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

Confidential

Copyright ©

Table of Content

Confidential

Copyright ©

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.

Confidential

Copyright ©

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.

Confidential

Copyright ©

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

Confidential

Copyright ©

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).**

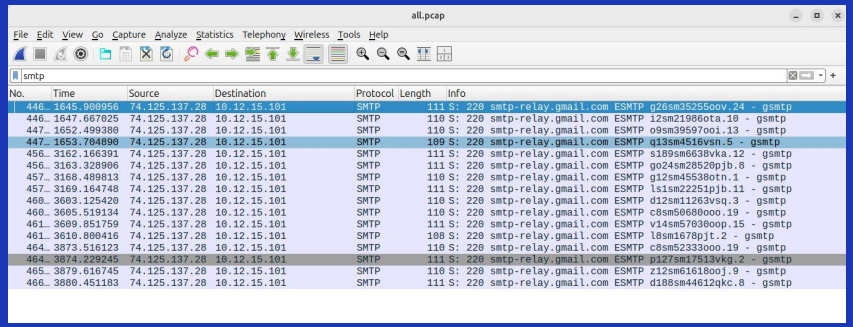
2. **QBot is used as a loader to call Cobalt Strike**

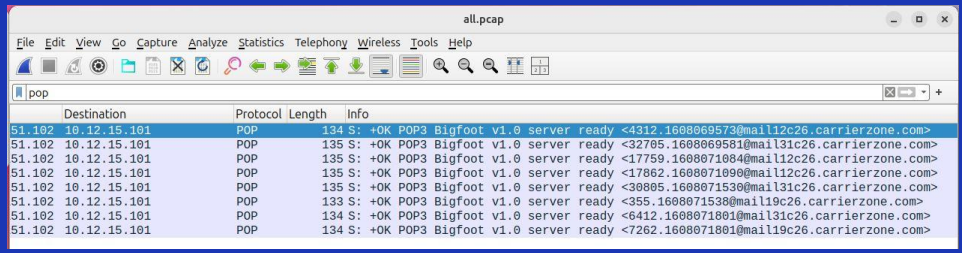
Confidential

Copyright ©

Monitoring Sources

Tactics: Traffic through POP





Confidential

Copyright ©

Monitoring Sources

However we can identify HTTP traffic:

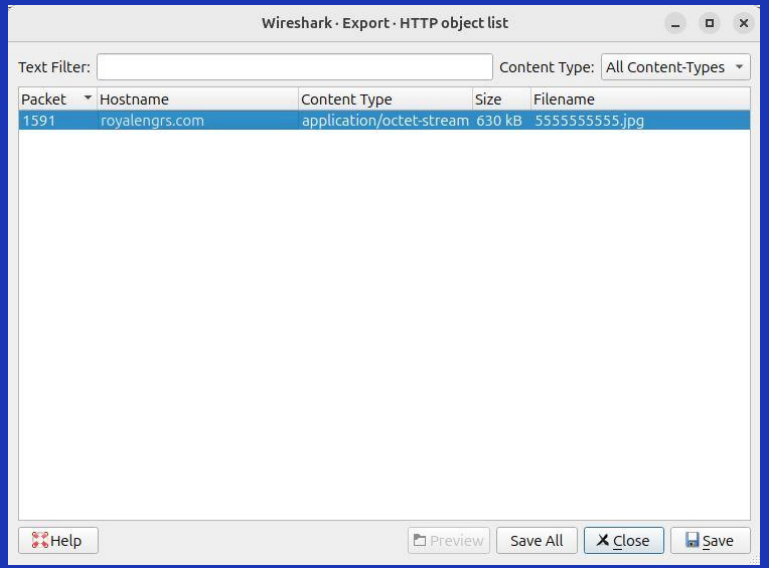
royalengrs.com	IP\162.241.219.74
5555555555.jpg	SHA256\a16e6a01dddea661581791c10cc4b3914c787bdbcf008eb873d00a46d42c8fb3
matesmapizza.com	* malicious website, downloading malware materials. Files might obfurcated
travmeetlett.com	* malicious website, downloading malware materials Files might obfurcated

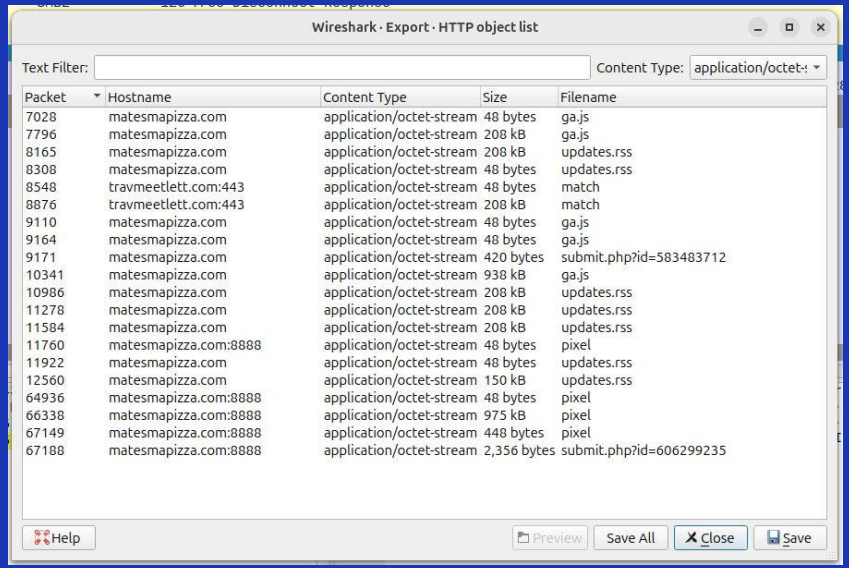
Confidential

Copyright ©

Monitoring Sources

However we can identify HTTP traffic:





Confidential

Copyright ©

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.

Confidential

Copyright ©

Identified Assets

By: Didier Desmangles

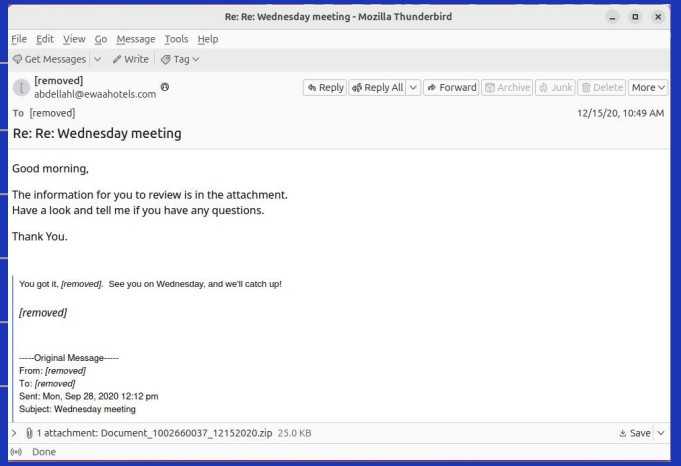
Entry point: Spam campaign in an attempt to find a victim
The infected attached files in the mail is a excel macro calling the QBot malware
The QBot is acting as a loader to call Cobalt Strike via 2 fakes websites
Cobalt Strike tries to steal informations from the Domain Controller (privilege escalation)

Confidential

Copyright ©

Identified Assets

FILENAME	SHA256
Document_1002660037_12152020.zip	6aa9fe7d0f7efce025a2935b4e7edda00cdb2051869cf0f0820deb6f4cddd280
Document_1002660037_12152020.xls	77e6b40ed8b90e08a91f798a00504718ac47a899b4be69ac0bb6558fac40a7e5
5555555555.jpg->JIOLAS.RRTTOOKK	a16e6a01dddea661581791c10cc4b3914c787bdbcf008eb873d00a46d42c8fb3
bxgacpfhyxqx.dll	05f5bfa493161d093a53a6b953fad443c18e60f85497eca3727ec25733edf57b

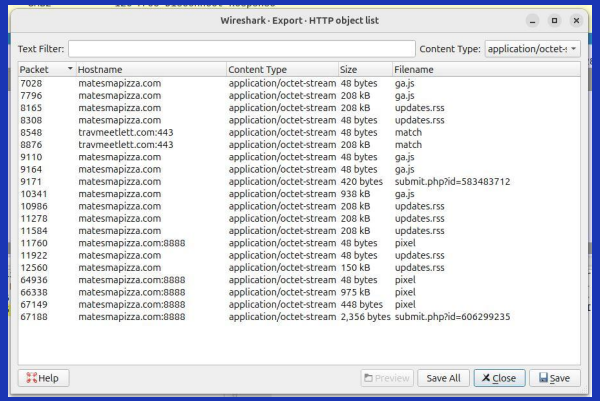


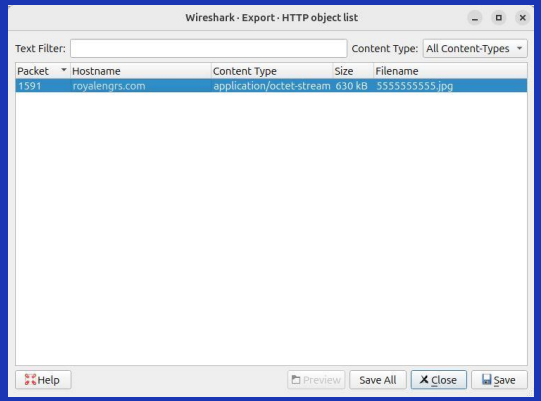
Confidential

Copyright ©

Identified Assets

Links (COBALT STRIKE)
matesmapizza.com
travmeetlett.com
royalengrs.com

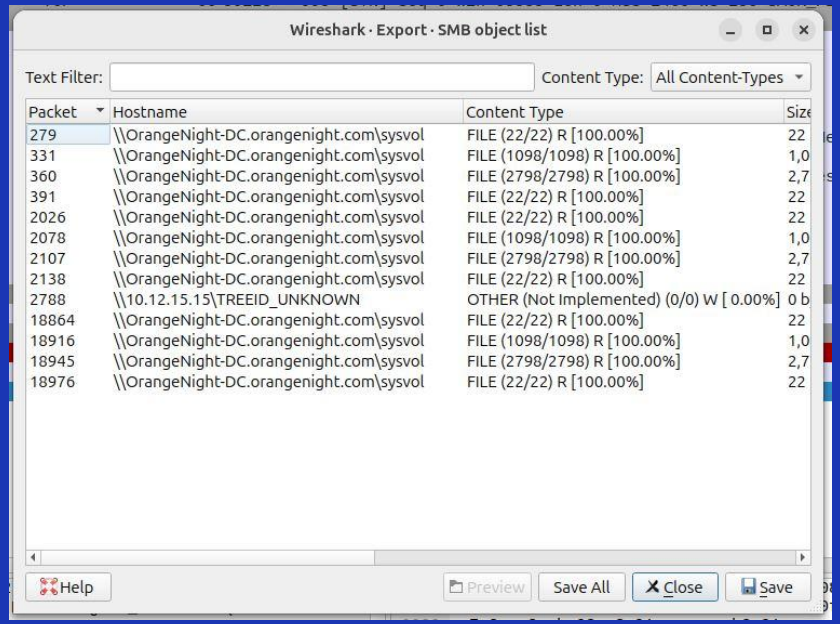




Confidential

Copyright ©

Identified Assets

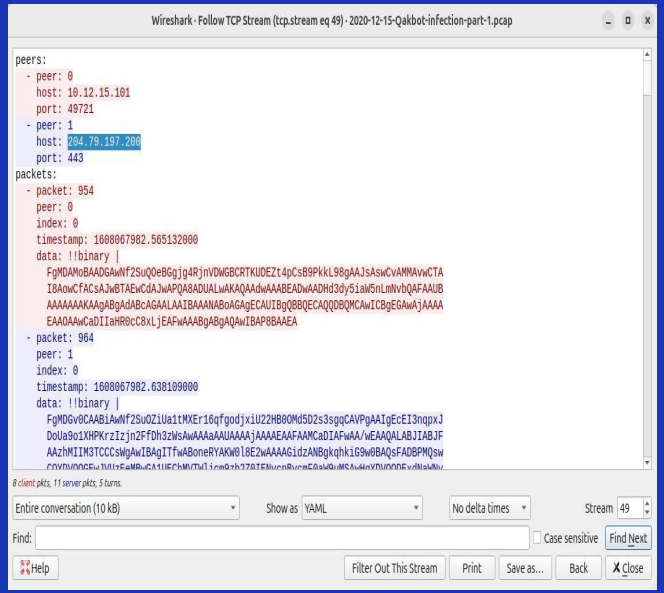


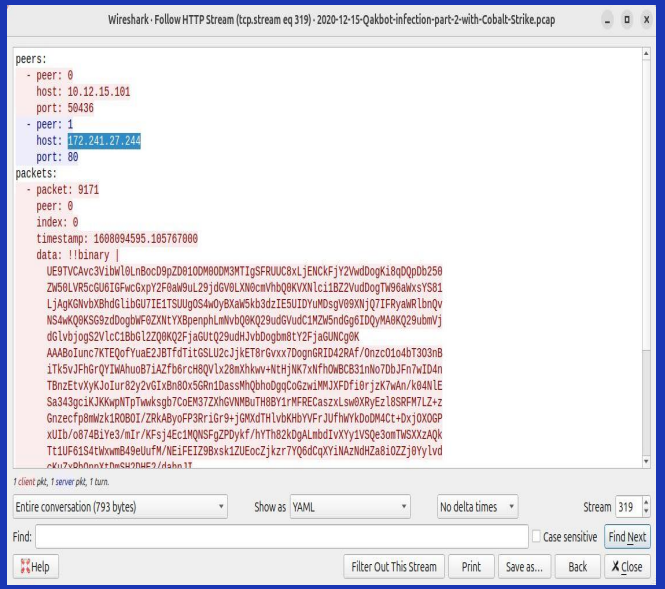
Confidential

Copyright ©

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





Confidential

Copyright ©

Impact Analysis and Triage

By: Giancarlo Montes

Confidential

Copyright ©

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.

Confidential

Copyright ©

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.

Confidential

Copyright ©

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.

Confide

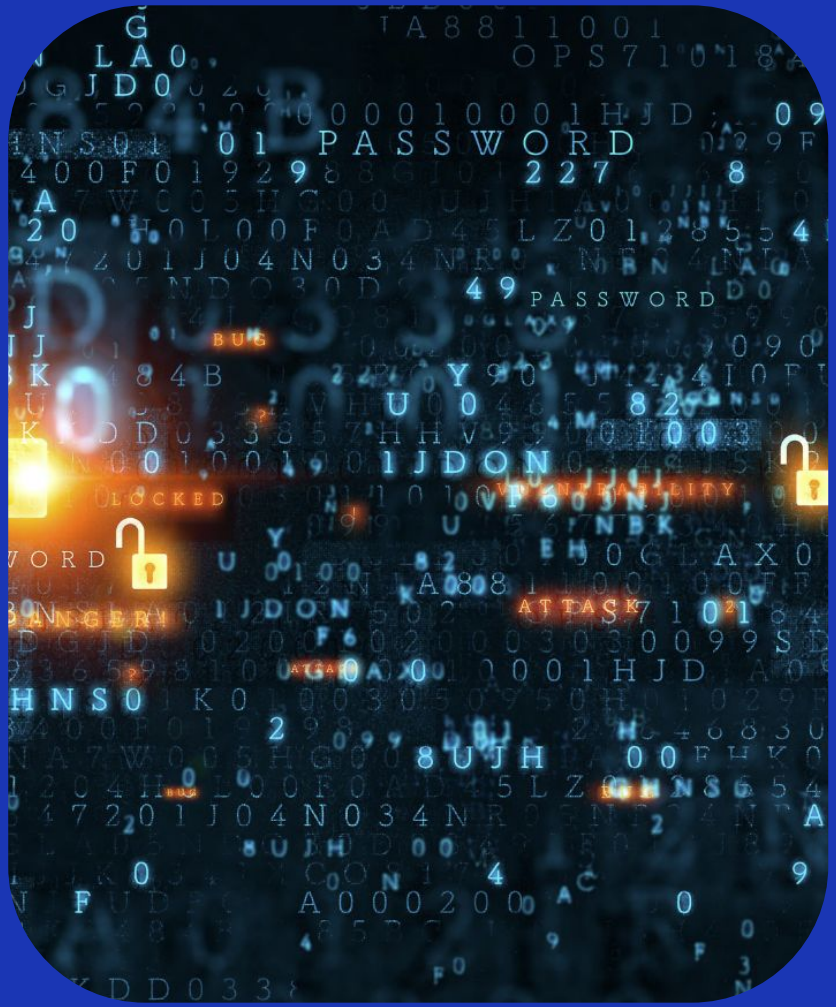
Threat Intelligence

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,.



Confidential

Copyright ©

Overview

QBot, also known as Qakbot, QBot, QuackBot, and Pinkslipbot, 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)

Confidential

Copyright ©

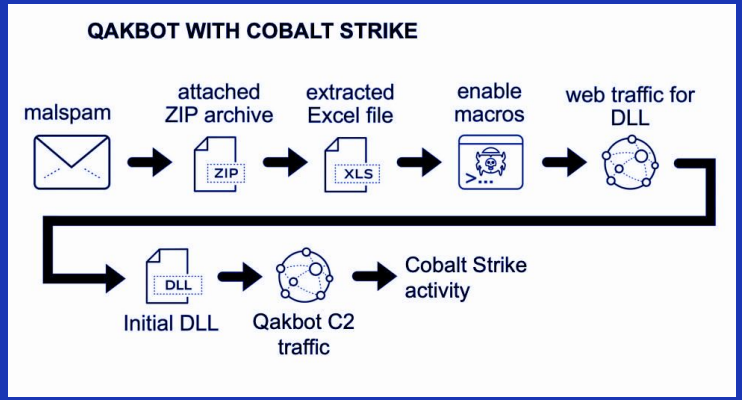
By: Isael Melendez

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)



Confidential

Copyright ©

By: Isael Melendez

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

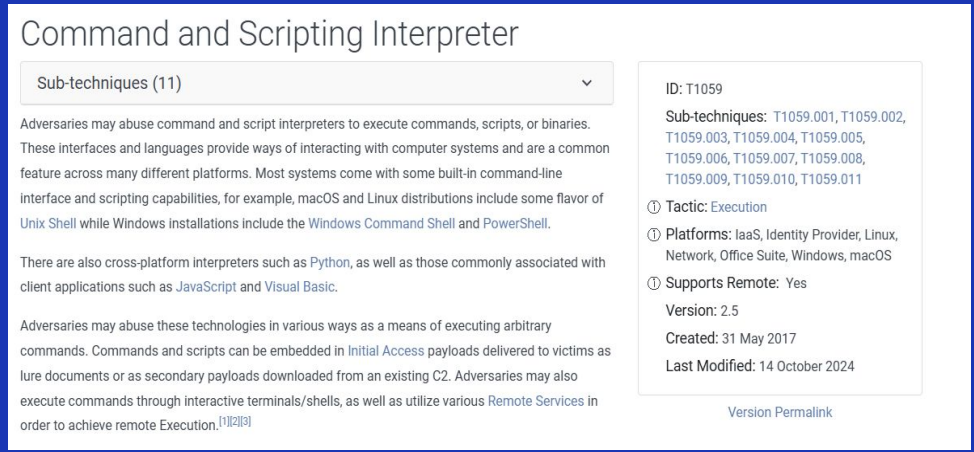
Privilege Escalation
T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder 7

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.[1][2][3]

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

Tactic: Execution

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

Supports Remote: Yes

Version: 2.5

Created: 31 May 2017

Last Modified: 14 October 2024

Version Permalink

Confidential

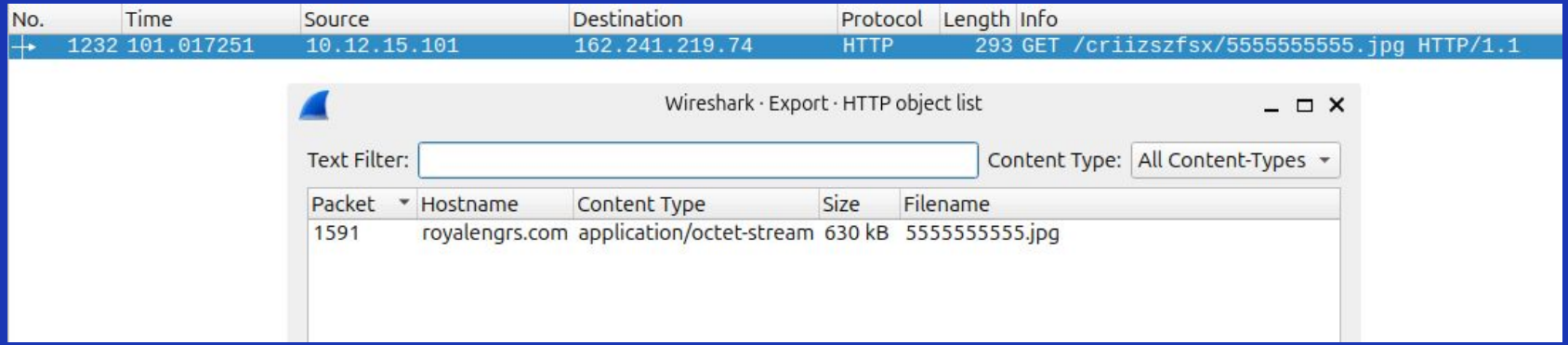
Copyright ©

By: Isael Melendez

IOCs

MALWARE FROM AN INFECTED WINDOWS HOST:

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



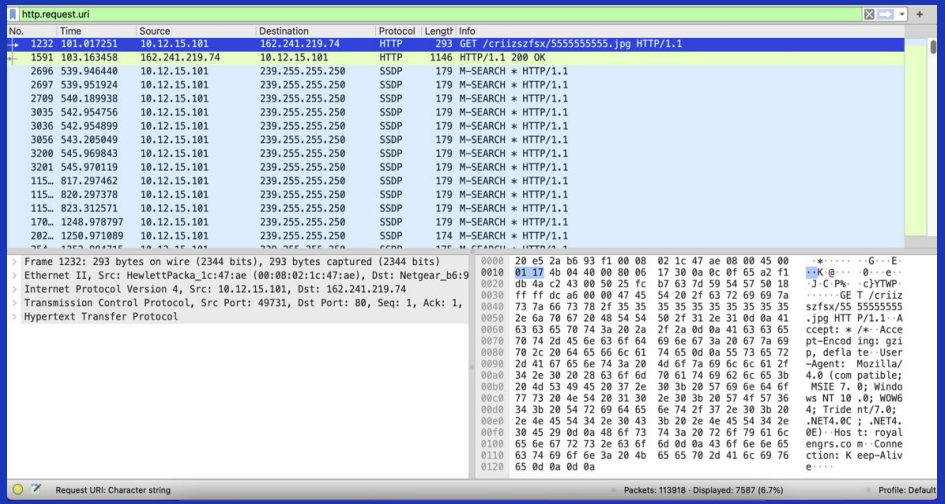
Confidential

Copyright ©

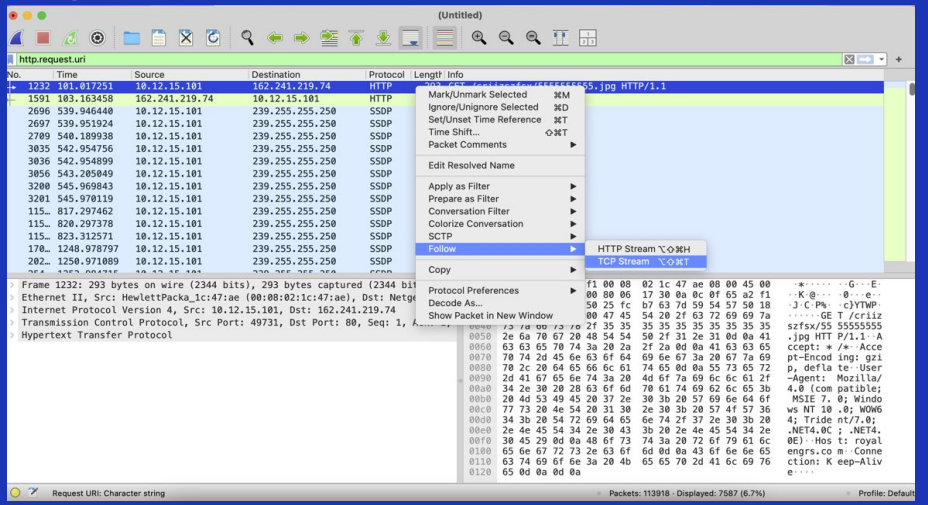
By: Isael Melendez

IOCs Initial files, zip and links

Find HTTP requests



Follow TCP stream to confirm and try to export the file



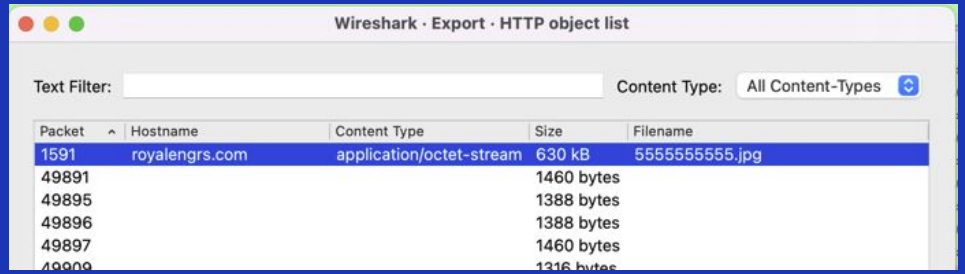
Confidential

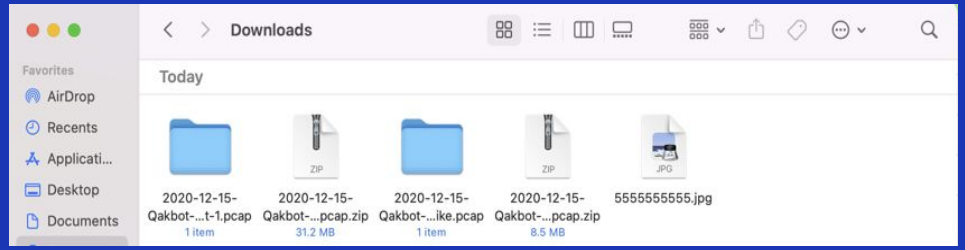
Copyright ©

By: Isael Melendez

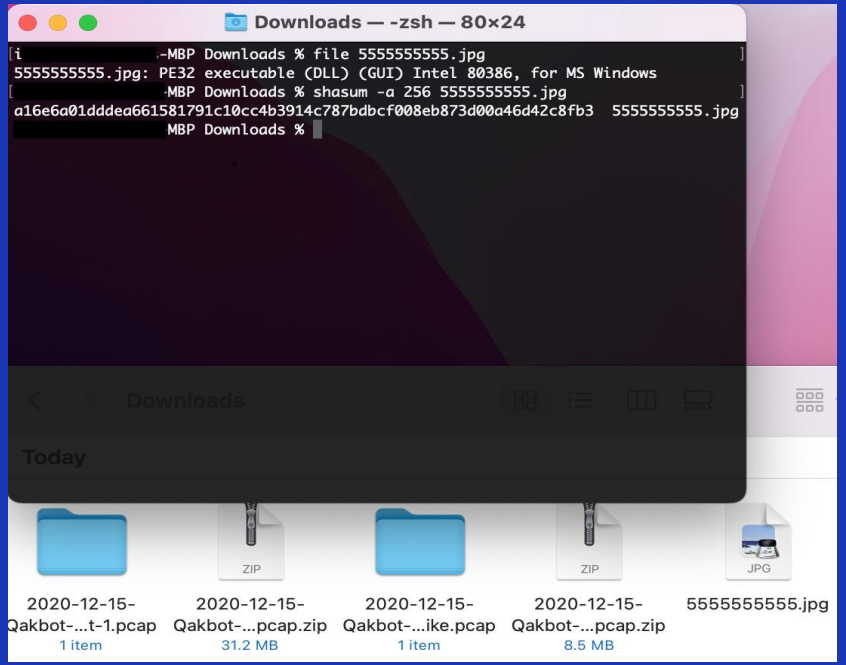
IOCs Initial files, zip and links

Export file





Checking exploited file Checksum



Confidential

Copyright ©

By: Isael Melendez

IOCs Initial files, zip and links

Submitted to VirusTotal

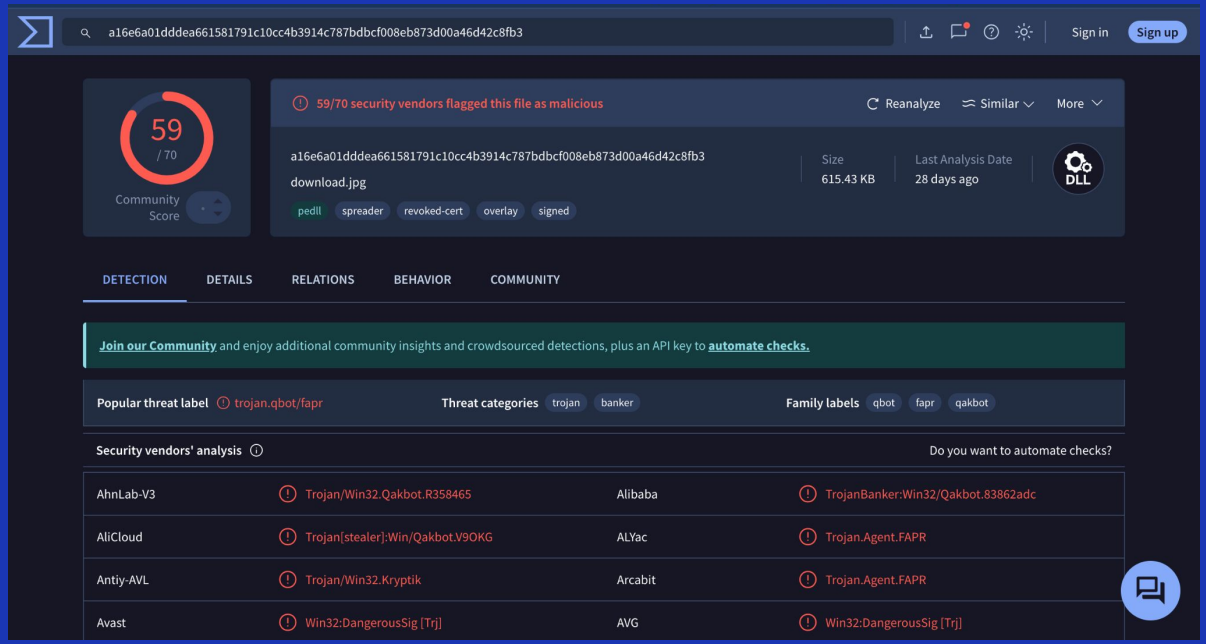
File Identified as Malicious:

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.



Confidential

Copyright ©

By: Isael Melendez

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?UGxlYXNlLCBtYW5hZ2UgeW91ciBkYXRh?=, (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?SW52YWxpZCBzaGlwbWVudCBhZGRyZXNz?=, (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?SW52YWxpZCBzaGlwbWVudCBhZGRyZXNz?=, (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?UGxlYXNlLCBtYW5hZ2UgeW91ciBkYXRh?=.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?SW52YWxpZCBzaGlwbWVudCBhZGRyZXNz?=.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?SW52YWxpZCBzaGlwbWVudCBhZGRyZXNz?=.eml

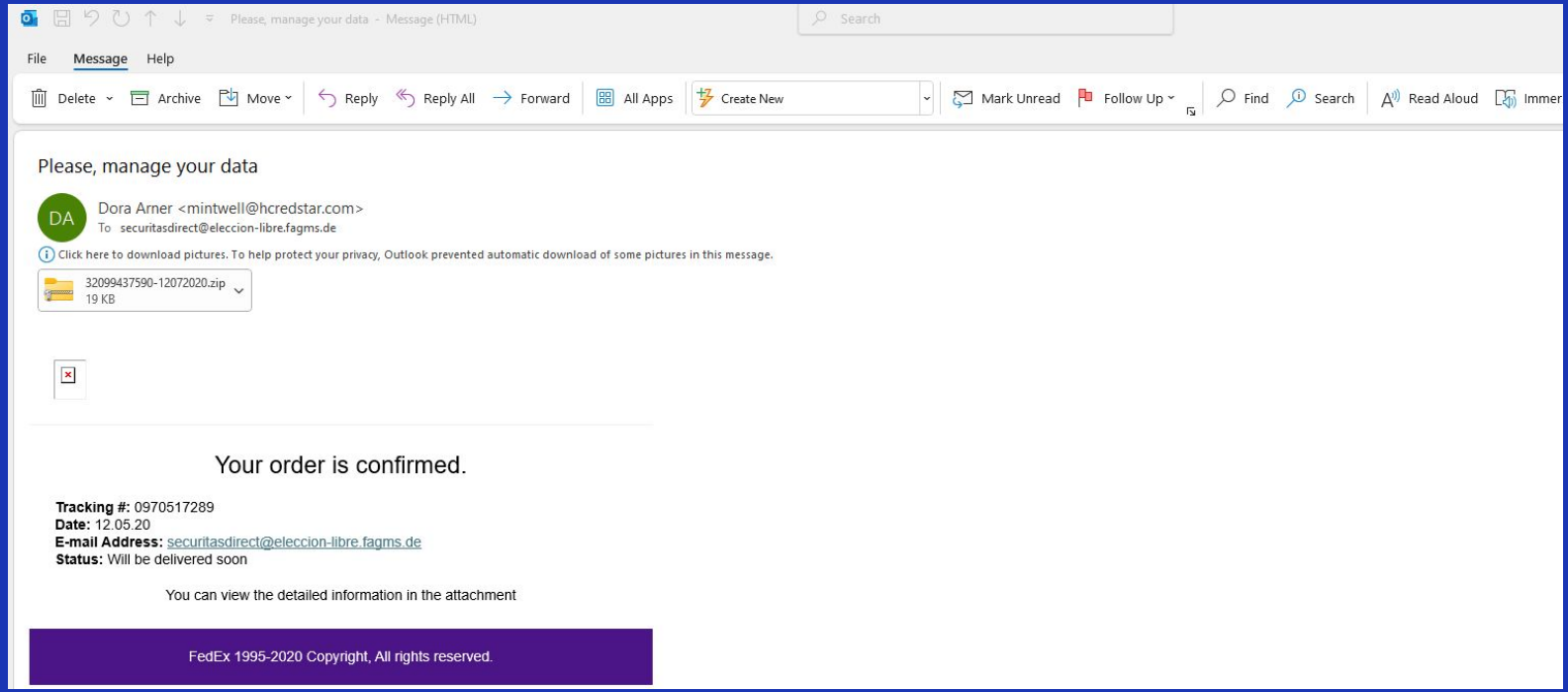
Confidential

Copyright ©

By: Isael Melendez

IOCs Initial files, zip and links

Email Phishing Attempts with attached files



Confidential

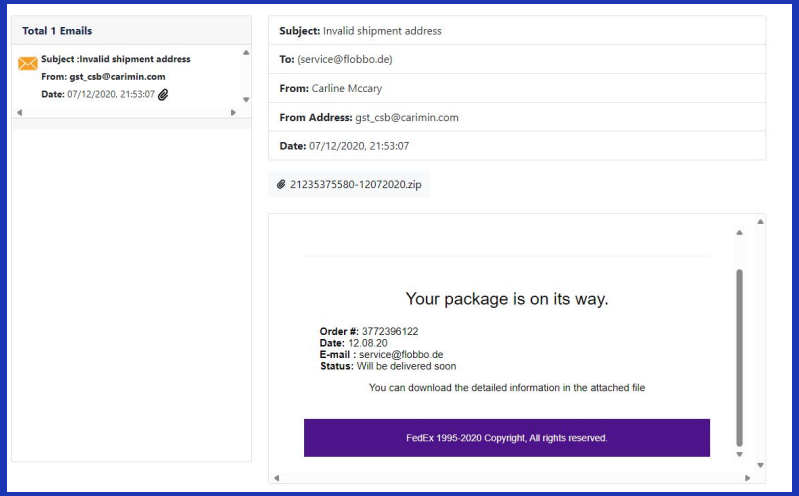
Copyright ©

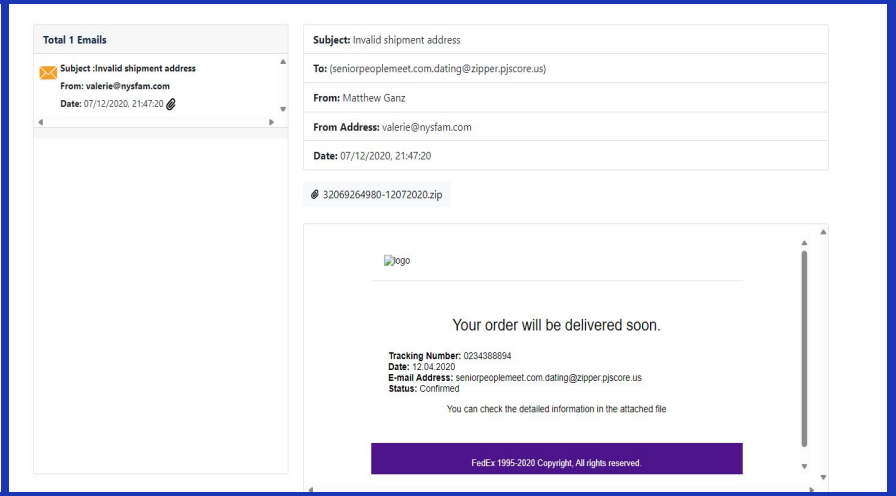
By: Isael Melendez

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%3fUGxlYXNlLCBtYW5hZ2UgeW91ciBkYXRh%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



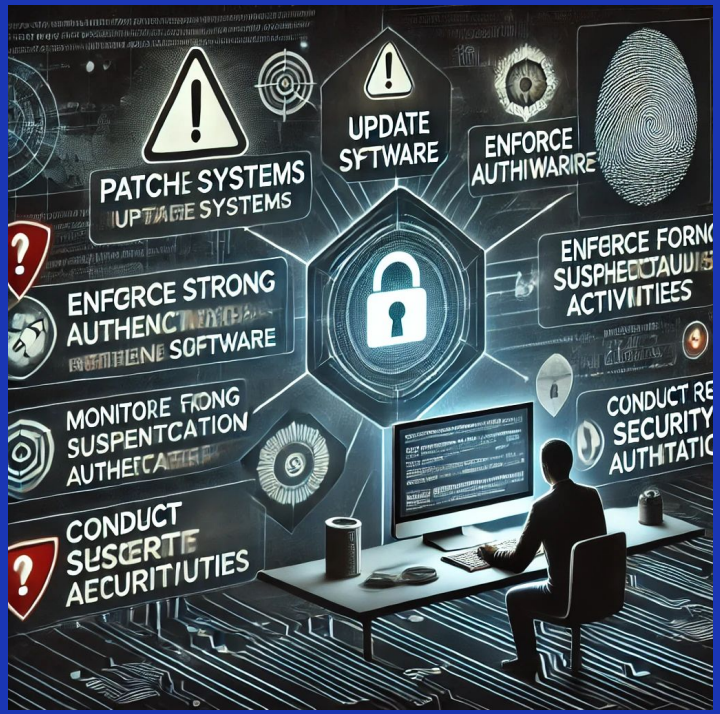


By: Isael Melendez

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.



Confidential

Copyright ©

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.

Confidential

Copyright ©

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.

Confidential

Copyright ©