

CODEPATH\*

CYB102

# Group 17 Capstone

Bryan Zevallos  
Didier Desmangles  
Isael Melendez  
Giancarlo Montes

Confidential

Copyright ©



# Sample Dataset

## QAKBOT (QBOT) INFECTION WITH COBALT STRIKE (BEACON)

Dataset available on

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

<https://www.malware-traffic-analysis.net/2020/12/07/index.html>

# Table of Content

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

# Monitoring Sources

By: Didier Desmangles

**“Monitoring sources”** refer to the various tools, systems, and data feeds that provide information on potential security threats and anomalous activity within an organization’s environment. These sources continuously gather data, detect unusual patterns, and alert analysts to possible incidents so they can respond effectively.



# Monitoring Sources

1. Download all available materials.
  - 1.1. PCAP
  - 1.2. Various zip files, ioc, malware files, eml
2. Network log was available as two separated .pcap files.
  - 2.1. We merge the 2 pcap with Wireshark to work on ONE pcap to facilitate the analysis.

# Monitoring Sources

## 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.
2. We started by “double-checking” with smtp, pop, imap
3. Investigation continue with following traffic stream
  - a. DNS, TCP, HTTP, IMF, SMB
4. Risk: Some Infected files are present in the pcap.  
The malware in the eml file is active

# Monitoring Sources

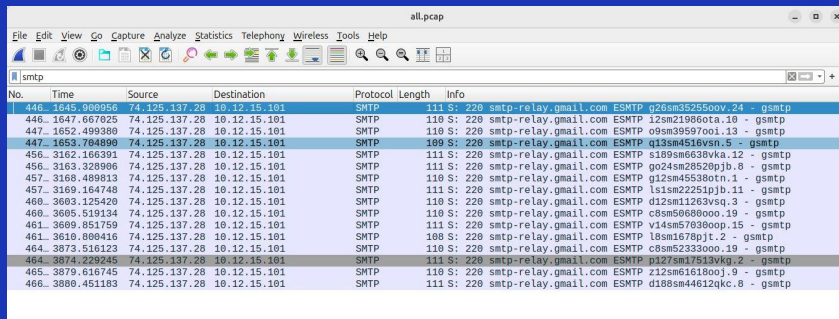
## Tactics:

**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).**
- 2. QBot is used as a loader to call Cobalt Strike**

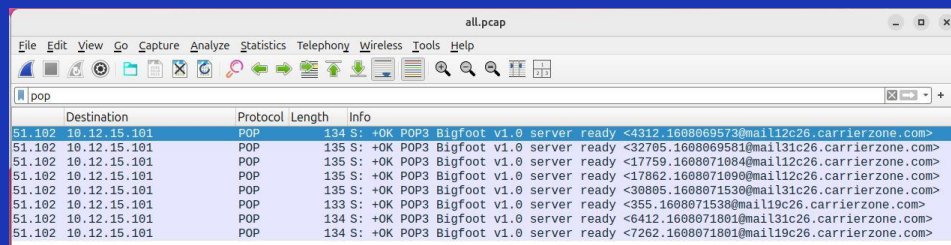
# Monitoring Sources

## Tactics: Traffic through POP



The image shows a Wireshark capture of SMTP traffic. The packet list on the left shows several SMTP packets. The selected packet is packet 446, which is an SMTP packet from 74.125.137.28 to 10.12.15.101. The packet details pane on the right shows the SMTP protocol structure, including the envelope and the message body.

No.	Time	Source	Destination	Protocol	Length	Info
446	1645.808956	74.125.137.28	10.12.15.101	SMTP	111 S: 220	smtp-relay.gmail.com ESMTp g26sm35255pov.24 - gsmt
446	1647.667825	74.125.137.28	10.12.15.101	SMTP	110 S: 220	smtp-relay.gmail.com ESMTp i2sm219860ta.10 - gsmt
447	1652.499380	74.125.137.28	10.12.15.101	SMTP	110 S: 220	smtp-relay.gmail.com ESMTp o9sm39597ooi.13 - gsmt
447	1653.784898	74.125.137.28	10.12.15.101	SMTP	109 S: 220	smtp-relay.gmail.com ESMTp q13sm4516vsn.5 - gsmt
456	3162.166391	74.125.137.28	10.12.15.101	SMTP	111 S: 220	smtp-relay.gmail.com ESMTp s189sm638vka.12 - gsmt
456	3163.328886	74.125.137.28	10.12.15.101	SMTP	111 S: 220	smtp-relay.gmail.com ESMTp go24sm28528pjb.8 - gsmt
457	3168.488113	74.125.137.28	10.12.15.101	SMTP	110 S: 220	smtp-relay.gmail.com ESMTp g12sm45538otn.1 - gsmt
457	3169.164748	74.125.137.28	10.12.15.101	SMTP	111 S: 220	smtp-relay.gmail.com ESMTp ls1sm22251pjb.11 - gsmt
460	3663.125420	74.125.137.28	10.12.15.101	SMTP	110 S: 220	smtp-relay.gmail.com ESMTp d12sm11263vsq.3 - gsmt
460	3665.519134	74.125.137.28	10.12.15.101	SMTP	110 S: 220	smtp-relay.gmail.com ESMTp c8sm506000oo.19 - gsmt
461	3669.851759	74.125.137.28	10.12.15.101	SMTP	111 S: 220	smtp-relay.gmail.com ESMTp v14sm57936oop.15 - gsmt
461	3610.808416	74.125.137.28	10.12.15.101	SMTP	108 S: 220	smtp-relay.gmail.com ESMTp l8sm1678pjt.2 - gsmt
464	3873.516123	74.125.137.28	10.12.15.101	SMTP	110 S: 220	smtp-relay.gmail.com ESMTp c8sm523330oo.19 - gsmt
464	3874.229245	74.125.137.28	10.12.15.101	SMTP	111 S: 220	smtp-relay.gmail.com ESMTp g127sm11513vkvk.2 - gsmt
465	3879.616745	74.125.137.28	10.12.15.101	SMTP	110 S: 220	smtp-relay.gmail.com ESMTp z12sm61618ooj.9 - gsmt
466	3880.451183	74.125.137.28	10.12.15.101	SMTP	111 S: 220	smtp-relay.gmail.com ESMTp d188sm44612qkc.8 - gsmt



The image shows a Wireshark capture of POP traffic. The packet list on the left shows several POP packets. The selected packet is packet 51, which is a POP packet from 10.12.15.101 to 134 S: +OK POP3 Bigfoot v1.0 server ready. The packet details pane on the right shows the POP protocol structure, including the command and the response.

No.	Time	Source	Destination	Protocol	Length	Info
51	102	10.12.15.101	134 S: +OK POP3 Bigfoot v1.0 server ready	POP	134 S: +OK POP3 Bigfoot v1.0 server ready	<4312.1608069573@mail12c26.carrierzone.com>
51	102	10.12.15.101	135 S: +OK POP3 Bigfoot v1.0 server ready	POP	135 S: +OK POP3 Bigfoot v1.0 server ready	<32705.1608069581@mail13c26.carrierzone.com>
51	102	10.12.15.101	135 S: +OK POP3 Bigfoot v1.0 server ready	POP	135 S: +OK POP3 Bigfoot v1.0 server ready	<17759.1608071884@mail12c26.carrierzone.com>
51	102	10.12.15.101	135 S: +OK POP3 Bigfoot v1.0 server ready	POP	135 S: +OK POP3 Bigfoot v1.0 server ready	<17862.1608071090@mail12c26.carrierzone.com>
51	102	10.12.15.101	135 S: +OK POP3 Bigfoot v1.0 server ready	POP	135 S: +OK POP3 Bigfoot v1.0 server ready	<30805.1608071530@mail13c26.carrierzone.com>
51	102	10.12.15.101	133 S: +OK POP3 Bigfoot v1.0 server ready	POP	133 S: +OK POP3 Bigfoot v1.0 server ready	<355.1608071538@mail19c26.carrierzone.com>
51	102	10.12.15.101	134 S: +OK POP3 Bigfoot v1.0 server ready	POP	134 S: +OK POP3 Bigfoot v1.0 server ready	<6412.1608071881@mail13c26.carrierzone.com>
51	102	10.12.15.101	134 S: +OK POP3 Bigfoot v1.0 server ready	POP	134 S: +OK POP3 Bigfoot v1.0 server ready	<7262.1608071881@mail19c26.carrierzone.com>



# Monitoring Sources

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

However we can identify HTTP traffic:

Wireshark · Export · HTTP object list

Text Filter:  Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
1591	royalengrs.com	application/octet-stream	630 kB	5555555555.jpg

Help Preview Save All Close Save

Wireshark · Export · HTTP object list

Text Filter:  Content Type: application/octet-stream

Packet	Hostname	Content Type	Size	Filename
7028	matesmapizza.com	application/octet-stream	48 bytes	ga.js
7796	matesmapizza.com	application/octet-stream	208 kB	ga.js
8165	matesmapizza.com	application/octet-stream	208 kB	updates.rss
8308	matesmapizza.com	application/octet-stream	48 bytes	updates.rss
8548	travmeetlett.com:443	application/octet-stream	48 bytes	match
8876	travmeetlett.com:443	application/octet-stream	208 kB	match
9110	matesmapizza.com	application/octet-stream	48 bytes	ga.js
9164	matesmapizza.com	application/octet-stream	48 bytes	ga.js
9171	matesmapizza.com	application/octet-stream	420 bytes	submit.php?id=583483712
10341	matesmapizza.com	application/octet-stream	938 kB	ga.js
10986	matesmapizza.com	application/octet-stream	208 kB	updates.rss
11278	matesmapizza.com	application/octet-stream	208 kB	updates.rss
11584	matesmapizza.com	application/octet-stream	208 kB	updates.rss
11760	matesmapizza.com:8888	application/octet-stream	48 bytes	pixel
11922	matesmapizza.com	application/octet-stream	48 bytes	updates.rss
12560	matesmapizza.com	application/octet-stream	150 kB	updates.rss
64936	matesmapizza.com:8888	application/octet-stream	48 bytes	pixel
66338	matesmapizza.com:8888	application/octet-stream	975 kB	pixel
67149	matesmapizza.com:8888	application/octet-stream	448 bytes	pixel
67188	matesmapizza.com:8888	application/octet-stream	2,356 bytes	submit.php?id=606299235

Help Preview Save All Close Save

# Identified Assets

By: Didier Desmangles

**Identifying assets** in the context of a cybersecurity attack involves pinpointing valuable resources within an organization that attackers could target. These assets can range from physical devices to sensitive data, software applications, and operational systems.



# Identified Assets

By: Didier Desmangles

Entry point: Spam campaign in an attempt to find a victim

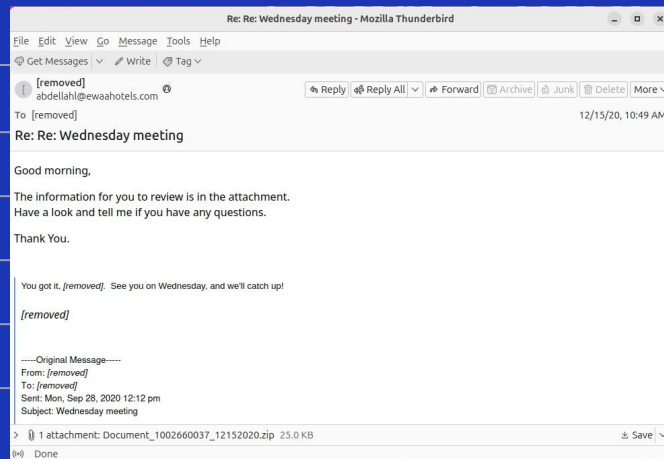
The infected attached files in the mail is a excel macro calling the QBot malware

The QBot is acting as a loader to call Cobalt Strike via 2 fakes websites

Cobalt Strike tries to steal informations from the Domain Controller (privilege escalation)

# Identified Assets

FILENAME	SHA256
Document_1002660037_12152020.zip	6aa9fe7d0f7efce025a2935b4e7edda00cdb2051869cf0f0820deb6f4cddd280
Document_1002660037_12152020.xls	77e6b40ed8b90e08a91f798a00504718ac47a899b4be69ac0bb6558fac40a7e5
555555555.jpg->JIOLAS.RRTTOOKK	a16e6a01dddea661581791c10cc4b3914c787bdbc008eb873d00a46d42c8fb3
bxgacpfhyxqx.dll	05f5bfa493161d093a53a6b953fad443c18e60f85497eca3727ec25733edf57b



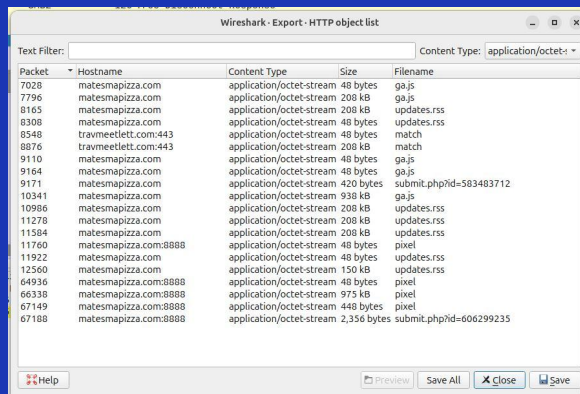
# Identified Assets

## Links (COBALT STRIKE)

matesmapizza.com

travmeetlett.com

royalengrs.com

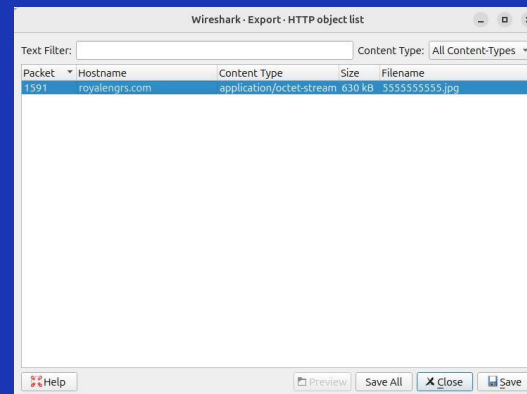


Wireshark - Export - HTTP object list

Text Filter: Content Type: application/octet-stream

Packet	Hostname	Content Type	Size	Filename
7028	matesmapizza.com	application/octet-stream	48 bytes	ga.js
7796	matesmapizza.com	application/octet-stream	208 kB	ga.js
8165	matesmapizza.com	application/octet-stream	208 kB	updates.rss
8308	matesmapizza.com	application/octet-stream	48 bytes	updates.rss
8548	travmeetlett.com:443	application/octet-stream	48 bytes	match
8876	travmeetlett.com:443	application/octet-stream	208 kB	match
9110	matesmapizza.com	application/octet-stream	48 bytes	ga.js
9164	matesmapizza.com	application/octet-stream	48 bytes	ga.js
9171	matesmapizza.com	application/octet-stream	420 bytes	submit.php?id=583483712
10341	matesmapizza.com	application/octet-stream	938 kB	ga.js
10986	matesmapizza.com	application/octet-stream	208 kB	updates.rss
11278	matesmapizza.com	application/octet-stream	208 kB	updates.rss
11584	matesmapizza.com	application/octet-stream	208 kB	updates.rss
11760	matesmapizza.com:8888	application/octet-stream	48 bytes	pixel
11922	matesmapizza.com	application/octet-stream	48 bytes	updates.rss
12560	matesmapizza.com	application/octet-stream	150 kB	updates.rss
64936	matesmapizza.com:8888	application/octet-stream	48 bytes	pixel
66338	matesmapizza.com:8888	application/octet-stream	975 kB	pixel
67149	matesmapizza.com:8888	application/octet-stream	448 bytes	pixel
67188	matesmapizza.com:8888	application/octet-stream	2,356 bytes	submit.php?id=606299235

Help Preview Save All Close Save



Wireshark - Export - HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
1591	royalengrs.com	application/octet-stream	630 kB	5555555555.jpg

Help Preview Save All Close Save

# Identified Assets

Wireshark · Export · SMB object list

Text Filter:  Content Type: All Content-Types

Packet	Hostname	Content Type	Size
279	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22
331	\\OrangeNight-DC.orangenight.com\sysvol	FILE (1098/1098) R [100.00%]	1,0
360	\\OrangeNight-DC.orangenight.com\sysvol	FILE (2798/2798) R [100.00%]	2,7
391	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22
2026	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22
2078	\\OrangeNight-DC.orangenight.com\sysvol	FILE (1098/1098) R [100.00%]	1,0
2107	\\OrangeNight-DC.orangenight.com\sysvol	FILE (2798/2798) R [100.00%]	2,7
2138	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22
2788	\\10.12.15.15\TREEID_UNKNOWN	OTHER (Not Implemented) (0/0) W [0.00%]	0 b
18864	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22
18916	\\OrangeNight-DC.orangenight.com\sysvol	FILE (1098/1098) R [100.00%]	1,0
18945	\\OrangeNight-DC.orangenight.com\sysvol	FILE (2798/2798) R [100.00%]	2,7
18976	\\OrangeNight-DC.orangenight.com\sysvol	FILE (22/22) R [100.00%]	22

Help Preview Save All Close Save

# Identified Assets

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

```
Wireshark - Follow TCP Stream (tcp.stream eq 49) - 2020-12-15-Qakbot-infection-part-1.pcap

peers:
- peer: 0
  host: 10.12.15.101
  port: 49721
- peer: 1
  host: 204.79.197.200
  port: 443

packets:
- packet: 954
  peer: 0
  index: 0
  timestamp: 1608067982.565132000
  data: !!binary |
    FgMDAMwBAADGwMf2suQ0eBgjg4RjnhVMGBCRtKUDZ14pCsB9PKkL8gAAJ3sSwCvAMMwWCTA
    I8AwCTACsA3wbTAEWcGdA3wAPQABADUAlwAKQAAdwAAABEADwAADH3dy518h5nLmVbQAFaUB
    AAAAAAAGABgABGABcAGAAALAI2BAANABoAGAGCAUTBgQB8QECAQDBQMCALICBgEGAwAJAAAA
    EAADAACwADIIaHR8cC8XLjEAFwAAABgABgAQAwI8AP8BAEA

- packet: 964
  peer: 1
  index: 0
  timestamp: 1608067982.638109000
  data: !!binary |
    FgMDGv9CAAB1AwMf2suOZ1Ua1tMXEr16qfgodjxLU22HB00M4S0Zs3sgqCAVPgAAIgeE13nqpxJ
    Doua9o1XHPKrZIZj2F0h3ZwSAAwAAABAAUAAAJAAAAEAAFAAMCAdIAFuAA/wEAAQALABJIABJF
    AAzNII3NCCCSWgAwIBAgITfwABoneRYAKw018E2wAAAAAGidzANBgkqhkiG9w0BAQsFAADBPQsw
    nYNYMUNGC5uLU1z56AMuCA1IECHMUTU15sm53h778TEKucnBueC6u5G0uM5AdwYVU00NEv8hAuUw

0 client pkts, 11 server pkts, 5 turns
Entire conversation (10 kB) Show as: YAML No delta times Stream 49
Find: Case sensitive Find Next
Filter Out This Stream Print Save as... Back X Close
```

```
Wireshark - Follow HTTP Stream (tcp.stream eq 319) - 2020-12-15-Qakbot-infection-part-2-with-Cobalt-Strike.pcap

peers:
- peer: 0
  host: 10.12.15.101
  port: 50430
- peer: 1
  host: 172.241.27.244
  port: 80

packets:
- packet: 9171
  peer: 0
  index: 0
  timestamp: 1608094595.105767000
  data: !!binary |
    UE9TVCAvc3V1bWl0LnBocD9pZD0100M600M3MTIgsFRUUC8xLjENCkfjY2VwdD9gKi8pQ0Db250
    ZW50LVRS5GUGIgfWc5xpT2F0aW9uL29jdGV0LXN0cnVhbgQKXXNlCl1BZ2VudDogT966awxsYS81
    LjAgKGNvbXBhdG1ibGUT1E1TSU0g0S4wYbXAw5K3dz1E5U1DYUM0sgV89XNjQ7IFRwRmRlbnQv
    NSAwQ8KSG9zZD9hbnF8ZXN1YXNpenphLmVbQ8KQ29udGVudC1KZWSnd5p6IDQyMA8KQ29ubmVj
    dGVlbj0gS2V1cC1BbG6122Q0KQ2FjagUTQ29udHJvdG9hbn8tY2FjagUNCgK
    AABoLunc7KTEQofYuaE2JBTf0t1t6SLU2c-jjKET8rGvxx7DognGRID42RAf/Onzc01o4bT303nB
    iTK5vJfH6rQYIWAhu087IAZfb6rch8QV1x28xhkwv+NthjNK7xlfh0MBC831nNo7DbJFn7wID4n
    TBnzEtVxYKJoIur82y2vGIxbn80u5GRn1DasshQhbdGgCoGzW1MMJXF0r16rjzK7wAn/k481E
    Sa34gciKJKwPmTptwksqg70cEK3TZxh6VNMbuTH8BY1rMFRCaszxLsw0XyEz18SRF7LZ+z
    Gnzcfp8mWzK1ROBOT/2RkAByoFP3Rr16r9+jGKdTHlvbKhYVFrJufmYKdo0M4Ct+DxjOXOGP
    xU1b/o874B1Ye3/mIr/FsJ4Ec1MQNSGF2P0y/kf/hYTh82kDgALmbd1vXYy1VSQe3onTWSXKzAQK
    Tt1U61S4tWomB49eUufN/NE1FEI29Bxsk1ZUEocZjKzr7YQ6dCqX1NAZNdHZA81OZZ30YyLvd
    zKx17uQdHnnXrTsw4S7N4E3/dshn.1T

1 client pkt, 1 server pkt, 1 turn
Entire conversation (793 bytes) Show as: YAML No delta times Stream 319
Find: Case sensitive Find Next
Filter Out This Stream Print Save as... Back X Close
```



# Impact Analysis and Triage

By: Giancarlo Montes



shutterstock.com • 2377513191

# Impact

Successful compromise by Cobalt Strike will result in the establishment of C2 channels between the target and the threat actor systems. The communication channel allows the threat actors to exfiltrate data from the target, compromise additional systems via lateral movement as well as the delivery of additional malware components such as ransomware.

## Examples of Cobalt Strike Being Used for Malicious Campaigns

- In **2018**, the **APT29** attacks on the U.S. energy sector (infiltrate networks, to execute payloads, and to steal sensitive information, such as login credentials and financial data.)
- In 2019, the **Lazarus hacking group** attacks on banks and financial institutions
- In 2020, the **Emissary Panda hacking group** attacks on government agencies and defense contractors.
- In 2020, **Trickbot** operators to deploy their Anchor backdoor and RYUK ransomware.

## The Dangers of Cobalt Strike

In the hands of a malicious attacker, Cobalt Strike can pose a significant risk to any organization. The platform's ability to mimic genuine network traffic makes it incredibly difficult to detect, allowing hackers to remain undetected within a network for extended periods. This stealthy nature, combined with its advanced post-exploitation capabilities, makes Cobalt Strike a formidable tool in the hands of cybercriminals.

# Triage:

**Detection:** Identify unusual network traffic, unauthorized access attempts, and alerts from intrusion detection systems (IDS).

**Scope:** Determine the extent of the infection, including which systems are compromised and the type of data accessed.

**High Severity:** Given the potential for data exfiltration, ransomware deployment, and persistent access, this incident is categorized as high severity.

**Immediate Action:** Prioritize containment and eradication to prevent further spread and data loss.

**Incident Response Team:** Network administrators to isolate affected systems, security analysts to analyze malware behavior, and IT personnel to restore services.

**Communication:** Notify stakeholders, including management and affected users, about the incident and potential impact.

**Password Changes:** Reset passwords and implement multi-factor authentication (MFA) to secure accounts.

**Malware Removal:** Use antivirus and anti-malware tools to remove Qakbot and Cobalt Strike Beacon from infected systems.

**Forensic Analysis:** Conduct a thorough investigation to understand the attack vector and identify vulnerabilities.

# Triage:

**Documentation:** Record the incident details, response actions, and lessons learned.

**Post-Incident Review:** Evaluate the incident response process and update policies and procedures to prevent future occurrences.

By following these steps, the organization can effectively manage the Qakbot infection and mitigate the impact of the Cobalt Strike Beacon.



# 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. MITRE ATT&CK

**Topics:**  
Overview, TTPs, Mitre ATT&CK, IOCs,.



# Overview

QBot, also known as Qakbot, QBot, QuackBot, and Pinksipbot, is a Banking Trojan that was first observed in 2007 and still being a dangerous and persistent threat to organizations. It spreads itself, evade detection and debugging, and install additional malware on compromised machines, such as **Cobalt Strike**

Cobalt Strike is a notorious post-exploitation tool that is used by threat actors to gain access to target systems and for the purposes of maintaining persistence. It's main used is to assess the security of networks systems and to identify and exploit potential vulnerabilities and weaknesses.

## Features and Capabilities:

- **Reconnaissance** (Discover client side software and versions)
- **Attack Packages** (Social Engineering, website clones)
- **Collaboration** (Share info with attackers groups in real time)
- **Post Exploitation**(Uses beacons, deploy PowerShell scripts, log keystrokes, screenshots, execute payloads)
- **Covert Communication** (Load C2 profiles, egress Network using HTTP,HTTPS,DNS,SMB protocols)
- **Browser Pivoting** (Used to get MFA)

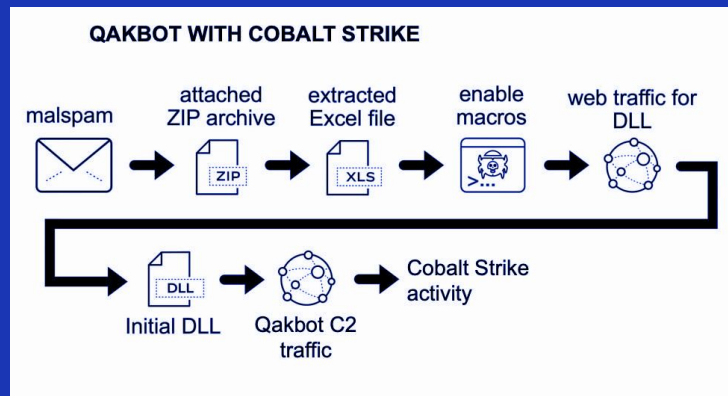


# TTPs

Malicious actors distribute QBot as attachments, typically Microsoft Office Excel documents, to phishing emails. The Office Excel application prompts the user that has opened the document that distributes QBot to enable Office macro execution. When the Office macro executes, the macro first downloads the QBot malware from an attacker-controlled endpoint and then executes the malware.

## Typical QBot malicious activity observed:

- Collecting information about the compromised host
- Stealing credentials (from browser data and cookies)
- Targeting web banking links
- Password brute-forcing
- Registry manipulation and creating scheduled tasks (for persistence)





# MITRE ATT&CK

## Execution

[T1059 - Command and Scripting Interpreter 4](#)

[T1059.001 - Command and Scripting Interpreter: PowerShell 5](#)

## Persistence

[T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder 6](#)

## Privilege Escalation

[T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder 7](#)

## Defence Evasion

[T1112 - Modify Registry 8](#)

## Credential Access

[T1539 - Steal Web Session Cookie 9](#)

## Discovery

[T1012 - Query Registry 10](#)

[T1082 - System Information Discovery 11](#)

## Command and Control

[T1071 - Application Layer Protocol 12](#)

[T1071.001 - Application Layer Protocol: Web Protocols](#)

### Command and Scripting Interpreter

Sub-techniques (11)

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

There are also cross-platform interpreters such as Python, as well as those commonly associated with client applications such as JavaScript and Visual Basic.

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in Initial Access payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various Remote Services in order to achieve remote Execution.<sup>[1][2][3]</sup>

ID: T1059

Sub-techniques: T1059.001, T1059.002, T1059.003, T1059.004, T1059.005, T1059.006, T1059.007, T1059.008, T1059.009, T1059.010, T1059.011

① **Tactic:** Execution

① **Platforms:** IaaS, Identity Provider, Linux, Network, Office Suite, Windows, macOS

① **Supports Remote:** Yes

Version: 2.5

Created: 31 May 2017

Last Modified: 14 October 2024

[Version Permalink](#)

Confidential

Copyright ©

By: Isael Melendez



# IOCs

## MALWARE FROM AN INFECTED WINDOWS HOST:

- **SHA256 hash:** dd592afe3cd134d0fcb0201a48c8af1f7371d99a6fb5d5f0a7568253d459f3f7
- **File size:** 630,200 bytes
- **File location:** <http://royalengrs.com/crizzszfsx/5555555555.jpg>
- **File location:** C:\IntelCompany\JIOLAS.RRTTOOKK
- **File description:** DLL for Qakbot retrieved by Excel macro
- **Run method:** rundll32.exe C:\IntelCompany\JIOLAS.RRTTOOKK,DllRegisterServer

No.	Time	Source	Destination	Protocol	Length	Info
1232	101.017251	10.12.15.101	162.241.219.74	HTTP	293	GET /crizzszfsx/5555555555.jpg HTTP/1.1

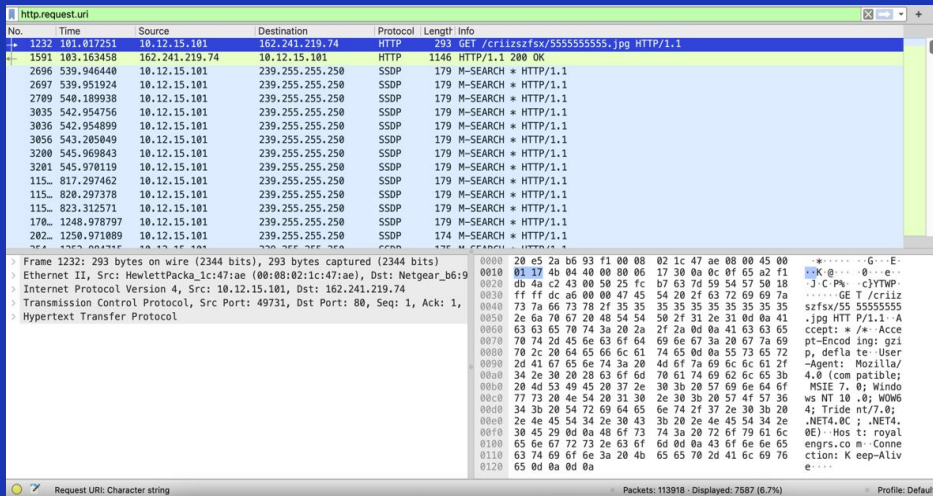
  

Packet	Hostname	Content Type	Size	Filename
1591	royalengrs.com	application/octet-stream	630 kB	5555555555.jpg

# IOCs

## Initial files, zip and links

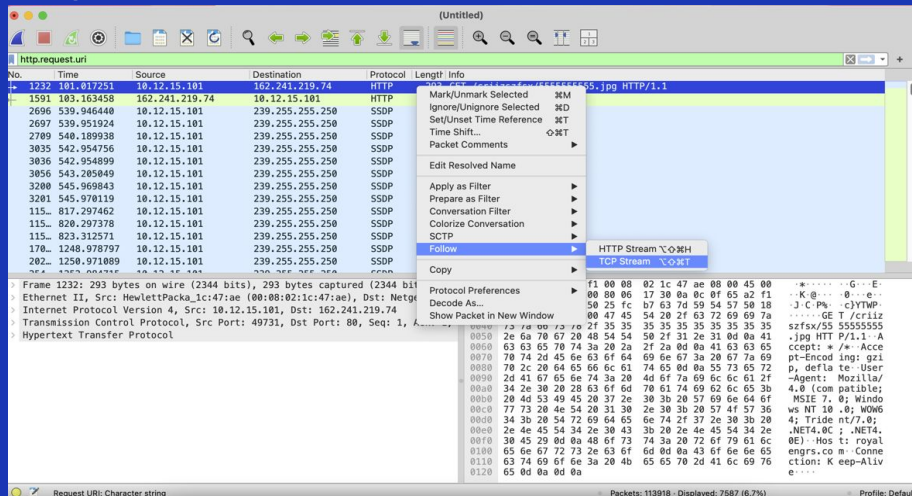
Find HTTP requests



No.	Time	Source	Destination	Protocol	Length	Info
1232	101.017251	10.12.15.101	162.241.219.74	HTTP	293	GET /cr12szsf5x/55555555.jpg HTTP/1.1
1591	103.163458	162.241.219.74	10.12.15.101	HTTP	1146	HTTP/1.1 200 OK
2696	539.946440	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
2697	539.951924	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
2769	540.189938	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3035	542.954756	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3036	542.954899	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3056	543.205849	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3200	545.969843	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3201	545.970119	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
115..	817.297462	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
115..	820.297378	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
115..	823.312571	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
202..	1250.971089	10.12.15.101	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1

Frame 1232: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0  
Ethernet II, Src: Hewlett-Packard\_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear\_b6:91:02:00:00:00:00:00  
Internet Protocol Version 4, Src: 10.12.15.101, Dst: 162.241.219.74  
Transmission Control Protocol, Src Port: 49731, Dst Port: 80, Seq: 1, Ack: 1, Window: 65535  
Hypertext Transfer Protocol

Follow TCP stream to confirm and try to export the file



No.	Time	Source	Destination	Protocol	Length	Info
1232	101.017251	10.12.15.101	162.241.219.74	HTTP	293	GET /cr12szsf5x/55555555.jpg HTTP/1.1
1591	103.163458	162.241.219.74	10.12.15.101	HTTP	1146	HTTP/1.1 200 OK
2696	539.946440	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
2697	539.951924	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
2769	540.189938	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3035	542.954756	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3036	542.954899	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3056	543.205849	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3200	545.969843	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3201	545.970119	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
115..	817.297462	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
115..	820.297378	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
115..	823.312571	10.12.15.101	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
170..	1248.978797	10.12.15.101	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
202..	1250.971089	10.12.15.101	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1

Frame 1232: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0  
Ethernet II, Src: Hewlett-Packard\_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear\_b6:91:02:00:00:00:00:00  
Internet Protocol Version 4, Src: 10.12.15.101, Dst: 162.241.219.74  
Transmission Control Protocol, Src Port: 49731, Dst Port: 80, Seq: 1, Ack: 1, Window: 65535  
Hypertext Transfer Protocol

# IOCs

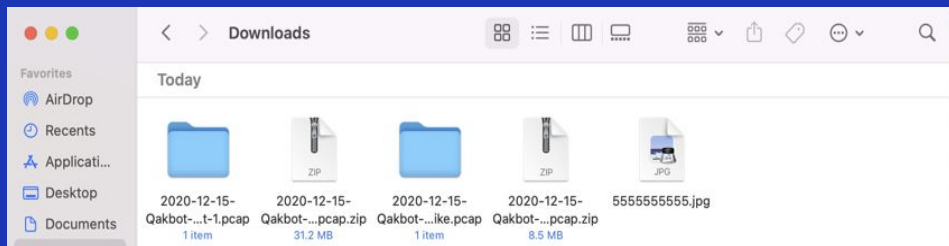
## Initial files, zip and links

### Export file

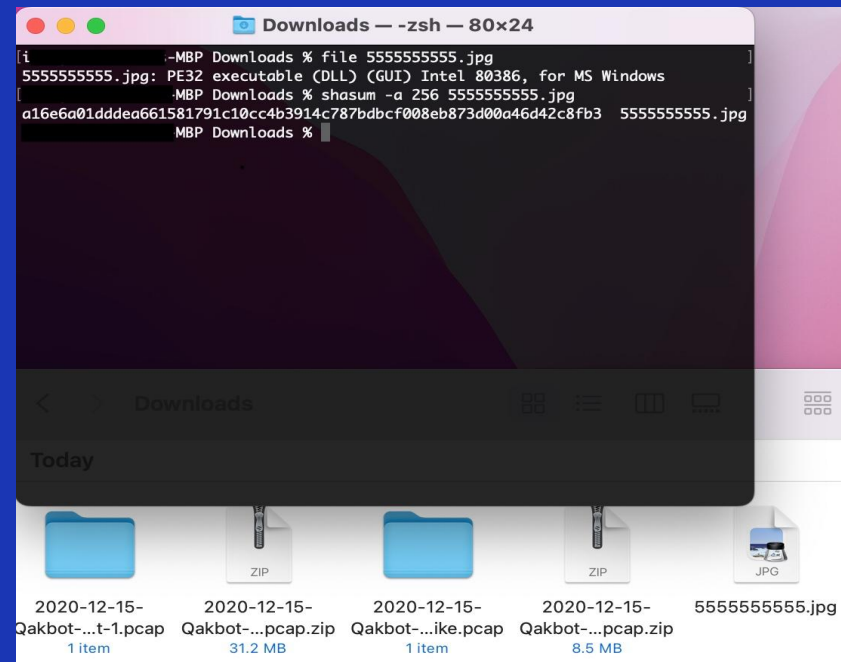
Wireshark · Export · HTTP object list

Text Filter:  Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
1591	royalengrs.com	application/octet-stream	630 kB	5555555555.jpg
49891			1460 bytes	
49895			1388 bytes	
49896			1388 bytes	
49897			1460 bytes	
49909			1316 bytes	



### Checking exploited file Checksum



# IOCs

## Initial files, zip and links

Submitted to VirusTotal

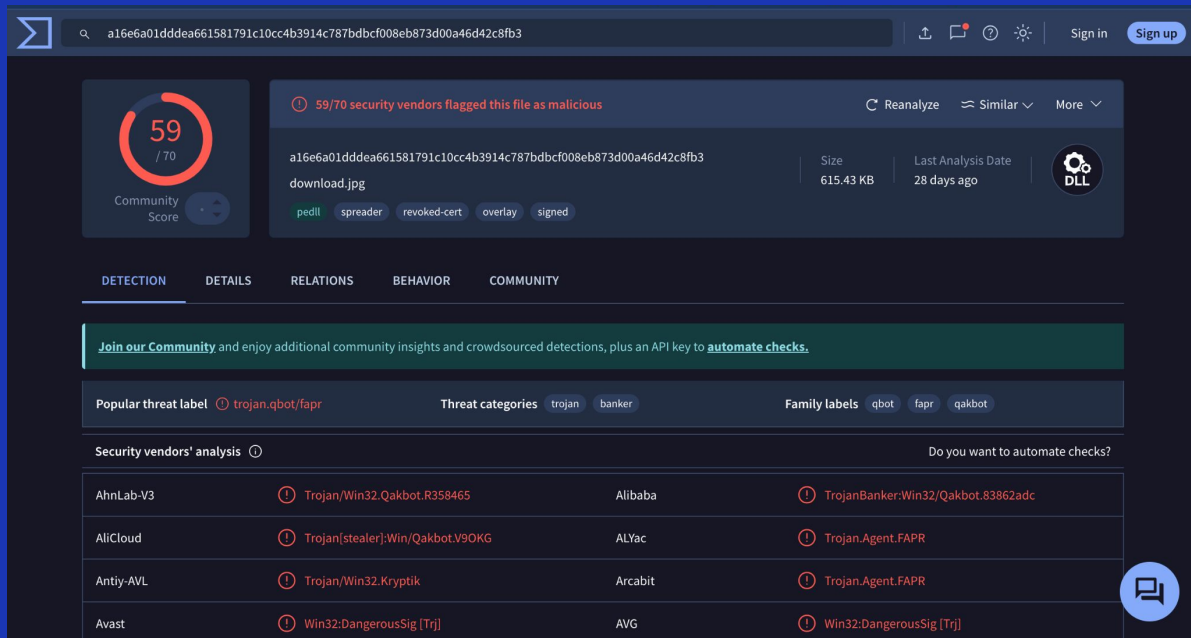
File Identified as Malicious:

**Trojan.Qakbot/FAPR.**

The detection suggests this file is associated with **Qakbot**, a well-known banking Trojan often used to steal credentials, financial information, and act as a downloader for additional malware.

**Family Tags:**

Tags such as **Qbot**, **Trojan**, and **Banker** indicate that this malware primarily targets financial systems and credentials, making it a significant risk.



The screenshot shows the VirusTotal analysis interface for a file. The file hash is a16e6a01dddea661581791c10cc4b3914c787bdbc008eb873d00a46d42c8fb3. The file is identified as download.jpg, 615.43 KB, and was last analyzed 28 days ago. The file is flagged as malicious by 59/70 security vendors. The file is associated with the Trojan.Qakbot/FAPR family. The file is a DLL. The file is associated with the tags: pedll, 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 checks](#).

Popular threat label **trojan.qbot/fapr** Threat categories **trojan** **banker** Family labels **qbot** **fapr** **qakbot**

Security vendors' analysis ☐ Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Qakbot.R358465	Alibaba	TrojanBanker:Win32/Qakbot.83862adc
AliCloud	Trojan[stealer]:Win/Qakbot.V9OKG	ALYac	Trojan.Agent.FAPR
Antiy-AVL	Trojan/Win32.Kryptik	Arcabit	Trojan.Agent.FAPR
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]

# IOCs

## Initial files, zip and links

### Email Phishing Attempts with attached files

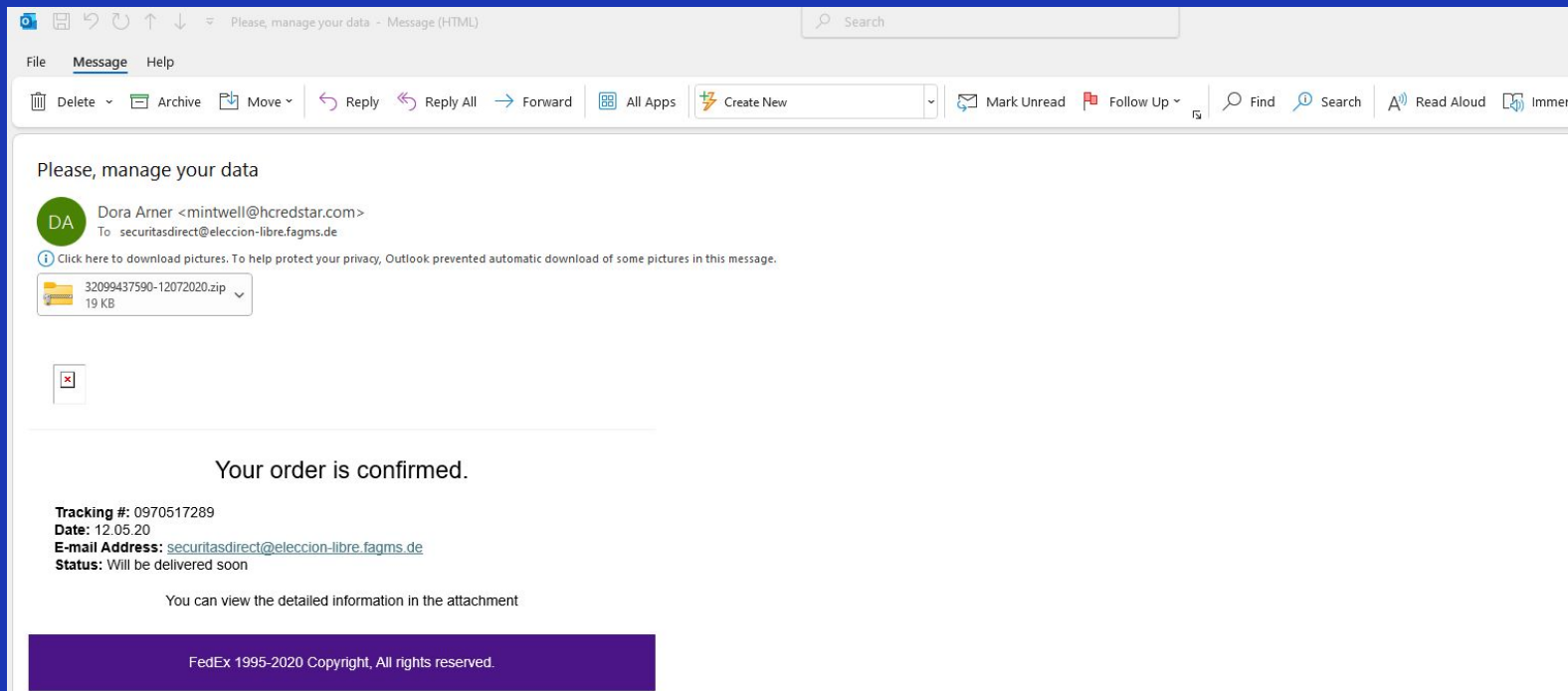
smtp.data.fragment						
No.	Time	Source	Destination	Protocol	Length	Info
21785	3209.674319	10.12.7.101	202.181.230.89	SMTP/I...	1209	subject: =?UTF-8?B?UGx1YXNlLCBtYW5hZ2Ugew91ciBkYXRh?=?, (text/html) (application/zip)   .
24388	3393.076886	10.12.7.101	175.98.142.67	SMTP/I...	474	from: "Sina Kettner" <sevenchiang@cuncyue.com>, subject: =?UTF-8?B?Ww91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=?, (text/html) (application/zip)   .
25943	3506.812320	10.12.7.101	143.95.249.137	SMTP/I...	1214	from: "Matthew Ganz" <valerie@nysfam.com>, subject: =?UTF-8?B?SW52YWxpZCBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=?, (text/html) (application/zip)   .
27858	3614.159716	10.12.7.101	185.81.2.164	SMTP/I...	469	from: "Nicholas Michels" <lruggeri@dagcom.com>, subject: =?UTF-8?B?Ww91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=?, (text/html) (application/zip)   .
29624	3669.692888	10.12.7.101	185.250.242.52	SMTP/I...	1317	from: "Lula Carbaugh" <k.suerdem@kbs-legal.com>, subject: =?UTF-8?B?Ww91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=?, (text/html) (application/zip)   .
30999	3710.722041	10.12.7.101	210.242.150.168	SMTP/I...	1071	from: "Gene Carlyle" <vivi.liang@tienpou.com>, subject: =?UTF-8?B?Ww91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=?, (text/html) (application/zip)   .
34164	3857.395677	10.12.7.101	124.150.143.188	SMTP/I...	930	subject: =?UTF-8?B?SW52YWxpZCBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=?, (text/html) (application/zip)   .

Wireshark - Export - IMF object list				
Text Filter:				
Content Type: All Content-Types				
Packet	Hostname	Content Type	Size	Filename
21785		EML file	28 kB	=?UTF-8?B?UGx1YXNlLCBtYW5hZ2Ugew91ciBkYXRh?=.eml
24388	sevenchiang@cuncyue.com	EML file	28 kB	=?UTF-8?B?Ww91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=.eml
25943	valerie@nysfam.com	EML file	29 kB	=?UTF-8?B?SW52YWxpZCBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=.eml
27858	lruggeri@dagcom.com	EML file	28 kB	=?UTF-8?B?Ww91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=.eml
29624	k.suerdem@kbs-legal.com	EML file	28 kB	=?UTF-8?B?Ww91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=.eml
30999	vivi.liang@tienpou.com	EML file	28 kB	=?UTF-8?B?Ww91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=.eml
34164		EML file	33 kB	=?UTF-8?B?SW52YWxpZCBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ=?=.eml

# IOCs Initial files, zip and links

## Email Phishing Attempts with attached files



Confidential

Copyright ©

By: Isael Melendez

# IOCs Initial files, zip and links

## EML Exported files and phishing email examples

✉ = %3fUTF-8%3fB%3fSW52YWxpZCBzaGlwbWVudCBhZGRyZXNz%3f=(1)	11/17/2024 9:31 AM	E-mail Message	34 KB
✉ = %3fUTF-8%3fB%3fSW52YWxpZCBzaGlwbWVudCBhZGRyZXNz%3f=	11/17/2024 9:31 AM	E-mail Message	30 KB
✉ = %3fUTF-8%3fB%3fUGxIXNILCBtYW5hZ2UgeW91ciBkYXRh%3f=	11/17/2024 9:31 AM	E-mail Message	28 KB
✉ = %3fUTF-8%3fB%3fWW91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ= %3f=(1)	11/17/2024 9:31 AM	E-mail Message	28 KB
✉ = %3fUTF-8%3fB%3fWW91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ= %3f=(2)	11/17/2024 9:31 AM	E-mail Message	28 KB
✉ = %3fUTF-8%3fB%3fWW91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ= %3f=(3)	11/17/2024 9:31 AM	E-mail Message	28 KB
✉ = %3fUTF-8%3fB%3fWW91ciBzaGlwbWVudCBhZGRyZXNzIGlzIGludmFsaWQ= %3f=	11/17/2024 9:31 AM	E-mail Message	28 KB

Total 1 Emails

✉ Subject:Invalid shipment address

From: gst\_csb@carimin.com

Date: 07/12/2020, 21:53:07

Subject:Invalid shipment address

To: (service@flobbo.de)

From: Carline Mccary

From Address: gst\_csb@carimin.com

Date: 07/12/2020, 21:53:07

📎 21235375580-12072020.zip

Your package is on its way.

Order #: 3772396122  
Date: 12.08.20  
E-mail : service@flobbo.de  
Status: Will be delivered soon

You can download the detailed information in the attached file

FedEx 1995-2020 Copyright. All rights reserved.

Total 1 Emails

✉ Subject:Invalid shipment address

From: valerie@nysfam.com

Date: 07/12/2020, 21:47:20

Subject:Invalid shipment address


To: (seniorpeoplemeet.com.dating@zipper.pjscore.us)

From: Matthew Ganz

From Address: valerie@nysfam.com

Date: 07/12/2020, 21:47:20

📎 32069264980-12072020.zip

Jogo

Your order will be delivered soon.

Tracking Number: 023438894  
Date: 12.08.2020  
E-mail Address: seniorpeoplemeet.com.dating@zipper.pjscore.us  
Status: Confirmed

You can check the detailed information in the attached file

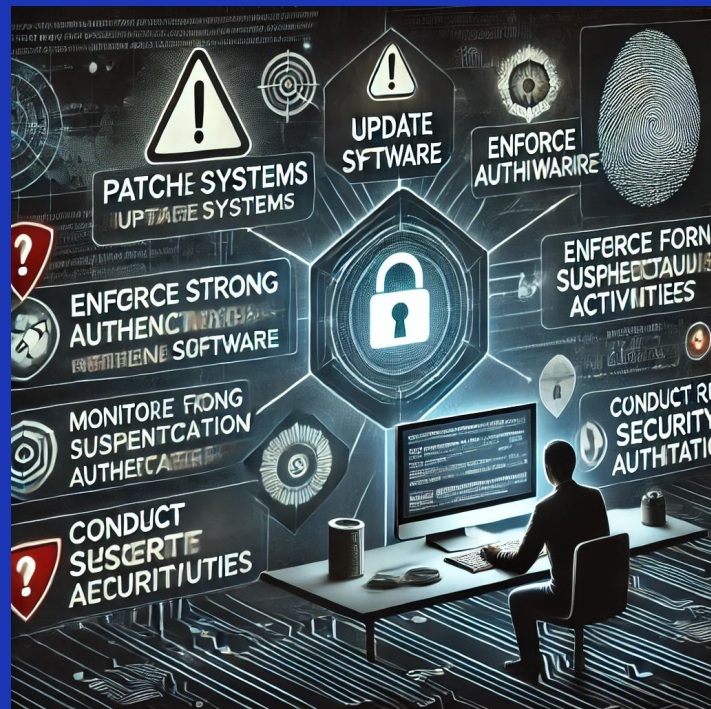
FedEx 1995-2020 Copyright. All rights reserved.



# 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

Case Management System involves the process of organizing, tracking, and investigating cybersecurity incidents to effectively respond to threats. It includes collecting and analyzing relevant data, managing workflows from detection to resolution, and ensuring that appropriate actions are taken to mitigate risks. By leveraging Case Management System(CSM), organizations can streamline incident handling, improve response times, and enhance overall security posture. CSM allows security teams to document actions, track progress, and analyze trends, helping to prevent future incidents and strengthen defenses.



# Conclusion

**Cobalt Strike** is a powerful tool that can be used both for legitimate penetration testing and malicious cyber activities. Its advanced features, such as the ability to mimic legitimate network traffic, establish robust Command and Control (C2) channels, and facilitate lateral movement within a network, make it a significant threat in the hands of cybercriminals.

Best Cybersecurity Practices to Combat Cobalt Strike:

- **Continuous Monitoring**: Implement real-time network monitoring and anomaly detection systems to identify unusual activities promptly.
- **Incident Response Plan**: Develop and regularly update an incident response plan to ensure quick and effective action in case of a security breach.
- **Employee Training**: Conduct regular cybersecurity awareness training to educate employees about phishing attacks, social engineering, and safe internet practices.
- **Threat Intelligence**: Stay informed about the latest threats and attack vectors by leveraging threat intelligence feeds and sharing information within the cybersecurity community.

By adopting these best practices, organizations can strengthen their defenses, detect potential threats early, and respond effectively to mitigate the risks posed by tools like Cobalt Strike.