

CODEPATH*

CYB102

Group

Capstone

Bryan Zevallos
Didier Desmangles
Isael Melendez
Giancarlo Montes



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

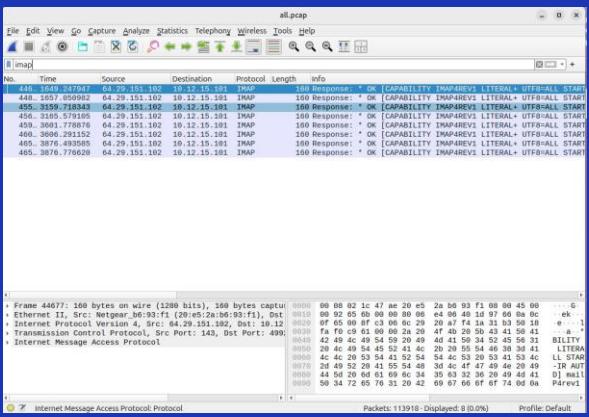
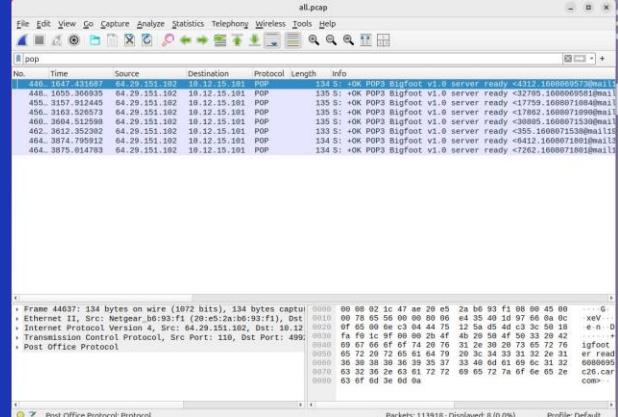
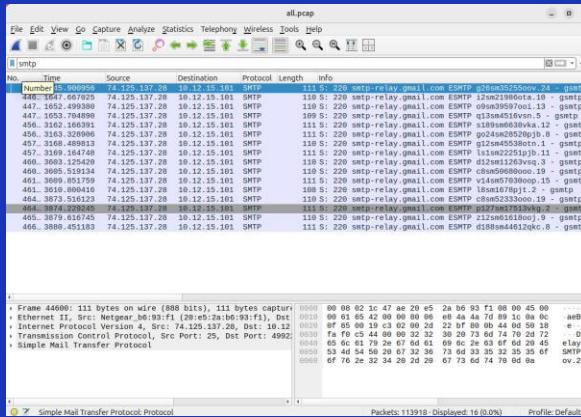
Tactics:

1. **Qakbot Cobalt Strike is used to steal information**
1. **A client got infected by a rogue email with Document_1002660037_12152020.zip attached to it (QBot)**
1. **Document_1002660037_12152020.zip starts 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



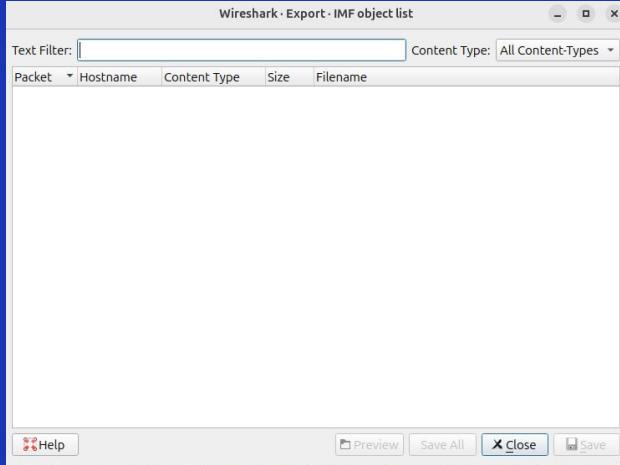
SMTP

POP

imap

Monitoring Sources

By: Didier Desmangles



**Nothing to export in
eml**

Monitoring Sources

By: Didier Desmangles

However we can identify HTTP traffic:

Wireshark - Export - HTTP object list				
Packet	Hostname	Content Type	Size	Filename
1591	royalenrgs.com	application/octet-stream	630 kB	5555555555.jpg
53670	matesmapizza.com	application/octet-stream	48 bytes	gajs
54438	matesmapizza.com	application/octet-stream	208 kB	gajs
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	gajs
55806	matesmapizza.com	application/octet-stream	48 bytes	gajs
55813	matesmapizza.com	application/octet-stream	420 bytes	submit.php?id=5834837
56983	matesmapizza.com	application/octet-stream	938 kB	gajs
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	matesmanizza.com:8888	application/octet-stream	2.356 bytes	submit.php?id=6062992

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\PC\$	FILE (160/160) R&W [100.00%]	160 bytes	\samr
2453	\ORANGENIGHT.COM\PC\$	FILE (160/160) R&W [100.00%]	160 bytes	\samr
3408	\ORANGENIGHT-DC\PC\$	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\TREED_UNKNOWN	OTHER (Not Implemented) (0/0) W [0.00%]	0 bytes	File_Id_00000618-0019-0000-0100-000001900000
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

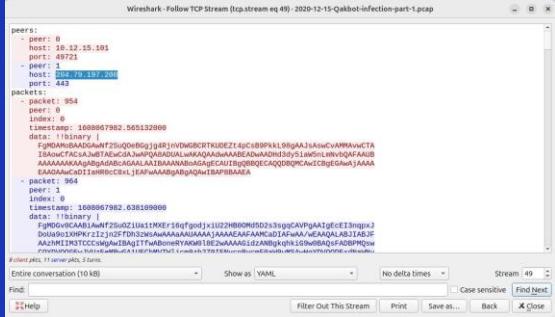
10.12.15.101 is the infected machine.

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

The screenshot shows an email client window titled "Re: Re: Wednesday meeting - Mozilla Thunderbird". The window has a standard menu bar with File, Edit, View, Go, Message, Tools, and Help. Below the menu is a toolbar with Get Messages, Write, Tag, Reply, Reply All, Forward, Archive, Junk, Delete, and More. The main pane displays an email message from "[removed]" (abdellahl@ewahotels.com) to "[removed]" (replied on 12/15/20, 10:49 AM). The subject is "Re: Re: Wednesday meeting". The message body contains:

Good morning,
The information for you to review is in the attachment.
Have a look and tell me if you have any questions.
Thank You.

In the message body, there is a quoted line: "You got it, [removed]. See you on Wednesday, and we'll catch up!" followed by "[removed]".

At the bottom, there is an "Original Message" section with the following details:

From: [removed]
To: [removed]
Sent: Mon, Sep 28, 2020 12:12 pm
Subject: Wednesday meeting

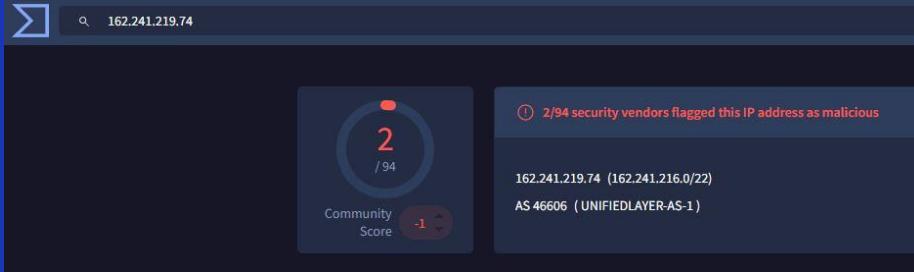
Below the message body, there is a status bar indicating "1 attachment: Document_1002660037_12152020.zip 25.0 KB" and "Save".

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

Σ a16e6a01dddea661581791c10cc4b3914c787bdbcf008eb873d00a46d42c8fb3

Community Score 59 / 70

59/70 security vendors flagged this file as malicious

a16e6a01dddea661581791c10cc4b3914c787bdbcf008eb873d00a46d42c8fb3
download.jpg

peddl spreader revoked-cert overlay signed

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate che

trojan.qbot/fapr

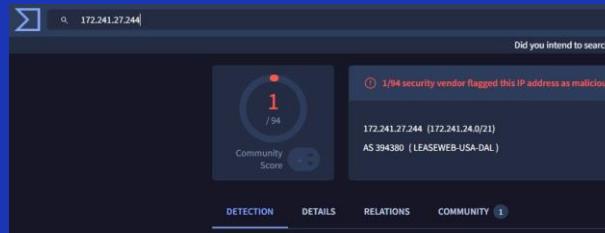
PE32 executable (DLL) (GUI) Intel
80386, for MS Windows

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**

Σ 6aa9fe7d0f7efce025a2935b4e7edda00cdb2051869cf0f0820deb6f4cddd280

34 / 62

Community Score

① 34/62 security vendors flagged this file as malicious

6aa9fe7d0f7efce025a2935b4e7edda00cdb2051869cf0f0820deb6f4cddd280
=?UTF-8?B?RG9jdW1lbmRfMTAwMjY2MDAzN18xMjE1MjAyMC56aXA=?=

zip attachment

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to auto

Confidential

Identified Assets

By: Didier Desmangles

Impact Analysis and Triage

By: Giancarlo Montes

Threat Intelligence

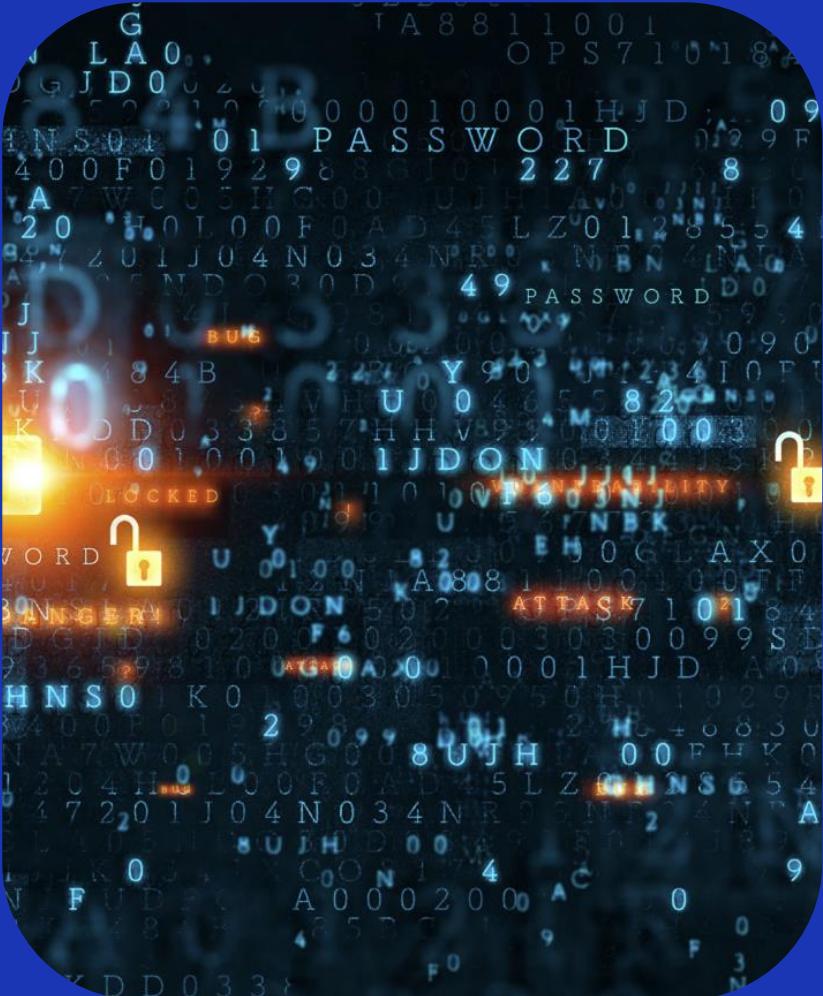
By: Israel Melendez

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

Search sources and Tools: Wireshark, VirusTotal, AbuseIPDB.

Topics:

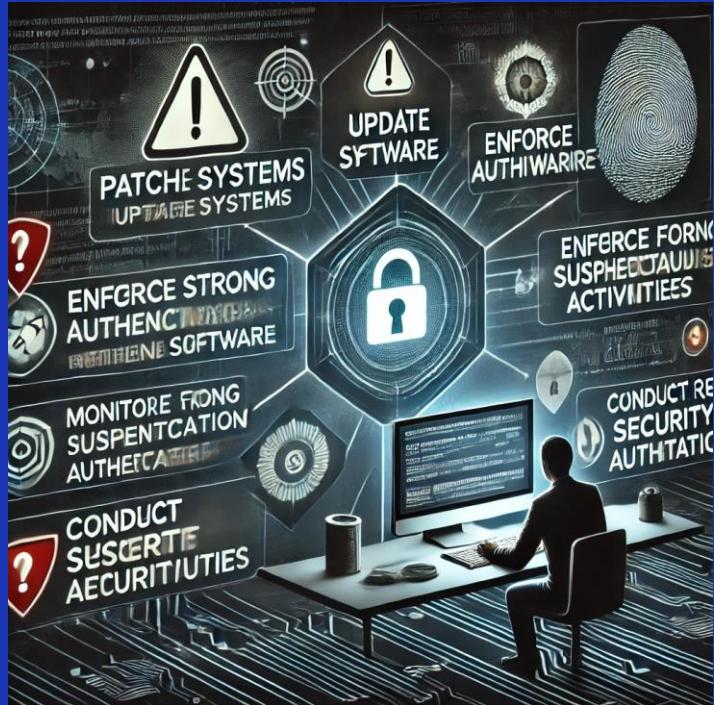
Overview, Impact, Incident Detection, IOCs, Threat Landscape, Mitre Technologies.



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