 Tech Country: US Tech Phone: +1.4806242599 Tec automated or robotic electronic processes designed to collect or compile this data for any purpose, including mining this data for yo
2022-12-18 00:31:50	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.133:80
2022-12-18 00:09:51	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	biolefirsmar.tk
2022-12-18 00:12:52	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'188.114.96.9', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2022-12-18 00:04:40	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'188.114.96.0'}], u'result': [{u'environment_id': 100, u'job_id': u'63237
2022-12-18 00:09:02	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.1:80
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:2087

2022-12-18 00:19:25	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [u'mydoom', u'upx'], u'crowdstrike_ai': None, u'total_processes': 2, u'threat_score': 1 "193.175.80.161:25"\n "17.171.2.72:25"\n "17.171.2.68:25"\n "17.172.224.47:25"\n "217.12.15.96:80"\n "209.202.251.1:80"\n "162.209.10 "\\Sessions\\1\\BaseNamedObjects\\Local\\WininetConnectionMutex"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\WininetProxyRegistryMutex .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)\nHost: search.lycos.com\nConnection: Keep-Alive"\n "GET /?fr=altavista H PHPSESSID=nk5rco1pvk06lvada52c9f0op3"\n "GET /default.asp?lpv=1&loc=searchhp&tab=web&query=reply+unicode.org HTTP/1.1\nAccept: */*\nA .NET4.0C; .NET4.0E)\nHost: search.lycos.com\nConnection: Keep-Alive\nCookie: PHPSESSID=nk5rco1pvk06lvada52c9f0op3"\n "GET /default.as Media Center PC 6.0; .NET4.0C; .NET4.0E)\nHost: search.yahoo.com\nConnection: Keep-Alive\nCookie: B=dbc2c8lcc2fkn&b=3&s=um; sSN=K6M9X
2022-12-18 00:09:33	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.11:80
2022-12-18 00:13:55	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:09:52	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	bonanzatradisibet.com
2022-12-18 00:25:43	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-192.w90-116.abo.wanadoo.fr
2022-12-18 00:21:02	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: -
2022-12-18 00:16:57	Linked URL - Internal	No	Web Spider	4	0	3	0	None	http://webmail.zerotwo-best-waifu.online/js/vendor/bootstrap.min.js
2022-12-18 00:03:11	Affiliate - Domain Name	No	DNS Resolver	2	0	3	0	None	googleusercontent.com
2022-12-18 00:09:43	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.3:8443
2022-12-18 00:21:54	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T20:48:43.322Z", "ip": "104.21.7.179", "location_updated_at": "2022-12-14T04:34:49.009243Z", "autonomo "2022-12-11T14:58:57.277135763Z"}, "mkt.mariahost.com.br": {"record_type": "A", "resolved_at": "2022-11-30T12:18:50.807559206Z"}, "cl "resolved_at": "2022-11-29T12:06:58.692918972Z"}, "www.instintoconquistador.com.cdn.cloudflare.net": {"record_type": "A", "resolved_a {"record_type": "A", "resolved_at": "2022-12-05T15:29:39.708544965Z"}, "olwitarventneeds.tk": {"record_type": "A", "resolved_at": "20 11-30T13:47:32.665078261Z"}, "tehnopolimer.ru": {"record_type": "A", "resolved_at": "2022-12-14T17:34:19.679431316Z"}, "www.ideometri "CNAME", "resolved_at": "2022-12-14T17:17:49.475328681Z"}, "select702rope.xyz": {"record_type": "A", "resolved_at": "2022-12-14T17:55 13T12:16:56.526232800Z"}, "speedtest.dylansheffer.app": {"record_type": "A", "resolved_at": "2022-11-25T12:05:41.308917269Z"}, "www.f
2022-12-18 00:12:29	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'compromised_ "IsoScope_c84_IE_EarlyTabStart_0xe68_Mutex"\n "{66D0969A-1E86-44CF-B4EC-3806DDDA3B5D}"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\Zor u'description': u'"urlblockindex_1_.bin" has type "data"- [targetUID: N/A]\n "RecoveryStore._5FC32A7B-771D-11ED-B8BD-0800278A77A4_.da "data"- Location: [%TEMP%\\~DFABD3E3197957479F.TMP]- [targetUID: 00000000-00003204]\n "EWM02H3X.txt" has type "ASCII text"- Location: u'threat_level': 1, u'type': 2, u'description': u'Potential IP "188.114.97.3" found in string "https://188.114.97.3/"\n Potential IP u'https://188.114.97.3/', u'submission_id': u'63922bb58f5d337c6c22e8a0', u'created_at': u'2022-12-08T18:23:49+00:00', u'filename': No u'Network Traffic', u'identifier': u'network-1', u'name': u'Contacts server', u'attck_id_wiki': None, u'threat_level_human': u'inform
2022-12-18 00:13:46	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	4	0	None	registrar-abuse@cloudflare.com
2022-12-18 00:30:56	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	reactivation-pending@mail.withheldforprivacy.com
2022-12-18 00:05:16	Account on External Site	No	Account Finder	0	0	2	0	None	Wikipedia (Category: news) https://en.wikipedia.org/wiki/User:rasputain
2022-12-18 00:19:06	Physical Location	No	ipstack	0	0	3	0	None	Italy
2022-12-18 00:19:12	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	{u'count': 6, u'search_terms': [{u'id': u'host', u'value': u'81.88.48.101'}], u'result': [{u'environment_id': 100, u'job_id': u'5d01f None, u'type_short': u'js', u'size': 713007}, {u'environment_id': 100, u'job_id': u'58eb94bcaac2ed1c6c81f64e', u'analysis_start_time'
2022-12-18 00:09:22	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': None, u'Leaks': None}
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	infoworld (Net ID: 00:02:2D:01:DD:9B)
2022-12-18 00:33:43	Open TCP Port	No	Pulsedive	0	0	4	0	None	195.110.124.188:21
2022-12-18	Physical Location	No	ipapi.co	0	0	1	0	None	Amsterdam, North Holland, NH, Netherlands, NL

00:12:01									
2022-12-18 00:35:32	Malicious Affiliate IP Address	Yes	VirusTotal	0	0	3	0	None	VirusTotal [81.88.52.235] https://www.virustotal.com/en/ip-address/81.88.52.235/information/
2022-12-18 00:22:21	Affiliate - Domain Whois	No	Whois	4	0	4	0	None	Domain Name: SETUPDNS.NET Registry Domain ID: 1581585796_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.register.it Registrar URL: htt except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Servic and Registrars. Domain Name: SETUPDNS.NET Registry Domain ID: 1581585796_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.register.it Re Tech Organization: GLOBAL DOMAIN PRIVACY Tech Street: Via Zanchi 22 Tech City: Bergamo Tech State/Province: BG Tech Postal Code: 2412
2022-12-18 00:04:12	Linked URL - Internal	No	Hybrid Analysis	4	0	1	0	None	http://misogyny.wtf/inject/UsRjS959Rqm4sPG4
2022-12-18 00:19:19	Raw Data from RIRs	No	Hybrid Analysis	0	0	3	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 7, u'threat_score': 100, u'compromised 206.214.220.79:8080\nConnection: Keep-Alive\nCache-Control: no-cache"\n "GET / HTTP/1.1\nCookie: 1E42=MBQfjXGAReVCY90IE5Tx6FfJ7kPkLiA 3705=UXLJV+AL9Wtp8GdISnKEM0C66vaznRXWu27GhaiiZ/WfqrwSD5he94GKvB5AbRb4DHKHjLcEENswsuEj0S+dvzTq6IU2UF8+VwIB+9+UaI18Qo2LOmtmDuckOcREVevN Control: no-cache"\n "GET / HTTP/1.1\nCookie: 661E=gtJNav4dB+bHZ9KXonqN1m+c8RbhyqinqoiOq8myuuqUesJRUBxONTdATrziIFLdC06uFHZRNkNZa2WksO 173.230.137.155:8080\nConnection: Keep-Alive\nCache-Control: no-cache"\n "GET / HTTP/1.1\nCookie: A537=UniLCdSHBDnkBq5RCN+a5eGN/ih+P0 BC42=O9H7rwg2LDzEbD72eAujPBK7HYFGQcZv0DkPHAjqVUx2ayQSdsHtXAIUufaBYCXygohiKxKBP6Z3oqx2W8bepHxLLq3Wi56wflVoesuyIOnUPobYCi9MpypROj/q8Ytb EA=iL6lSYNFF52Rmv5KENNAPwgfNTENgqW3DJgpJeUaTs8M+ioDK66SDgOhmryUAFMQ3iD5CrLKFOMR7Dk/+jCDBo1RzmnKoj6fAzN4LGp6Zes9t5t8JQ+LEVFlU1tmRIvbZe 5812=aTSVQjO3jBoTh0QNRIkpRPjM7DzVR5xLF9akSUFjyFwCaDhHNWEgIv9kIiK5HTRMfK9XNWGR9uSWGFpwjI7/za5/CM1PwPFUJPQnWF9UFaYYLYPQ0Oxx8QQ2Abs+kJZa
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:2052
2022-12-18 00:19:07	Country	No	Country Name Extractor	0	0	4	0	None	United States
2022-12-18 00:21:23	Open TCP Port	No	Censys	0	0	2	0	None	2606:4700:3032::ac43:be81:80
2022-12-18 00:21:06	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["253"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date": "DISPLAY_UTF8", "Connec
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	wooowoowokjbgdhm.provhvfvqqho.repl.co
2022-12-18 00:03:05	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:d8:e8:f9:6e:af:5c:60:20:62:8a:c9:01:2c:b1:dd:b1:ef Signature Algorithm: sha256W X509v3 Authority Key Identifier: keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1 Authority Information Access: OCSP e4:26:28:75:34:87:50:e0:1b:62:3a:4b:eb:c8:bd:8f:50:e4: 53:a4:ac:3f:f9:38:25:0e:15:6b:4f:c7:67:d3:fa:70:c7:d8: e6:29:7c:90:6f:27:66:e9
2022-12-18 00:19:06	Physical Location	No	ipstack	0	0	3	0	None	Italy
2022-12-18 00:08:40	BGP AS Membership	No	RIPE	0	0	3	0	None	15169
2022-12-18 00:09:18	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.4:8443
2022-12-18 00:03:11	Affiliate - IP Address	No	DNS Look-aside	2	0	2	0	None	81.88.52.240
2022-12-18 00:16:52	Software Used	Yes	Tool - Wappalyzer	0	0	2	0	None	Bootstrap
2022-12-18 00:04:48	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:f8:40:07:a9:2a:29:fa:95:e2:5f:ea:f2:e9:75:79:57:8e Signature Algorithm: sha256W fc:a2:6d:82:28:e4:4c:91:9c:41:cb:49:9c:63:4a:05:00:10: 2b:5b:42:3b:ca:d7:a6:77:ee:3e:fa:ba:30:7d:73:b6:2e:2c: 86:e2:ce:98:ab:39:f4:51
2022-12-18 00:03:27	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	198.204.149.34.bc.googleusercontent.com
2022-12-18 00:04:11	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	cdnjs.cloudflare.com
2022-12-18 00:02:50	IPv6 Address	No	Mnemonic PassiveDNS	13	0	1	0	None	2606:4700:3031::6815:7b3
2022-12-18 00:25:38	Affiliate - Internet Name	No	DNS Resolver	0	0	4	0	None	lfbn-nic-1-313-181.w90-116.abo.wanadoo.fr
2022-12-18 00:03:06	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:05:62:a3:2a:56:6a:d6:e7:de:85:5f:24:ee:fd:d0:9c:8a Signature Algorithm: sha256W Identifier: keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6 Authority Information Access: OCSP - URI:http://r3.o.le 8c:45:b9:a2:ea:86:2a:ca:78:fe:d4:2c:98:57:dd:08:e1:72: 5a:16:be:91:29:90:d9:35:81:21:d8:c1:95:38:43:d7:29:3e: dc:73:af:9b:cd:6b:92:1e
2022-12-18 00:31:18	Similar Domain - Whois	No	Whois	0	0	2	0	None	Domain Name: plague.games Registry Domain ID: f12e18082d0d4e8986ee91e215341031-DONUTS Registrar WHOIS Server: http://whois.zzy.cn Reg Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record i circumstances may this data be used to: a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of request, where it can be reasonably confirmed that the requester holds a specific legitimate interest and a proper legal basis for ac
2022-12-	SSL	No	SSL Certificate	0	0	3	0	None	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Organization Validation Secure Server CA

18 00:23:00	Certificate - Issued by		Analyzer						
2022-12-18 00:11:03	Affiliate - Domain Whois	No	Whois	5	0	3	0	None	Domain Name: REGISTRAR-SERVERS.COM Registry Domain ID: 1326800137_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registr to view the registrar's reported date of expiration for this registration. TERMS OF USE: You are not authorized to access or query ou may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right t Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Em
2022-12-18 00:02:43	SSL Certificate - Raw Data	No	CertSpotter	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 04:6b:c5:5a:1c:aa:de:11:25:3a:85:ac:27:46:ac:84:c2:a9 Signature Algorithm: ecdsa-w ecdsa-with-SHA256 30:46:02:21:00:C2:6E:51:36:59:0D:CE:4E:3E:93:68: B7:52:EC:0D:A3:64:2B:FD:C3:C4:8C:29:56:48:6F:95: D8:9B:CC:44:7E:02
2022-12-18 00:13:28	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	2	0	None	abuse@enom.com
2022-12-18 00:16:46	Co-Hosted Site	No	ThreatMiner	0	0	2	0	None	ebruouryverify.ebrouinforma.repl.co
2022-12-18 00:03:25	SSL Certificate - Raw Data	No	Certificate Transparency	1	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:05:62:a3:2a:56:6a:d6:e7:de:85:5f:24:ee:fd:d0:9c:8a Signature Algorithm: sha256W Identifier: keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6 Authority Information Access: OCSP - URI:http://r3.o.le
2022-12-18 00:06:02	Affiliate - Domain Name	No	DNS Resolver	0	0	2	0	None	registrar-servers.com
2022-12-18 00:24:05	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	chacha20-poly1305@openssh.com
2022-12-18 00:13:56	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:09:46	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	arro-studio.com
2022-12-18 00:24:41	Physical Location	No	MetaDefender	0	0	1	0	None	Amsterdam, Netherlands
2022-12-18 00:08:59	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.0:8080
2022-12-18 00:04:28	Affiliate - Internet Name	No	DNS Raw Records	1	0	1	0	None	eforward2.registrar-servers.com
2022-12-18 00:21:09	Open TCP Port	No	Censys	0	0	2	0	None	188.114.96.0:443
2022-12-18 00:22:14	Open TCP Port	No	Censys	0	0	2	0	None	172.67.169.215:2095
2022-12-18 00:21:11	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	<no ssid> (Net ID: 00:02:2D:03:10:83)
2022-12-18 00:16:59	Web Content Type	No	Web Spider	0	0	4	0	None	text/css
2022-12-18 00:21:23	Raw Data from RIRs	No	Censys	0	0	2	0	None	{"last_updated_at": "2022-12-17T20:22:45.925Z", "ip": "2606:4700:3032::ac43:be81", "location_updated_at": "2022-12-15T10:47:52.536571 25T17:18:30.899764295Z"}, "rouzzz.tk": {"record_type": "AAAA", "resolved_at": "2022-11-27T16:33:19.875741780Z"}, "drafexinte.cf": {"r {"record_type": "AAAA", "resolved_at": "2022-12-02T17:25:07.932475201Z"}, "saymulbestpropunes.cf": {"record_type": "AAAA", "resolved_ 04T15:28:45.315201663Z"}, "squarerxylawthoulich.tk": {"record_type": "AAAA", "resolved_at": "2022-11-03T16:35:32.240609622Z"}, "itali {"record_type": "AAAA", "resolved_at": "2022-11-26T16:49:44.449163363Z"}, "searchdoctors.org": {"record_type": "AAAA", "resolved_at": "sheylarivera.com": {"record_type": "AAAA", "resolved_at": "2022-11-21T13:46:57.180736459Z"}, "pjou77g.cn": {"record_type": "AAAA", " "webmail.egwunso.com": {"record_type": "AAAA", "resolved_at": "2022-11-11T13:12:29.864284296Z"}, "trx.video": {"record_type": "AAAA",
2022-12-18 00:41:03	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@namecheap.com
2022-12-18 00:21:37	Physical Location	No	Censys	0	0	2	0	None	Campinas, Sao Paulo, Brazil, South America
2022-12-18 00:04:01	Physical Location	No	ipstack	0	0	2	0	None	United States

2022-12-18 00:04:02	Physical Location	No	ipstack	0	0	2	0	None	United States
2022-12-18 00:26:48	Affiliate - Domain Whois	No	Whois	0	0	6	0	None	Domain name: dominiando.uk Data validation: Nominet was able to match the registrant's name and address against a 3rd party data sour
2022-12-18 00:21:34	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:03:11	Affiliate - Domain Name	No	DNS Resolver	2	0	3	0	None	webapps.net
2022-12-18 00:04:04	Web Technology	No	Tool - WhatWeb	0	0	1	0	None	Python
2022-12-18 00:12:28	Raw Data from RIRs	No	ipapi.co	0	0	2	0	None	{u'region_code': u'NJ', u'country_tld': u'.us', u'ip': u'2606:4700:3032::ac43:8925', u'currency_name': u'Dollar', u'currency': u'USD'
2022-12-18 00:20:52	BGP AS Membership	No	Censys	0	0	1	0	None	8075
2022-12-18 00:24:07	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	gdpr-masking@gdpr-masked.com
2022-12-18 00:18:17	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.6:8080
2022-12-18 00:03:30	Internet Name - Unresolved	No	DNS Resolver	0	0	2	0	None	api.plague.fun
2022-12-18 00:13:55	HTTP Status Code	No	Web Spider	0	0	2	0	None	None
2022-12-18 00:08:36	Open TCP Port	No	LeakIX	0	0	1	0	None	137.117.157.128:80
2022-12-18 00:20:49	BGP AS Membership	No	Censys	0	0	1	0	None	8075
2022-12-18 00:08:22	Physical Location	No	Fraudguard	0	0	1	0	None	Netherlands, North Holland, Amsterdam
2022-12-18 00:07:10	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 77, u'compromised_ touched "Internet Explorer(Ver 1.0)" (Path: "HKCU\\CLSID\\{0002DF01-0000-0000-C000-000000000046}\\TREATAS")\n "iexplore.exe" touched 00AA006946EE}\\TREATAS")\n "IEXPLORE.EXE" touched "Office Document Cache Handler" (Path: "HKLM\\SOFTWARE\\CLASSES\\WOW6432NODE\\CLSID u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 7, u'description': u'"bor.cestval u'description': u'"IEXPLORE.EXE" (Path: "HKLM\\SYSTEM\\CONTROLSET001\\CONTROL\\NLS\\LANGUAGE"; Key: "INSTALLLANGUAGEFALLBACK")'}, {u' "57C8EDB95DF3F0AD4EE2DC2B8CFD4157" has type "Microsoft Cabinet archive data 4817 bytes 1 file"\n "JTUHjIg1_i6t8kCHKm4532VJOt5-QNFgpCt "IEXPLORE.EXE" (Path: "HKLM\\SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\APP PATHS\\IEXPLORE.EXE")'}, {u'category': u'Network Relat
2022-12-18 00:06:47	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': u'Windows Gui', u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 1, u'threat_score': 100, u'c "ReadProcessMemory" (Indicator: "ReadProcessMemory")\n "WriteProcessMemory" (Indicator: "WriteProcessMemory")\n "GetProcAddress" (Inc (Indicator: "select"), "{1f676c76-80e1-4239-95bb-83d0f6d0da78}" />-->\n Windows 10 -->\n <supportedOS Id="{8e0f7a12-bfb3-4fe8-b9a5-48 "HKCU\\SOFTWARE\\POLICIES\\MICROSOFT\\SYSTEMCERTIFICATES\\CA\\CRLS"; Key: "")\n "m3-ge3Gj.exe" (Path: "HKCU\\SOFTWARE\\POLICIES\\MICR "HKCU\\SOFTWARE\\POLICIES\\MICROSOFT\\SYSTEMCERTIFICATES\\TRUST"; Key: "")\n "m3-ge3Gj.exe" (Path: "HKCU\\SOFTWARE\\POLICIES\\MICROSO u'capec_id': None, u'attck_id': None, u'relevance': 1, u'threat_level': 0, u'type': 0, u'description': u'"8d0dbcd19eb9014afee5433bf54 u'CAPEC-203', u'attck_id': u'T1112', u'relevance': 10, u'threat_level': 0, u'type': 3, u'description': u'"m3-ge3Gj.exe" (Path: "HKLM\
2022-12-18 00:12:33	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 35, u'compromised_ deflate\nHost: performance.radar.cloudflare.com\nDNT: 1\nConnection: Keep-Alive" (Indicator: "user-agent: ")'}, {u'category': u'Gener 0, u'type': 7, u'description': u'"188.114.97.3:80"\n "104.18.31.78:443"'}, {u'category': u'Unusual Characteristics', u'origin': u'Bir [%APPDATA%\\Microsoft\\Windows\\Cookies\\63CJVUP7.txt]- [targetUID: 00000000-00002832]\n "LM0USI2F.txt" has type "ASCII text"- Locati 32x32 32 bits/pixel"- [targetUID: N/A]\n "~DF6F835D267B734551.TMP" has type "data"- Location: [%TEMP%\\~DF6F835D267B734551.TMP]- [tar application/javascript, */*;q=0.8\nReferer: http://188.114.97.3/\nAccept-Language: en-US\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Tr None, u'interesting': False, u'error_type': None, u'state': u'SUCCESS', u'entrypoint': None, u'mitre_attcks': [{u'parent': None, u'at
2022-12-18 00:03:23	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	lfbn-nic-1-332-112.w90-116.abo.wanadoo.fr
2022-12-18 00:20:40	Raw Data from RIRs	No	LeakIX	0	0	3	0	None	{u'Services': None, u'Leaks': None}
2022-12-18 00:21:09	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-C
2022-12-18 00:56:41	Similar Domain - Whois	No	Whois	1	0	2	0	None	Domain Name: MISOGYNY.NET Registry Domain ID: 1847059997_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: htt query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to right to modify these terms at any time. The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars. Domain Name: MI

									Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Post written permission of this registrar. By submitting an inquiry, you agree to these terms and limitations of warranty. In particular,
2022-12-18 00:37:36	Similar Domain	Yes	TLD Searcher	0	0	1	0	None	plague.myds.me
2022-12-18 00:04:57	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': None, u'compromise "IsoScope_714_ConnHashTable<1812>_HashTable_Mutex"\n "UpdatingNewTabPageData"\n "Local\\ZonesCacheCounterMutex"\n "Local\\URLBLOCK_F "PSFactoryBuffer" (Path: "HKLM\\SOFTWARE\\CLASSES\\CLSID\\{057EEE47-2572-4AA1-88D7-60CE2149E33C}")\n "iexplore.exe" touched "Network 2F70F99015C2}\\IMPLEMENTED CATEGORIES\\{00021493-0000-0000-C000-000000000046}")\n "iexplore.exe" touched "ImeCommonAPIClassFactory_K (Path: "HKLM\\SOFTWARE\\CLASSES\\CLSID\\{2206CDB0-19C1-11D1-89E0-00C04FD7A829}\\IMPLEMENTED CATEGORIES\\{00021493-0000-0000-C000-0000 "favicon_2_.ico" has type "MS Windows icon resource - 1 icon 32x32"\n "search__0633EE93-D776-472f-A0FF-E1416B8B2E3A_.ico" has type " 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,
2022-12-18 00:08:26	Internet Name	No	Certificate Transparency	7	0	1	0	None	www.zerotwo-best-waifu.online
2022-12-18 00:12:51	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'188.114.97.3', u'currency_name': u'Euro', u'currency': u'EUR', u'country_pop
2022-12-18 00:26:31	Malicious IP Address	Yes	MetaDefender	0	1	2	0	None	webroot.com [104.21.7.179]
2022-12-18 00:04:45	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 50, u'compromised_ "\\Sessions\\1\\BaseNamedObjects\\Local\\VERMGMTBlockListFileMutex"'}, {u'category': u'General', u'origin': u'Network Traffic', u'ide 0548-48B1-A6EE-88BD00B4A5E7}\\TREATAS")\n "iexplore.exe" touched "Task Bar Communication" (Path: "HKLM\\SOFTWARE\\CLASSES\\CLSID\\{56 "IEXPLORE.EXE" touched "Browser Application State" (Path: "HKCU\\WOW6432NODE\\CLSID\\{E569BDE7-A8DC-47F3-893F-FD2B31B3EEFD}")\n "IEXP "6BADA8974A10C4BD62CC921D13E43B18_28DEA62A0AE77228DD387E155AD0BA27" has type "data"\n "~DFF33487CE549C314A.TMP" has type "data"\n "Re u'CAPEC-647', u'attck_id': u'T1012', u'relevance': 10, u'threat_level': 0, u'type': 3, u'description': u'"iexplore.exe" (Path: "HKCU\ {u'category': u'Unusual Characteristics', u'origin': u'Binary File', u'identifier': u'binary-5', u'name': u'Drops cabinet archive fil
2022-12-18 00:21:09	Physical Location	No	Censys	0	0	2	0	None	Amsterdam, North Holland, 1012, Netherlands, Europe
2022-12-18 00:03:11	Affiliate - Internet Name	No	DNS Resolver	1	0	2	0	None	188.204.149.34.bc.googleusercontent.com
2022-12-18 00:09:54	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	brunildelucciano.xyz
2022-12-18 00:08:52	Open TCP Port	No	LeakIX	0	0	2	0	None	104.21.28.240:8443
2022-12-18 00:21:17	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:13:36	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@cloudflare.com
2022-12-18 00:12:57	Malicious IP on Same Subnet	Yes	blocklist.de	0	0	2	0	None	blocklist.de List [137.117.0.0/16] http://lists.blocklist.de/lists/all.txt
2022-12-18 00:17:08	SSL Certificate Host Mismatch	Yes	SSL Certificate Analyzer	0	0	2	0	None	*.amen.fr, amen.fr
2022-12-18 00:05:09	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 100, u'compromised None, u'attck_id': u'T1071.001', u'relevance': 1, u'threat_level': 0, u'type': 2, u'description': u'"GET /W2gQQnU.png HTTP/1.1\nAccep "\\Sessions\\1\\BaseNamedObjects\\Local\\URLBLOCK_DOWNLOAD_MUTEX"\n "\\Sessions\\1\\BaseNamedObjects\\Local\\ZonesCacheCounterMutex"\ {u'category': u'Installation/Persistence', u'origin': u'Binary File', u'identifier': u'binary-0', u'name': u'Dropped files', u'attck_ "data"- Location: [%LOCALAPPDATA%\\Microsoft\\Internet Explorer\\DomainSuggestions\\en-US.4]- [targetUID: 00000000-00001500]\n "image HTTP/1.1\nAccept: */*\nAccept-Encoding: gzip, deflate\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\nHos XW5oyMLA0~WHL#F4m[)MDw*dIm\nAt\nv1FAQQN7B9R~Xa|zo&kF+xCkCAzX;xS(A^Hku10:0#V%-/]W614IrQ^;"21Z@vZ%rO*-;b0nHv&Fm/ix,w1;JH\ndgnbI,/dAt<Vm
2022-12-18 00:18:08	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.2:8443
2022-12-18 00:06:15	Web Content Type	No	Web Spider	0	0	1	0	None	text/html; charset=utf-8
2022-12-18 00:02:39	IP Address	No	SpiderFoot UI	13	0	0	0	None	4.228.83.86
2022-12-18 00:09:38	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.13:443
2022-12-18 00:22:04	Netblock Membership	No	Censys	0	0	2	0	None	90.116.0.0/16
2022-12-18 00:28:12	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	plague@koptevo.net

2022-12-18 00:03:24	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	181.204.149.34.bc.googleusercontent.com
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	krillnet (Net ID: 00:01:8E:15:D4:A6)
2022-12-18 00:03:26	Affiliate - Internet Name	No	DNS Resolver	0	0	3	0	None	187.204.149.34.bc.googleusercontent.com
2022-12-18 00:09:27	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'https', u'event_type': u'service', u'ip': u'34.149.204.188', u'vendor': u'', u'port': u'443', u'transp {u'motd': u'', u'version': 0, u'banner': u'', u'fingerprint': u''}, u'reverse': u'', u'geoip': {u'region_iso_code': u'US-MO', u'count u'type': u'', u'severity': u'', u'stage': u''}, u'event_pipeline': [u'CertStream', u'l9scan', u'tcpid', u'HttpPlugin'], u'http': {u's chunked\r\n\nPage title: Run this Repl to see the results here.', u'time': u'2022-11-04T13:58:07.142072015Z'}, {u'protocol': u'http', {u'region_iso_code': u'US-MO', u'country_iso_code': u'US', u'city_name': u'Kansas City', u'location': {u'lat': 39.1027, u'lon': -94.5 []], u'ssl': {u'cypher_suite': u'', u'jarm': u'', u'certificate': {u'domain': None, u'cn': u'', u'valid': False, u'not_after': u'0001- u'6d1f2e7c9fe9889bd904db585ef3c0324ee34bc4eeb3ad23c386006fe4b42ba6', u'leak': {u'dataset': {u'files': 0, u'rows': 0, u'ransom_notes':
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	GP (Net ID: 00:01:24:F1:7F:54)
2022-12-18 00:15:33	Malicious Internet Name	Yes	VirusTotal	0	1	1	0	None	VirusTotal [zerotwo-best-waifu.online] https://www.virustotal.com/en/domain/zerotwo-best-waifu.online/information/
2022-12-18 00:09:15	Raw Data from RIRs	No	LeakIX	0	0	2	0	None	{u'Services': [{u'protocol': u'http', u'event_type': u'service', u'ip': u'20.226.83.185', u'vendor': u'', u'port': u'80', u'transport {u'region_iso_code': u'BR-SP', u'country_iso_code': u'BR', u'city_name': u'Campinas', u'location': {u'lat': -22.9035, u'lon': -47.056 Python/3.9.11'}, u'length': 0, u'favicon_hash': u'', u'root': u''}, u'tags': [], u'ssl': {u'cypher_suite': u'', u'jarm': u'', u'certi u'2.2.2', u'os': u'', u'name': u'Werkzeug', u'fingerprint': u''}}, u'event_fingerprint': u'6d1f2e7c95e97940a96e74f75c97a5c4e667444107 14T16:13:08.569376224Z'}], u'Leaks': None}
2022-12-18 00:18:23	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.9:8443
2022-12-18 00:11:09	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 % administr
2022-12-18 00:03:10	SSL Certificate - Raw Data	No	SSL Certificate Analyzer	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 06:3f:d1:a5:92:cd:9c:90:1c:37:fe:d5:5f:00:4b:51 Signature Algorithm: sha256WithRSA Key Usage: critical Digital Signature, Key Encipherment X509v3 Basic Constraints: critical CA:FALSE X509v3 Extended Key Usage: TLS We 79:CC:54:BE:98:3D:56:78:1C:E9:A5:43:73:6C:54:FD: A2:57:9B:67:6E:F6:02 Signed Certificate Timestamp: Version : v1 (0x0) Log ID : E8:3E
2022-12-18 00:08:26	Netblock Membership	No	RIPE	1	0	2	0	None	172.67.176.0/20
2022-12-18 00:21:09	HTTP Headers	No	Censys	0	0	2	0	None	{"Content_Length": ["151"], "_encoding": {"Content_Length": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ray": "DISPLAY_UTF8", "Conr
2022-12-18 00:21:10	WiFi Access Point Nearby	No	Wigle.net	0	0	5	0	None	zoom (Net ID: 00:01:38:A4:44:3A)
2022-12-18 00:21:02	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-(
2022-12-18 00:06:51	Open TCP Port	No	Pulsedive	0	0	2	0	None	172.67.137.37:8080
2022-12-18 00:21:23	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: -
2022-12-18 00:23:28	Raw DNS Records	No	DNS Raw Records	0	0	2	0	None	www.zerotwo-best-waifu.online. 900 IN CNAME zerotwo-best-waifu.online.
2022-12-18 00:04:47	Raw Data from RIRs	No	Hybrid Analysis	0	0	2	0	None	[{u'subsystem': None, u'classification_tags': [], u'crowdstrike_ai': None, u'total_processes': 3, u'threat_score': 50, u'compromised_ u'Binary File', u'identifier': u'binary-16', u'name': u'Drops files marked as clean', u'attck_id_wiki': None, u'threat_level_human': "80237EE4964FC9C409AAF55BF996A292_C5130A0BDC8C859A2757D77746C10868" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptr "6BADA8974A10C4BD62CC921D13E43B18_711ED44619924BA6DC33E69F97E7FF63" has type "data"- Location: [%LOCALAPPDATA%\\ow\\Microsoft\\Cryptr u'threat_level_human': u'informative', u'capec_id': None, u'attck_id': None, u'relevance': 3, u'threat_level': 0, u'type': 3, u'descr EXPLORER\\VERSIONMANAGER"; Key: "DOWNLOADVERSIONLIST"; Value: "")\n "IEXPLORE.EXE" (Path: "HKCU\\SOFTWARE\\MICROSOFT\\INTERNET EXPLOR age=0, no-cache, no-store\nPragma: no-cache\nDate: Fri, 03 Jun 2022 03:34:52 GMT\nConnection: keep-alive\nStrict-Transport-Security:
2022-12-18 00:07:17	HTTP Headers	No	Web Spider	2	0	2	0	None	{"content-length": "1078", "x-powered-by": "Express", "accept-ranges": "bytes", "keep-alive": "timeout=5", "last-modified": "Thu, 03
2022-12-18 00:21:30	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date'
2022-12-18 00:18:46	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.20:8443
2022-12-	HTTP	No	Censys	0	0	2	0	None	

18 00:21:58	Headers								{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Date"
2022-12-18 00:21:30	Open TCP Port	No	Censys	0	0	2	0	None	172.67.190.129:8080
2022-12-18 00:09:40	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	84010.ir
2022-12-18 00:21:13	Open TCP Port	No	Censys	0	0	2	0	None	188.114.97.0:2095
2022-12-18 00:04:11	SSL Certificate - Issued by	No	SSL Certificate Analyzer	0	0	2	0	None	C=US,O=Cloudflare\, Inc.,CN=Cloudflare Inc ECC CA-3
2022-12-18 00:24:58	Affiliate - IP Address	No	DNS Look-aside	1	0	3	0	None	90.116.149.189
2022-12-18 00:21:02	HTTP Headers	No	Censys	0	0	2	0	None	{"_encoding": {"Referrer_Policy": "DISPLAY_UTF8", "Expires": "DISPLAY_UTF8", "Vary": "DISPLAY_UTF8", "Server": "DISPLAY_UTF8", "Cf_Ra
2022-12-18 00:21:02	Open TCP Port	No	Censys	0	0	2	0	None	104.21.28.240:80
2022-12-18 00:06:40	Open TCP Port	No	Pulsedive	0	0	2	0	None	188.114.97.1:80
2022-12-18 00:09:52	Co-Hosted Site	No	HackerTarget	0	0	2	0	None	blog.kharkevich.org
2022-12-18 00:39:06	Affiliate - Email Address	No	E-Mail Address Extractor	0	0	3	0	None	abuse@ddns.com.au
2022-12-18 00:08:30	Open TCP Port	No	LeakIX	0	0	1	0	None	plague.fun:443
2022-12-18 00:02:39	IP Address	No	SpiderFoot UI	15	0	0	0	None	51.103.210.236
2022-12-18 00:09:11	Open TCP Port	No	LeakIX	0	0	2	0	None	172.67.190.129:443
2022-12-18 00:21:27	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:21:17	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-O
2022-12-18 00:18:15	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.97.5:80
2022-12-18 00:14:01	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.138:443
2022-12-18 00:02:47	SSL Certificate - Raw Data	No	CertSpotter	0	0	1	0	None	Certificate: Data: Version: 3 (0x2) Serial Number: 03:2c:cd:9b:50:65:02:e8:a9:66:93:11:97:33:8f:e3:ed:9b Signature Algorithm: sha256W SHA256 30:45:02:21:00:C3:25:CA:E0:91:C9:7B:9B:32:99:32: 0F:57:E2:A5:48:D4:29:C0:95:B6:AC:62:47:D9:B4:27: 82:7B:81:DD:35:02:20:04:E1:4
2022-12-18 00:13:04	Affiliate Description - Category	No	DuckDuckGo	0	0	3	0	None	Internet service providers of France
2022-12-18 00:14:01	Open TCP Port	No	Pulsedive	0	0	3	0	None	188.114.96.138:8080
2022-12-18 00:09:02	Open TCP Port	No	LeakIX	0	0	2	0	None	188.114.97.1:8080
2022-12-18 00:02:43	SSL Certificate Expiring	Yes	CertSpotter	0	0	1	0	None	2023-01-04 20:16:47
2022-12-18 00:19:01	Malicious IP Address	Yes	VirusTotal	0	1	2	0	None	VirusTotal [172.67.190.129] https://www.virustotal.com/en/ip-address/172.67.190.129/information/
2022-12-18 00:17:08	Co-Hosted Site	No	SSL Certificate Analyzer	0	0	2	0	None	amen.fr
2022-12-18 00:21:30	Software Used	Yes	Censys	0	0	2	0	None	CloudFlare CloudFlare Load Balancer
2022-12-18 00:21:54	Open TCP Port	No	Censys	0	0	2	0	None	104.21.7.179:2096