

**CODEPATH\***  
**CYB102**

# Group 17 Capstone

Bryan Zevallos  
Didier Desmangles  
Isael Melendez  
Giancarlo Montes



# 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 steal 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

all.pcap

No.	Time	Source	Destination	Protocol	Length	Info
446	16:45.908956	74.125.137.28	10.12.15.101	SMTP	111 S:	220 smtp-relay.gmail.com ESMTP q26sm352550ov.24 - gsmtp
447	16:45.909007	74.125.137.28	10.12.15.101	SMTP	118 S:	220 smtp-relay.gmail.com ESMTP l26sm352550ov.10 - gsmtp
447	16:45.909080	74.125.137.28	10.12.15.101	SMTP	110 S:	220 smtp-relay.gmail.com ESMTP p26sm352550ov.10 - gsmtp
447	16:45.909099	74.125.137.28	10.12.15.101	SMTP	109 S:	220 smtp-relay.gmail.com ESMTP q12sm4516vsm.10 - gsmtp
456..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	113 S:	220 smtp-relay.gmail.com ESMTP s18sm64638vka.12 - gsmtp
456..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	111 S:	220 smtp-relay.gmail.com ESMTP go24sm20520pbjh.8 - gsmtp
457..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	118 S:	220 smtp-relay.gmail.com ESMTP l12sm45380tbn.1 - gsmtp
457..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	118 S:	220 smtp-relay.gmail.com ESMTP l12sm45380tbn.1 - gsmtp
460..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	118 S:	220 smtp-relay.gmail.com ESMTP l12sm45380tbn.1 - gsmtp
460..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	118 S:	220 smtp-relay.gmail.com ESMTP c86sm50080oo.19 - gsmtp
461..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	111 S:	220 smtp-relay.gmail.com ESMTP V14sm57030oo.15 - gsmtp
461..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	108 S:	220 smtp-relay.gmail.com ESMTP l18sm1678pt.2 - gsmtp
464..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	118 S:	220 smtp-relay.gmail.com ESMTP c8sm52330oo.19 - gsmtp
464..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	111 S:	220 smtp-relay.gmail.com ESMTP p127sm17513vk.2 - gsmtp
465..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	118 S:	220 smtp-relay.gmail.com ESMTP z12sm61618oo.9 - gsmtp
466..	16:45.909101	74.125.137.28	10.12.15.101	SMTP	111 S:	220 smtp-relay.gmail.com ESMTP d18sm44612qkc.8 - gsmtp

all.pcap

No.	Time	Source	Destination	Protocol	Length	Info
51.102	10:12.15.101			POP	134 S:	+OK POP3 Bigfoot v1.0 server ready <4312.1608069573@mail12c26.carrierzone.com>
51.102	10:12.15.101			POP	135 S:	+OK POP3 Bigfoot v1.0 server ready <32705.1608069581@mail31c26.carrierzone.com>
51.102	10:12.15.101			POP	135 S:	+OK POP3 Bigfoot v1.0 server ready <17759.1608071084@mail12c26.carrierzone.com>
51.102	10:12.15.101			POP	135 S:	+OK POP3 Bigfoot v1.0 server ready <17662.1608071099@mail12c26.carrierzone.com>
51.102	10:12.15.101			POP	135 S:	+OK POP3 Bigfoot v1.0 server ready <30805.1608071030@mail31c26.carrierzone.com>
51.102	10:12.15.101			POP	133 S:	+OK POP3 Bigfoot v1.0 server ready <355.1608071538@mail19c26.carrierzone.com>
51.102	10:12.15.101			POP	134 S:	+OK POP3 Bigfoot v1.0 server ready <6412.1608071801@mail31c26.carrierzone.com>
51.102	10:12.15.101			POP	134 S:	+OK POP3 Bigfoot v1.0 server ready <7262.1608071801@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				
Packet	Hostname	Content Type	Size	Filename
1591	royalengrs.com	application/octet-stream	630 kB	5555555555.jpg

Wireshark - Export - HTTP object list				
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

# 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

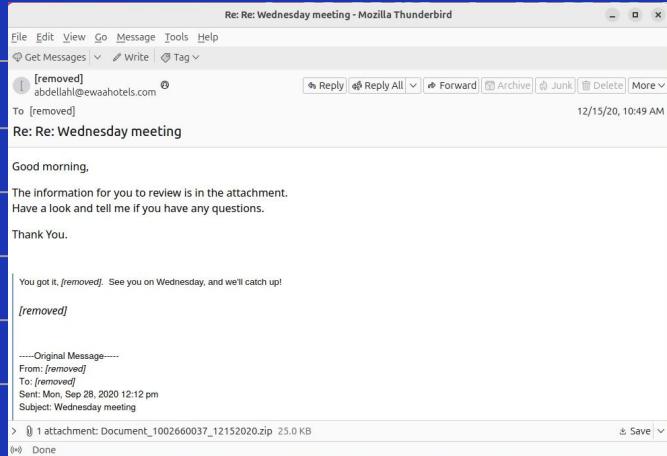
The infected attached files in the mail is a excel macro calling the QBot malware

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
5555555555.jpg->JIOLAS.RRTTOOKK	a16e6a01dddea661581791c10cc4b3914c787bdbcf008eb873d00a46d42c8fb3
bwgacpfhyxqx.dll	05f5bfa493161d093a53a6b953fad443c18e60f85497eca3727ec25733edf57b



# Identified Assets

## Links (COBALT STRIKE)

[matesmapizza.com](http://matesmapizza.com)

[travmeetlett.com](http://travmeetlett.com)

[royalengrs.com](http://royalengrs.com)

Packet	Hostname	Content Type	Size	Filename
7028	matesmapizza.com	application/octet-stream	48 bytes	g9.js
7796	matesmapizza.com	application/octet-stream	200 kb	g9.js
8165	matesmapizza.com	application/octet-stream	200 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	g9.js
9164	matesmapizza.com	application/octet-stream	48 bytes	g9.js
9171	matesmapizza.com	application/octet-stream	420 bytes	submit.php?id=583483712
10341	matesmapizza.com	application/octet-stream	938 kb	g9.js
10986	matesmapizza.com	application/octet-stream	200 kb	updates.rss
11270	matesmapizza.com	application/octet-stream	200 kb	updates.rss
11584	matesmapizza.com	application/octet-stream	200 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

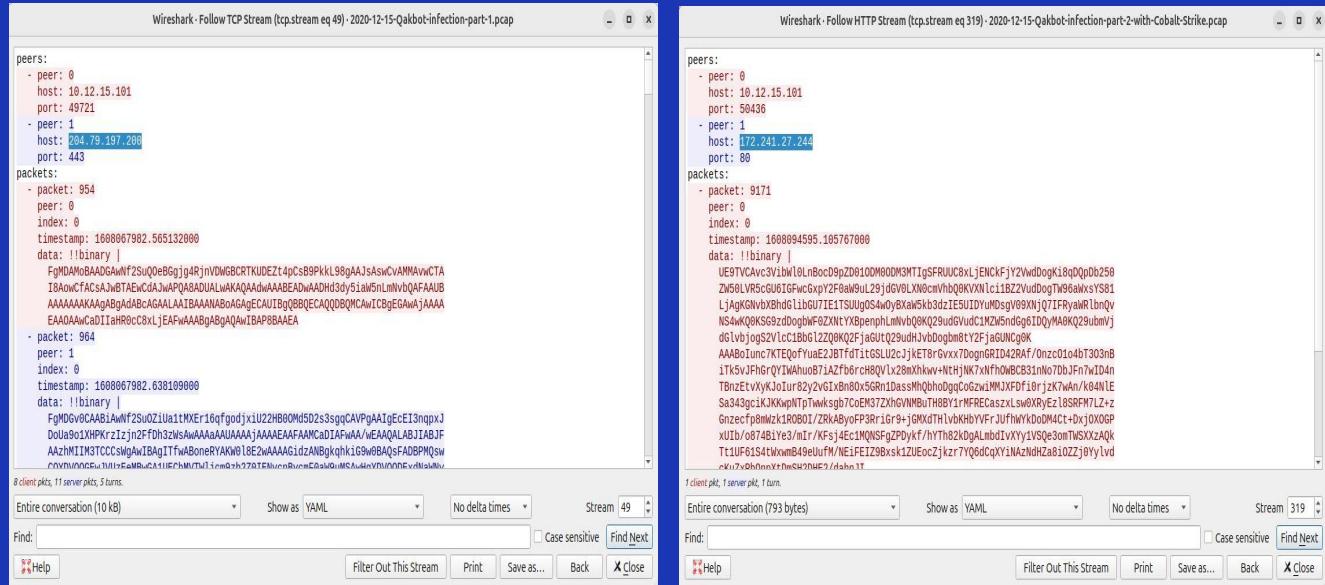
Packet	Hostname	Content Type	Size	Filename
11591	royalengrs.com	application/octet-stream	630 kb	5555555555.jpg

# Identified Assets

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\TREED_ID_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

# 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



# 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.



**Cybersecurity Incident  
& Vulnerability Response Playbooks**

Confide

# 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, 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. Its main use 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)

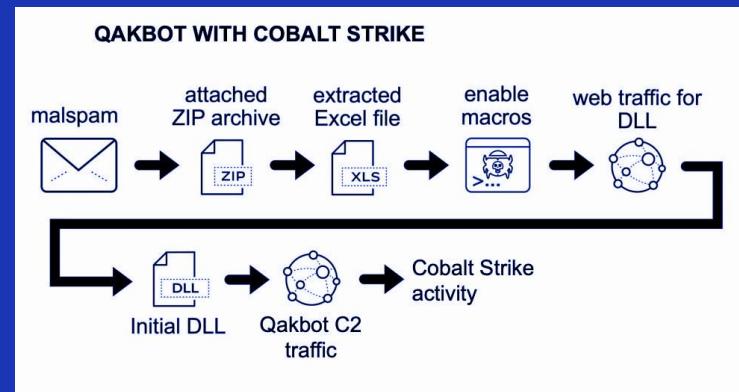


# TTPs

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

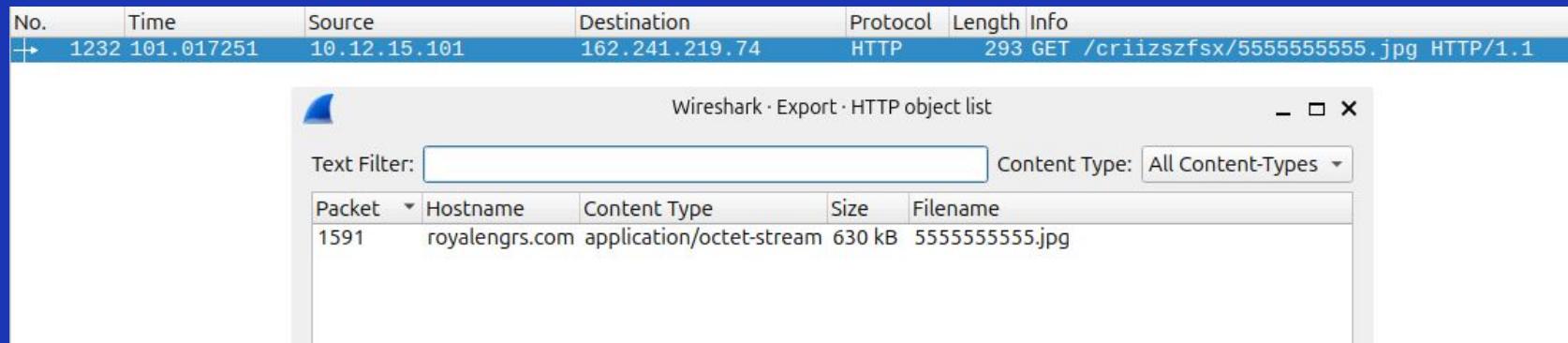
Last Modified: 14 October 2024

[Version Permalink](#)

# TOCs

## MALWARE FROM AN INFECTED WINDOWS HOST:

- **SHA256 hash:** dd592afe3cd134d0fcb0201a48c8af1f7371d99a6fb5d5f0a7568253d459f3f7
- **File size:** 630,200 bytes
- **File location:** http://royalengrs.com/criizzfsx/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



The screenshot shows a Wireshark capture of an HTTP request. The packet details table highlights a GET request from 10.12.15.101 to 162.241.219.74 for the file /criizzfsx/5555555555.jpg. The content pane displays the raw HTTP object list, which includes the host (royalengrs.com), content type (application/octet-stream), size (630 kB), and filename (5555555555.jpg).

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

Wireshark · Export · HTTP object list

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

Follow TCP stream to confirm and try to export the file

The screenshot shows the NetworkMiner interface with the following details:

- Toolbar:** Includes icons for file operations, search, and various analysis tools.
- Header:** (Untitled)
- Panels:**
  - Details:** Shows a table of captured packets with columns: No., Time, Source, Destination, Protocol, Length, Info.
  - Selected:** Shows the selected packet's details: 1222 [10.12.15.101] > 162.24.219.74 [HTTP/1.1].
  - Hex:** Displays the raw hex and ASCII data of the selected packet.
  - Dec:** Displays the decoded data of the selected packet.
  - File:** Shows options for saving the file as a PCAP or PDF.
  - Help:** Includes links to documentation and forums.
- Bottom Panel:** Shows the raw bytes of the selected packet.
- Context Menu:** Opened over the selected packet, containing options like "Edit Resolved Name", "Apply as Filter", "Prepare as Filter", "Conversation Filter", "Colorize Conversation", "Follow", "HTTP Stream", "TCP Stream", and "Copy".

# 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	

Downloads

Today

- 2020-12-15-Qakbot...t-1.pcap
- 2020-12-15-Qakbot...pcap.zip
- 2020-12-15-Qakbot...ike.pcap
- 2020-12-15-Qakbot...pcap.zip
- 5555555555.jpg

## Checking exploited file Checksum

```
[i -MBP Downloads % file 5555555555.jpg
5555555555.jpg: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
[i -MBP Downloads % shasum -a 256 5555555555.jpg
a16e6a01dddea661581791c10cc4b3914c787bdbcf008eb873d00a46d42c8fb3 5555555555.jpg
[MBP Downloads %]
```

Downloads

Today

- 2020-12-15-Qakbot...t-1.pcap
- 2020-12-15-Qakbot...pcap.zip
- 2020-12-15-Qakbot...ike.pcap
- 2020-12-15-Qakbot...pcap.zip
- 5555555555.jpg

# TOCs 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 page for the file `a16e6a01dddea661581791c10cc4b3914c787bdbcf008eb873d00a46d42c8fb3`. The main interface includes:

- Community Score:** 59 / 70
- File Details:** download.jpg, Size: 615.43 KB, Last Analysis Date: 28 days ago, DLL
- Detection:** 59/70 security vendors flagged this file as malicious
- Behavior:** peddl, spreader, revoked-cert, overlay, signed
- Relations:** trojan, banker
- Community:** qbot, fapr, qakbot
- Popular threat label:** trojan.qbot/fapr
- Security vendors' analysis:** AhnLab-V3, AliCloud, Antiy-AVL, Avast
- Do you want to automate checks?** (checkbox)

# IOCs Initial files, zip and links

## Email Phishing Attempts with attached files

The screenshot shows two windows from the Wireshark application. The top window is titled "smtp.data.fragment" and displays a table of SMTP messages. The columns are: No., Time, Source, Destination, Protocol, Length, and Info. The messages are numbered 21785 through 34164, with various source and destination IP addresses and ports. The protocol is consistently SMTP/I\_. The length column shows values like 1209, 474, 1214, etc. The info column contains detailed subject lines for each message, often including encoded URLs or file paths. The bottom window is titled "Wireshark - Export - IMF object list" and shows a table of EML files. The columns are: Packet, Hostname, Content Type, Size, and Filename. The entries correspond to the messages in the top table, with hostnames such as sevenchiang@cuncyue.com, valerie@nysfam.com, lruggeri@dagcom.com, k.suerdem@kbs-legal.com, vivi.liang@tienpou.com, and the IP address 124.150.143.188. The content type is always EML file, size varies (e.g., 28 kB, 33 kB), and the filename is the same as the subject line.

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?UGxjYXNlCBtYW5hZ2UgeW91ciBkYXRh?=. (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?WW91ciBzaGlwbVVudCBhZGRyZXNzIGlzIGludmFsawQ=?=. (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?SW52YwpZCBzaGlwbVVudCBhZGRyZXNz?=. (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?WW91ciBzaGlwbVVudCBhZGRyZXNzIGlzIGludmFsawQ=?=. (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?WW91ciBzaGlwbVVudCBhZGRyZXNzIGlzIGludmFsawQ=?=. (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?WW91ciBzaGlwbVVudCBhZGRyZXNzIGlziGludmFsawQ=?=. (text/html) (application/zip)   .
34164	3857.395677	10.12.7.101	124.150.143.188	SMTP/I_	930	subject: =?UTF-8?B?SW52YwpZCBzaGlwbVVudCBhZGRyZXNz?=. (text/html) (application/zip)   .

Packet	Hostname	Content Type	Size	Filename
21785		EML file	28 kB	=?UTF-8?B?UGxjYXNlCBtYW5hZ2UgeW91ciBkYXRh?=.eml
24388	sevenchiang@cuncyue.com	EML file	28 kB	=?UTF-8?B?WW91ciBzaGlwbVVudCBhZGRyZXNzIGlzIGludmFsawQ=?=.eml
25943	valerie@nysfam.com	EML file	29 kB	=?UTF-8?B?SW52YwpZCBzaGlwbVVudCBhZGRyZXNz?=.eml
27858	lruggeri@dagcom.com	EML file	28 kB	=?UTF-8?B?WW91ciBzaGlwbVVudCBhZGRyZXNzIGlzIGludmFsawQ=?=.eml
29624	k.suerdem@kbs-legal.com	EML file	28 kB	=?UTF-8?B?WW91ciBzaGlwbVVudCBhZGRyZXNzIGlzIGludmFsawQ=?=.eml
30999	vivi.liang@tienpou.com	EML file	28 kB	=?UTF-8?B?WW91ciBzaGlwbVVudCBhZGRyZXNzIGlzIGludmFsawQ=?=.eml
34164		EML file	33 kB	=?UTF-8?B?SW52YwpZCBzaGlwbVVudCBhZGRyZXNz?=.eml

# IOCs Initial files, zip and links

## Email Phishing Attempts with attached files

Please, manage your data - Message (HTML)

File    Message    Help

Delete    Archive    Move    Reply    Reply All    Forward    All Apps    Create New

Mark Unread    Follow Up    Find    Search    Read Aloud    Immersive

Please, manage your data

DA Dora Arner <mintwell@hcredstar.com>  
To: securitasdirect@eleccion-libre.fagms.de

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

32099437590-12072020.zip  
19 KB

Your order is confirmed.

Tracking #: 0970517289  
Date: 12.05.20  
E-mail Address: [securitasdirect@eleccion-libre.fagms.de](mailto:securitasdirect@eleccion-libre.fagms.de)  
Status: Will be delivered soon

You can view the detailed information in the attachment

FedEx 1995-2020 Copyright, All rights reserved.

Confidential

Copyright ©

By: Israel Melendez

# IOCs Initial files, zip and links

## EML Exported files and phishing email examples

=%3fUTF-8%3fB%3fSW52YWxpZCBzaGlwbVVudCBhZGRyZXNz%3f=(1)	11/17/2024 9:31 AM	E-mail Message	34 KB
=%3fUTF-8%3fB%3fSW52YWxpZCBzaGlwbVVudCBhZGRyZXNz%3f=	11/17/2024 9:31 AM	E-mail Message	30 KB
=%3fUTF-8%3fB%3fUGxIYXNlCBtYW5hZ2UgeW91ciBkYXRh%3f=	11/17/2024 9:31 AM	E-mail Message	28 KB
=%3fUTF-8%3fB%3fWW91ciBzaGlwbVVudCBhZGRyZXNzIGlzIGludmFsaWQ=%3f=(1)	11/17/2024 9:31 AM	E-mail Message	28 KB
=%3fUTF-8%3fB%3fWW91ciBzaGlwbVVudCBhZGRyZXNzIGlzIGludmFsaWQ=%3f=(2)	11/17/2024 9:31 AM	E-mail Message	28 KB
=%3fUTF-8%3fB%3fWW91ciBzaGlwbVVudCBhZGRyZXNzIGlzIGludmFsaWQ=%3f=(3)	11/17/2024 9:31 AM	E-mail Message	28 KB
=%3fUTF-8%3fB%3fWW91ciBzaGlwbVVudCBhZGRyZXNzIGlzIGludmFsaWQ=%3f=	11/17/2024 9:31 AM	E-mail Message	28 KB

Total 1 Emails

**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

**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

Your order will be delivered soon.

Tracking Number: 0234388894  
Date: 12.04.2020  
E-mail Address: seniorpeoplemeet.com.dating@zipper.pjscore.us  
Status: Confirmed

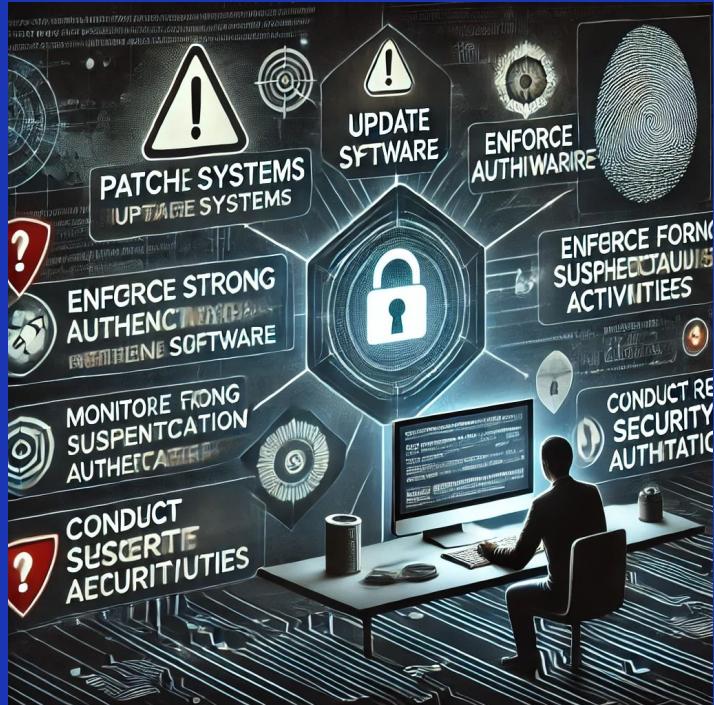
You can check the detailed information in the attached file

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.