CODEPATH

CYB102 Group Capstone

Bryan Zevallos
Didier Desmangles
Isael Melendez
Giancarlo Montes

Table of Content

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)

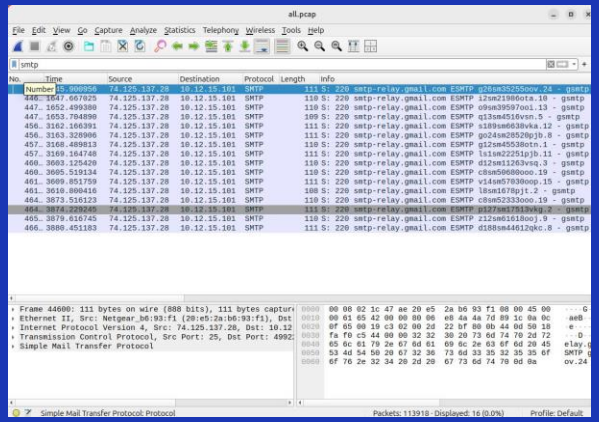
1. Document_1002660037_12152020.zip start by collecting informations.

1. It downloads Cobalt Strike payload (the Beacon) to establish persistent communication channel with CnC.

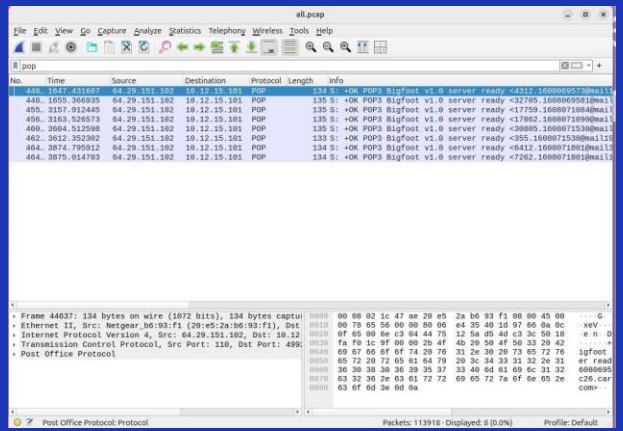
Monitoring Sources

By: Didier Desmangles

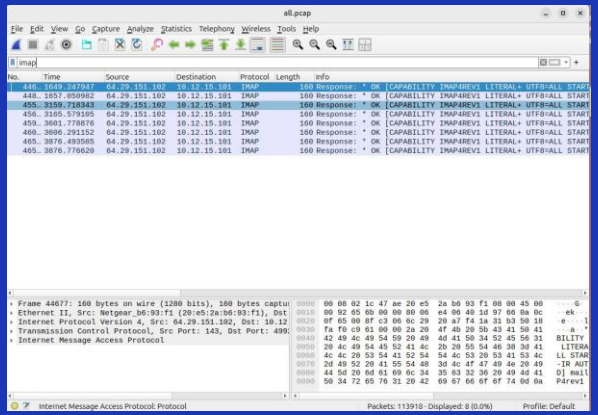
No mail entry point in pcap



SMTP



POP

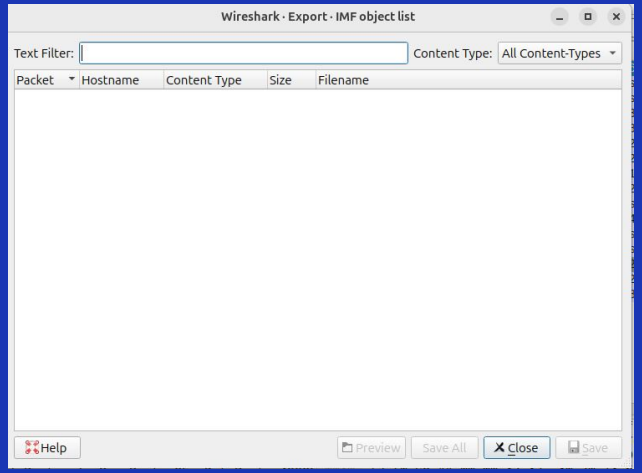


imap

Monitoring Sources

By: Didier Desmangles

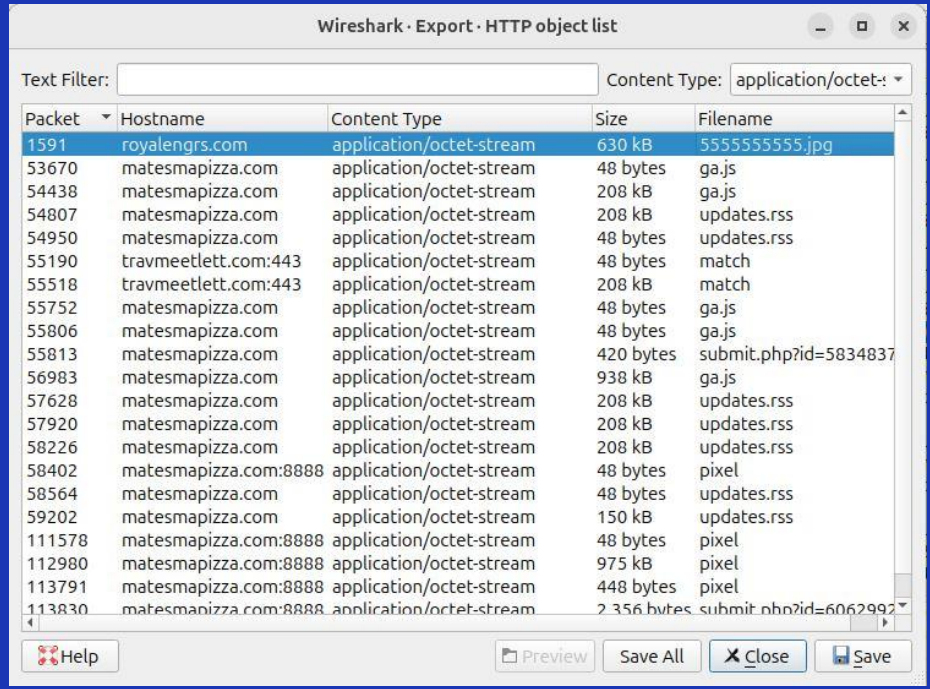
Nothing to export in eml



Monitoring Sources

By: Didier Desmangles

However we can identify HTTP traffic:



Monitoring Sources

By: Didier Desmangles

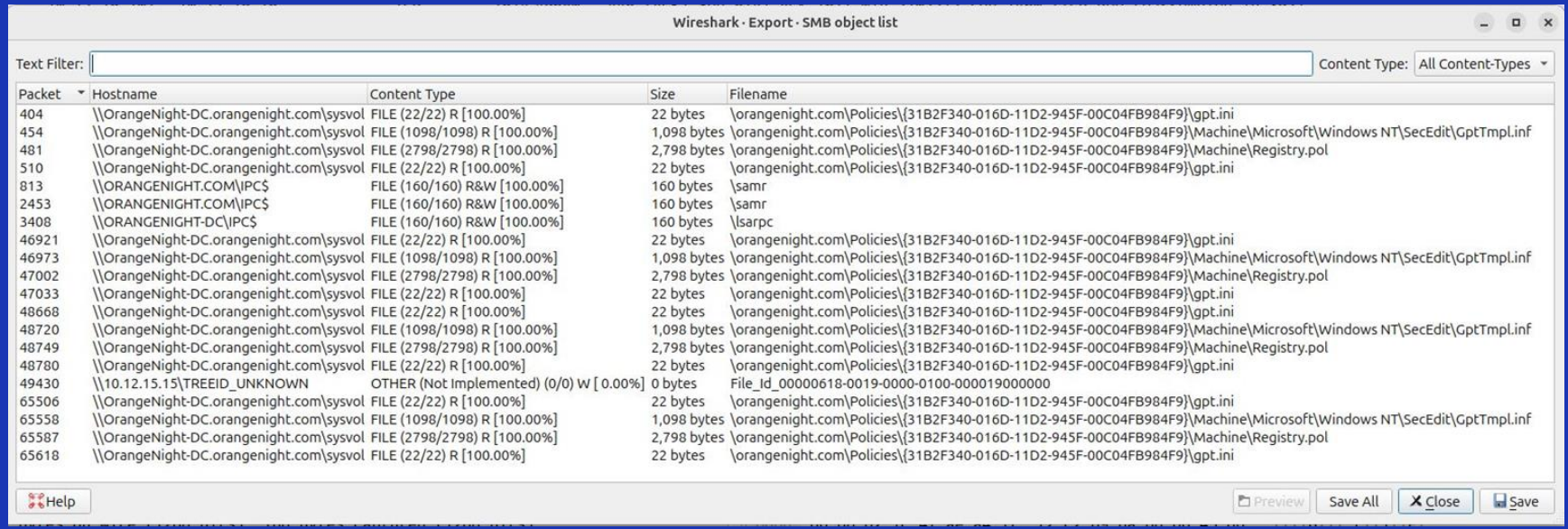
However we can identify HTTP traffic:

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

Monitoring Sources

By: Didier Desmangles

SMB Activities



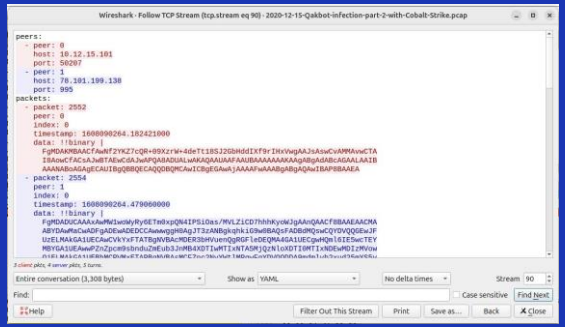
Packet	Hostname	Content Type	Size	Filename
404	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22 bytes	\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
454	\\OrangeNight-DC.orangenight.com\sysvol	FILE (1098/1098) R [100.00%]	1,098 bytes	\orangenight.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows 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

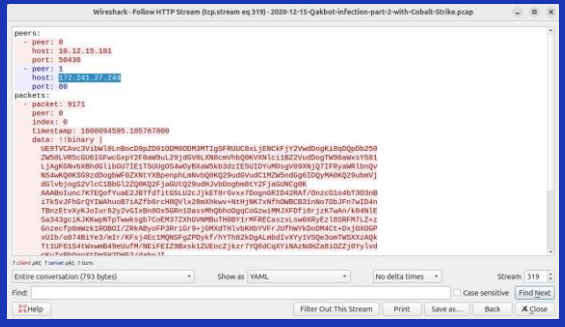
10.12.15.101 is the infected machine.
It's exfiltrating data from the domain controller (10.12.15.15) via SMB protocol (credential theft)

Monitoring Sources

By: Didier Desmangles

IP Addresses found by following several TCP Stream

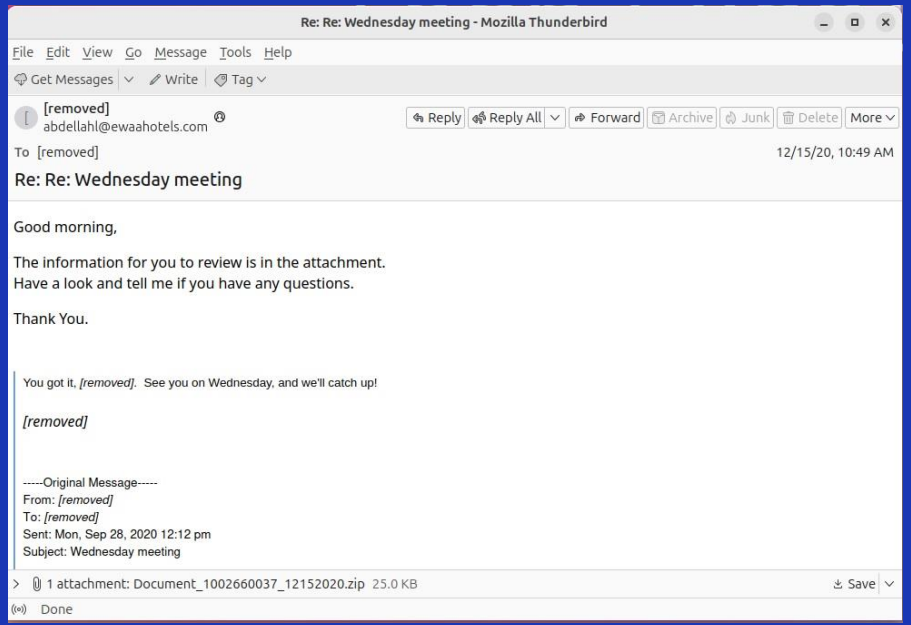




Monitoring Sources

By: Didier Desmangles

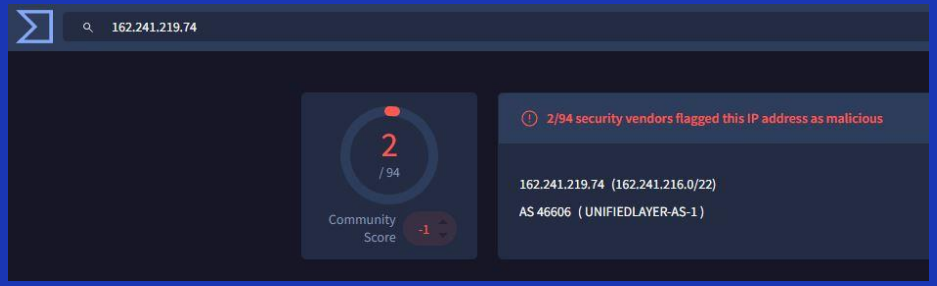
Inspecting the malicious email



Monitoring Sources

By: Didier Desmangles

royalengrs.com	IP\162.241.219.74

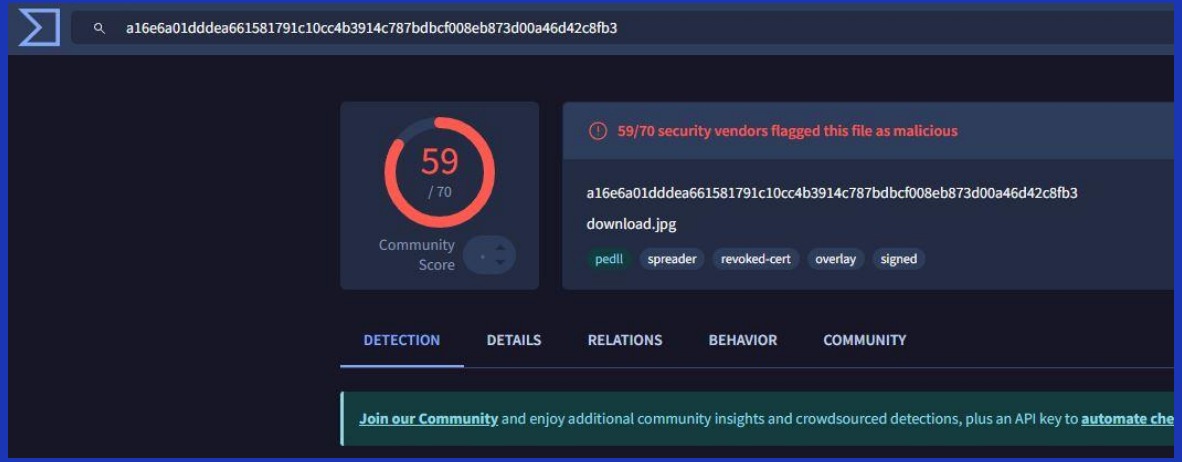


IP is associated with malicious activities

Monitoring Sources

By: Didier Desmangles

5555555555.jpg	SHA256\a16e6a01dddea661581791c10cc4b3914c787bdbcf008eb873d00a46d42c8fb3



trojan.qbot/fapr
PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Monitoring Sources

By: Didier Desmangles

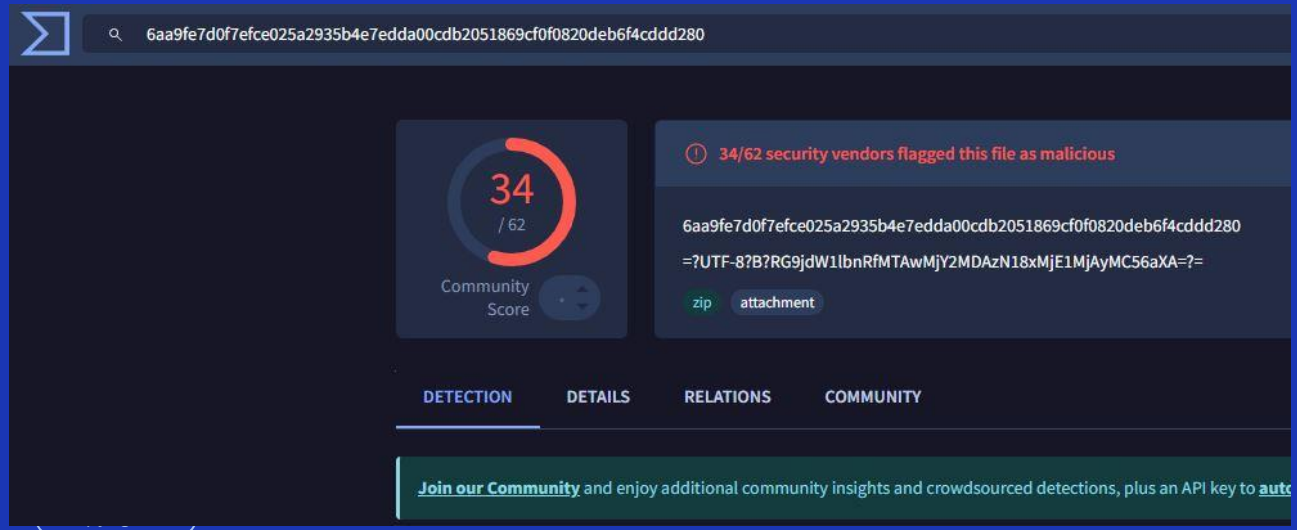
IP Addresses found by following several TCP Stream

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

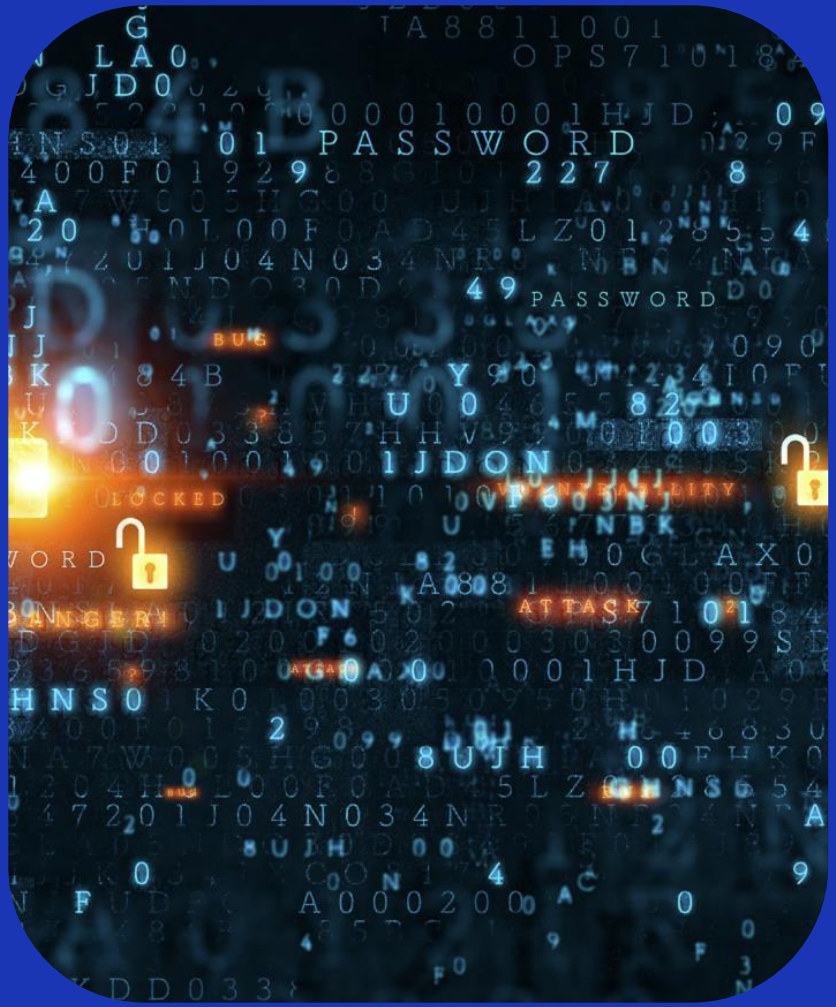
Threat Intelligence

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.



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.

Conclusion