

CODEPATH*

CYB102

Group

Capstone

Bryan Zevallos
Didier Desmangles
Isael Melendez
Giancarlo Montes

Confidential

Copyright ©



Table of Content

- Sample Dataset
- Monitoring Sources
- Identified Assets
- Impact Analysis and Triage
- Threat Intelligence
- Recommended Remediation
- Case Management System
- Conclusion

Sample Dataset

We choose to work on

QAKBOT (QBOT) INFECTION WITH COBALT STRIKE (BEACON)

Dataset available on

<https://www.malware-traffic-analysis.net/2020/12/15/index.html>

Monitoring Sources

By: Didier Desmangles

1. Download all available materials.

1. PCAP
2. Various zip files, ioc, malware files, eml

1. Network log was available as two separated .pcap files.

1. We merge the 2 pcap with Wireshark to work on ONE pcap to facilitate the analysis.

1. First observation:

The pcap have been sanitized to avoid any accidental risk of infection.

Monitoring Sources

By: Didier Desmangles

1. Download all available materials.

1. PCAP
2. Various zip files, ioc, malware files, eml

1. Network log was available as two separated .pcap files.

1. We merge the 2 pcap with Wireshark to work on ONE pcap to facilitate the analysis.

1. First observation:

The pcap have been sanitized to avoid any accidental risk of infection.

Monitoring Sources

By: Didier Desmangles

Wireshark

1. **We use several filters to analyse the pcap. Knowing that the file has been sanitized, we looked for other signs of suspicious activity.**
1. **We started by “double-checking” with smtp, pop, imap**
1. **Investigation continue with following traffic stream TCP, HTTP, IMF, SMB**

Monitoring Sources

By: Didier Desmangles

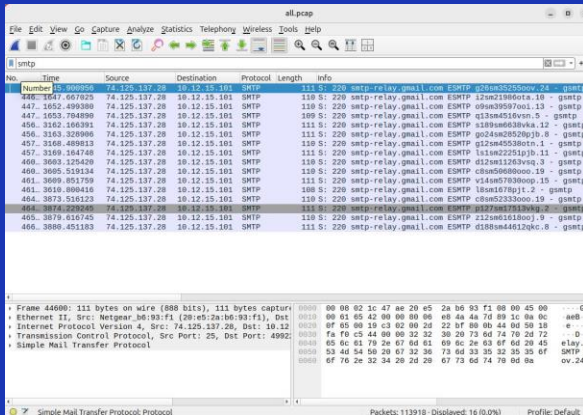
Tactics:

1. **Qakbot Cobalt Strike is used to still information**
1. **A client got infected by a rogue email with Document_1002660037_12152020.zip attached to it (QBot)**
1. **Document_1002660037_12152020.zip start by collecting informations.**
1. **It downloads Cobalt Strike payload (the Beacon) to establish persistent communication channel with CnC.**

Monitoring Sources

By: Didier Desmangles

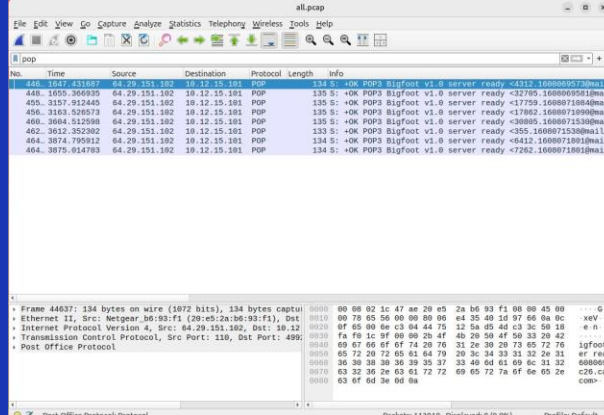
No mail entry point in pcap



Wireshark capture of SMTP traffic. The packet list shows an SMTP session between 74.125.137.28 and 10.12.15.101. The packet details pane shows the SMTP protocol structure, including the MAIL FROM, RCPT TO, and DATA fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
447	1652.499380	74.125.137.28	10.12.15.101	SMTP	111	220 smtp-relay.gmail.com ESMTP g2hae50250wv.04 - gsmtp
448	1652.501920	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP l2hae50250wv.10 - gsmtp
449	1652.503980	74.125.137.28	10.12.15.101	SMTP	100	S: 220 smtp-relay.gmail.com ESMTP p9hae50250wv.11 - gsmtp
450	1652.506040	74.125.137.28	10.12.15.101	SMTP	109	S: 220 smtp-relay.gmail.com ESMTP g3hae50250wv.12 - gsmtp
451	1652.508100	74.125.137.28	10.12.15.101	SMTP	111	S: 220 smtp-relay.gmail.com ESMTP l3hae50250wv.13 - gsmtp
452	1652.510160	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP p0hae50250wv.14 - gsmtp
453	1652.512220	74.125.137.28	10.12.15.101	SMTP	111	S: 220 smtp-relay.gmail.com ESMTP g4hae50250wv.15 - gsmtp
454	1652.514280	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP l4hae50250wv.16 - gsmtp
455	1652.516340	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP p1hae50250wv.17 - gsmtp
456	1652.518400	74.125.137.28	10.12.15.101	SMTP	111	S: 220 smtp-relay.gmail.com ESMTP g5hae50250wv.18 - gsmtp
457	1652.520460	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP l5hae50250wv.19 - gsmtp
458	1652.522520	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP p2hae50250wv.20 - gsmtp
459	1652.524580	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP g6hae50250wv.21 - gsmtp
460	1652.526640	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP l6hae50250wv.22 - gsmtp
461	1652.528700	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP p3hae50250wv.23 - gsmtp
462	1652.530760	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP g7hae50250wv.24 - gsmtp
463	1652.532820	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP l7hae50250wv.25 - gsmtp
464	1652.534880	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP p4hae50250wv.26 - gsmtp
465	1652.536940	74.125.137.28	10.12.15.101	SMTP	110	S: 220 smtp-relay.gmail.com ESMTP g8hae50250wv.27 - gsmtp
466	1652.539000	74.125.137.28	10.12.15.101	SMTP	111	S: 220 smtp-relay.gmail.com ESMTP l8hae50250wv.28 - gsmtp

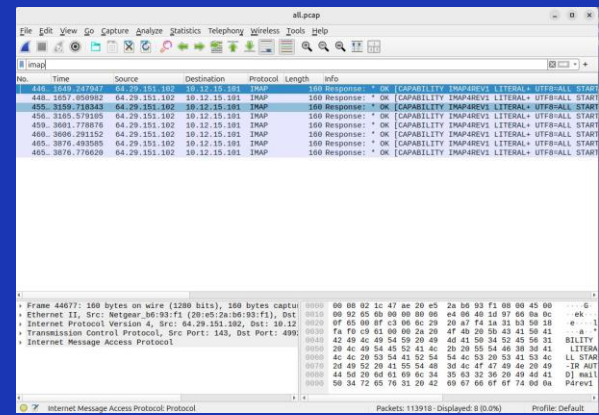
SMTP



Wireshark capture of POP traffic. The packet list shows a POP session between 64.29.151.102 and 10.12.15.101. The packet details pane shows the POP protocol structure, including the USER, PASS, and RETR commands. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
448	1647.411000	64.29.151.102	10.12.15.101	POP	134	S: OK POP3 BigFoot v1.0 server ready <3762.1600871803@mail13>
449	1655.366935	64.29.151.102	10.12.15.101	POP	135	S: OK POP3 BigFoot v1.0 server ready <3762.1600871804@mail13>
450	3157.912445	64.29.151.102	10.12.15.101	POP	135	S: OK POP3 BigFoot v1.0 server ready <3762.1600871805@mail13>
451	3163.320573	64.29.151.102	10.12.15.101	POP	135	S: OK POP3 BigFoot v1.0 server ready <3762.1600871806@mail13>
452	3604.512598	64.29.151.102	10.12.15.101	POP	135	S: OK POP3 BigFoot v1.0 server ready <3762.1600871807@mail13>
453	3621.352582	64.29.151.102	10.12.15.101	POP	135	S: OK POP3 BigFoot v1.0 server ready <3762.1600871808@mail13>
454	3874.795912	64.29.151.102	10.12.15.101	POP	134	S: OK POP3 BigFoot v1.0 server ready <3762.1600871809@mail13>
455	3875.814783	64.29.151.102	10.12.15.101	POP	134	S: OK POP3 BigFoot v1.0 server ready <3762.1600871810@mail13>

POP



Wireshark capture of IMAP traffic. The packet list shows an IMAP session between 64.29.151.102 and 10.12.15.101. The packet details pane shows the IMAP protocol structure, including the CAPABILITY, NOOP, and SELECT commands. The packet bytes pane shows the raw data in hexadecimal and ASCII.

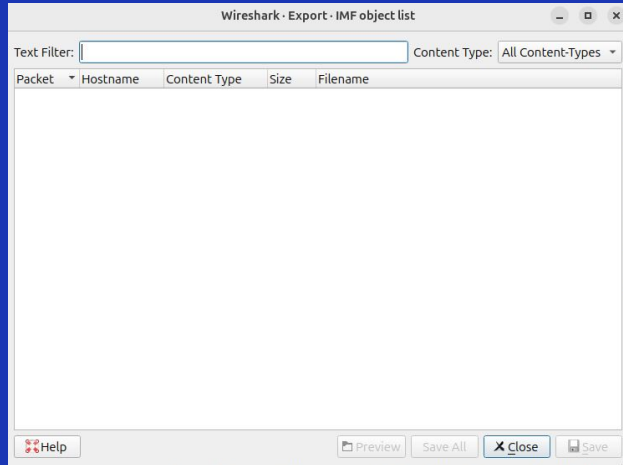
No.	Time	Source	Destination	Protocol	Length	Info
448	1649.817947	64.29.151.102	10.12.15.101	IMAP	160	Response: * OK [CAPABILITY IMAP4REV1 LITERAL+ UTF8=ALL START
449	1657.809982	64.29.151.102	10.12.15.101	IMAP	160	Response: * OK [CAPABILITY IMAP4REV1 LITERAL+ UTF8=ALL START
450	3159.718343	64.29.151.102	10.12.15.101	IMAP	160	Response: * OK [CAPABILITY IMAP4REV1 LITERAL+ UTF8=ALL START
451	3165.579105	64.29.151.102	10.12.15.101	IMAP	160	Response: * OK [CAPABILITY IMAP4REV1 LITERAL+ UTF8=ALL START
452	3601.778816	64.29.151.102	10.12.15.101	IMAP	160	Response: * OK [CAPABILITY IMAP4REV1 LITERAL+ UTF8=ALL START
453	3606.291152	64.29.151.102	10.12.15.101	IMAP	160	Response: * OK [CAPABILITY IMAP4REV1 LITERAL+ UTF8=ALL START
454	3876.893205	64.29.151.102	10.12.15.101	IMAP	160	Response: * OK [CAPABILITY IMAP4REV1 LITERAL+ UTF8=ALL START
455	3876.776620	64.29.151.102	10.12.15.101	IMAP	160	Response: * OK [CAPABILITY IMAP4REV1 LITERAL+ UTF8=ALL START

imap

Monitoring Sources

By: Didier Desmangles

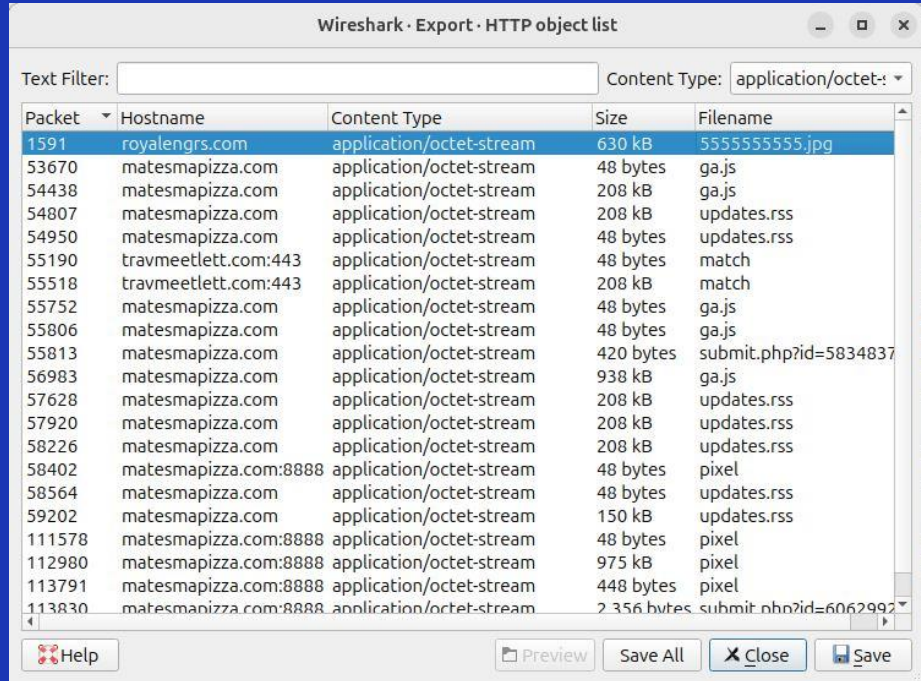
**Nothing to export in
eml**



Monitoring Sources

By: Didier Desmangles

However we can identify HTTP traffic:



Wireshark · Export · HTTP object list

Text Filter: Content Type: application/octet-stream

Packet	Hostname	Content Type	Size	Filename
1591	royallengrs.com	application/octet-stream	630 kB	555555555.jpg
53670	matesmapizza.com	application/octet-stream	48 bytes	ga.js
54438	matesmapizza.com	application/octet-stream	208 kB	ga.js
54807	matesmapizza.com	application/octet-stream	208 kB	updates.rss
54950	matesmapizza.com	application/octet-stream	48 bytes	updates.rss
55190	travmeetlett.com:443	application/octet-stream	48 bytes	match
55518	travmeetlett.com:443	application/octet-stream	208 kB	match
55752	matesmapizza.com	application/octet-stream	48 bytes	ga.js
55806	matesmapizza.com	application/octet-stream	48 bytes	ga.js
55813	matesmapizza.com	application/octet-stream	420 bytes	submit.php?id=5834837
56983	matesmapizza.com	application/octet-stream	938 kB	ga.js
57628	matesmapizza.com	application/octet-stream	208 kB	updates.rss
57920	matesmapizza.com	application/octet-stream	208 kB	updates.rss
58226	matesmapizza.com	application/octet-stream	208 kB	updates.rss
58402	matesmapizza.com:8888	application/octet-stream	48 bytes	pixel
58564	matesmapizza.com	application/octet-stream	48 bytes	updates.rss
59202	matesmapizza.com	application/octet-stream	150 kB	updates.rss
111578	matesmapizza.com:8888	application/octet-stream	48 bytes	pixel
112980	matesmapizza.com:8888	application/octet-stream	975 kB	pixel
113791	matesmapizza.com:8888	application/octet-stream	448 bytes	pixel
113830	matesmapizza.com:8888	application/octet-stream	2 356 bytes	submit.php?id=6062992

Help Preview Save All Close Save

Monitoring Sources

By: Didier Desmangles

However we can identify HTTP traffic:

royalengrs.com	IP\162.241.219.74
5555555555.jpg	SHA256\a16e6a01dddea661581791c10cc4b3914c787bdbcf008eb873d00a46d42c8fb3
matesmapizza.com	* malicious website, downloading malware materials. Files might obfuscated
travmeetlett.com	* malicious website, downloading malware materials Files might obfuscated

Monitoring Sources

By: Didier Desmangles

SMB Activities

Wireshark - Export - SMB object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
404	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
454	\\OrangeNight-DC.orangenight.com\sysvol	FILE (1098/1098) R [100.00%]	1,098 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
481	\\OrangeNight-DC.orangenight.com\sysvol	FILE (2798/2798) R [100.00%]	2,798 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Registry.pol
510	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
813	\\ORANGENIGHT.COM\IPC\$	FILE (160/160) R&W [100.00%]	160 bytes	\\samr
2453	\\ORANGENIGHT.COM\IPC\$	FILE (160/160) R&W [100.00%]	160 bytes	\\samr
3408	\\ORANGENIGHT-DC\IPC\$	FILE (160/160) R&W [100.00%]	160 bytes	\\lsarpc
46921	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
46973	\\OrangeNight-DC.orangenight.com\sysvol	FILE (1098/1098) R [100.00%]	1,098 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
47002	\\OrangeNight-DC.orangenight.com\sysvol	FILE (2798/2798) R [100.00%]	2,798 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Registry.pol
47033	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
48668	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
48720	\\OrangeNight-DC.orangenight.com\sysvol	FILE (1098/1098) R [100.00%]	1,098 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
48749	\\OrangeNight-DC.orangenight.com\sysvol	FILE (2798/2798) R [100.00%]	2,798 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Registry.pol
48780	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
49430	\\10.12.15.15\TREEID_UNKNOWN	OTHER (Not Implemented) (0/0) W [0.00%]	0 bytes	File_id_00000618-0019-0000-0100-000019000000
65506	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
65558	\\OrangeNight-DC.orangenight.com\sysvol	FILE (1098/1098) R [100.00%]	1,098 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
65587	\\OrangeNight-DC.orangenight.com\sysvol	FILE (2798/2798) R [100.00%]	2,798 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Registry.pol
65618	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22 bytes	\\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini

Help Preview Save All Close Save

10.12.15.101 is the infected machine.

It's exfiltrating data from the domain controller (10.12.15.15) via SMB protocol (credential theft)

Monitoring Sources

By: Didier Desmangles

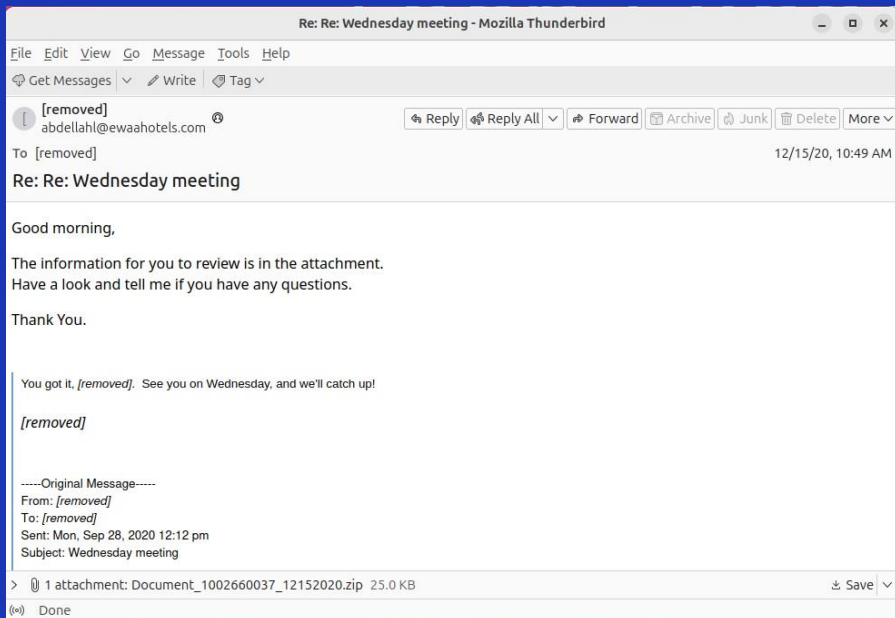
IP Addresses found by following several TCP Stream



Monitoring Sources

By: Didier Desmangles

Inspecting the malicious email



Confidential

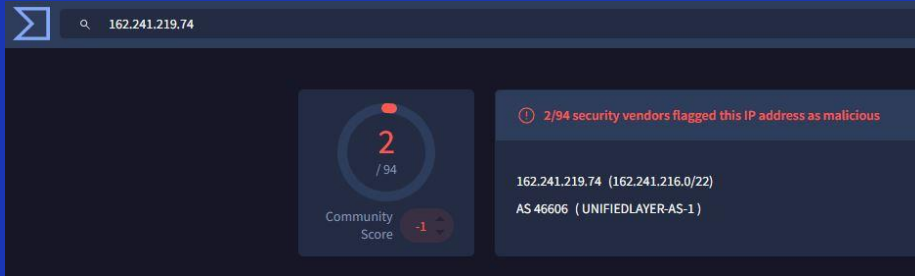
Copyright ©

Monitoring Sources

By: Didier Desmangles

royalengrs.com

IP\162.241.219.74



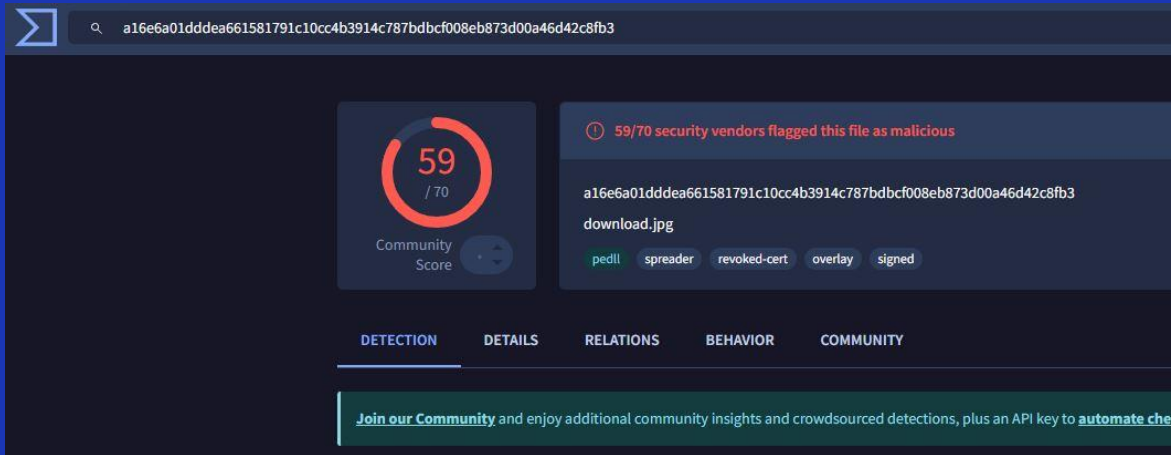
IP is associated with malicious activities

Monitoring Sources

By: Didier Desmangles

555555555.jpg

SHA256\a16e6a01dddea661581791c10cc4b3914c787bdbcf008eb873d00a46d42c8fb3



trojan.qbot/fapr

PE32 executable (DLL) (GUI) Intel
80386, for MS Windows

Monitoring Sources

By: Didier Desmangles

IP Addresses found by following several TCP Stream

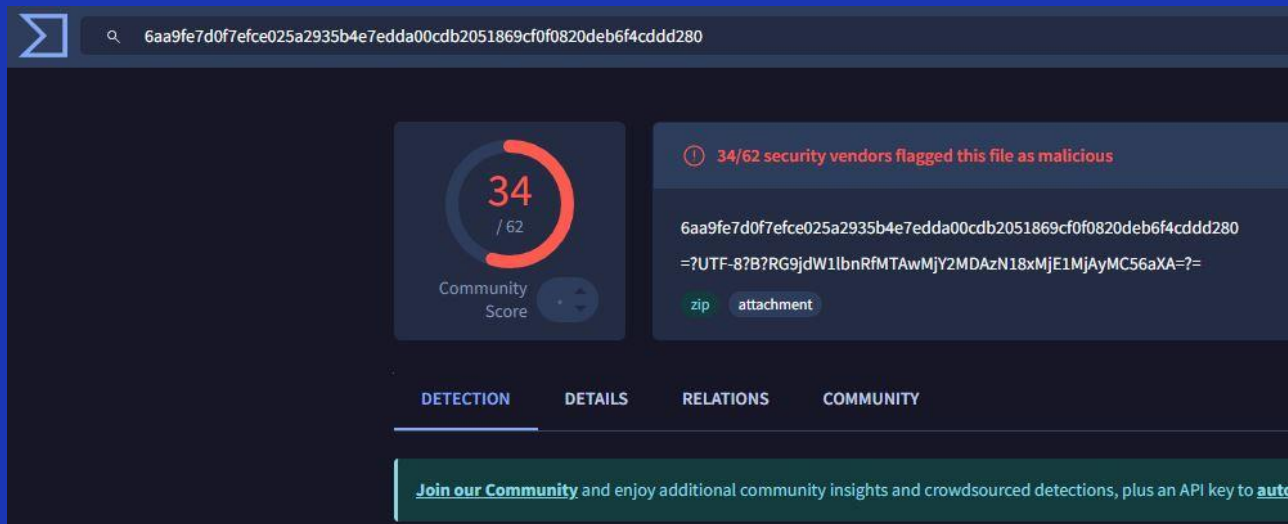
78.101.199.138
185.125.206.173
172.241.27.244
162.241.219.74
204.79.197.200
74.125.137.28
52.183.220.149
64.29.151.102
96.6.230.82



Monitoring Sources

By: Didier Desmangles

The mail comes with a malicious zip file: Document_1002660037_12152020.zip
SHA256: 6aa9fe7d0f7efce025a2935b4e7edda00cdb2051869cf0f0820deb6f4cddd280



Identified Assets

By: Didier Desmangles

Impact Analysis and Triage

By: Giancarlo Montes

Threat Intelligence

By: Isael Melendez

Objective: Understanding Threat Actor's Tactics, Techniques and Procedures (TTPs) and important IOCs.

Search sources and Tools: Wireshark, VirusTotal, AbuseIPDB.

Topics:

Overview, Impact, Incident Detection, IOCs, Threat Landscape, Mitre Technologies.

Confidential

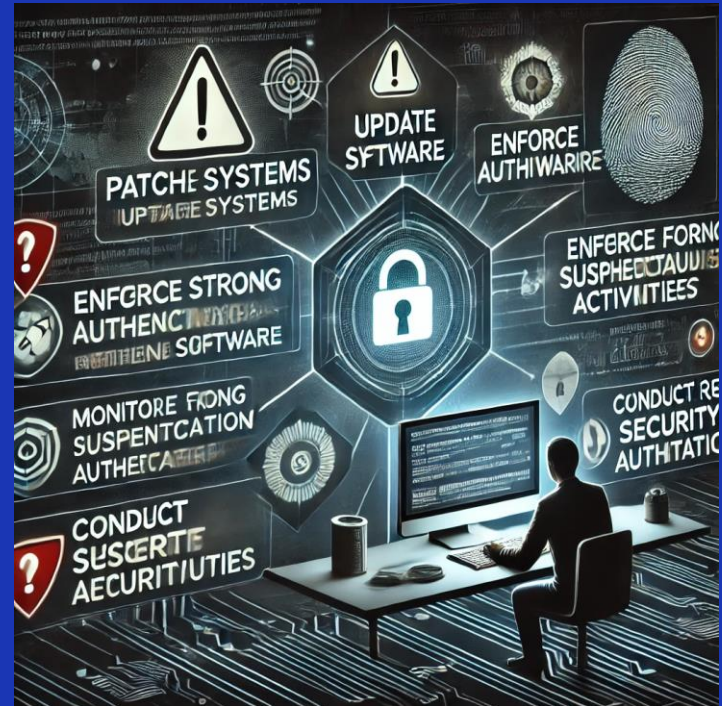
Copyright ©



Recommended Remediation

By: Bryan Zevallos

Recommended remediation involves actions like blocking attacking IPs, making the network defense stronger, and updating firewalls. To effectively remediate an issue involving a malicious hash, it's crucial to first verify the hash against trusted threat intelligence sources like VirusTotal. Once confirmed, isolate any affected systems from the network to prevent further damage, and remove or quarantine the malicious file. A comprehensive review of system logs and forensic analysis should be conducted to assess the full impact and ensure no additional systems are compromised. Finally, update security tools, patch vulnerabilities, and continuously monitor for signs of re-infection to maintain a secure environment.



Case Management System

By: Bryan Zevallos

In a Case Management System (CMS) utilizing Server Message Block (SMB) for file sharing, an SMB attack involving a malicious hash can compromise the integrity of sensitive client data. Upon detecting such an attack, it's crucial to verify the hash through trusted threat intelligence platforms and immediately isolate any affected systems to prevent further damage. The malicious file should be removed or quarantined, and a comprehensive review of system logs should be conducted to determine the entry point and impact of the attack. Patching vulnerabilities, updating security systems, and monitoring the network for any unusual behavior will help secure the CMS and prevent future SMB attacks. We used Catalyst for this project.

Confidential

Copyright ©



Conclusion