International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Exploring Cyber Threats and Threat Actors in the Financial Sector: A Comprehensive Study

Srivastava Shivang[1], Chinnuswamy Tamizhselvan[2], Parameswaran Ganesan[3], Rengabashyam Asha[4]

[1,2,3,4]Graduate Student, Nanyang Technological University

Abstract:
This paper aims to discuss the recent activities of Financially motivated Threat actors and gather IOCs and Threat Intelligence based on the same. Common TTPs are mapped for 18 FIN threat actor groups along with known mitigations as per MITRE Attack Framework. In particular, FIN 7 is discussed in detail, including the lifecycle of Qakbot Malware and malwares are analyzed to gather IOCs using Static Analysis. Intrusion Detection Systems (Snort and YARA) are drafted for Qakbot. A comprehensive analysis on Diamond Model, Kill Chain and Pyramid of Pain is performed for Qakbot Malware and mitigations are mapped to MITRE ATTACK framework. Threat intelligence is gathered on the 1000 latest samples of Qakbot to deep dive into most commonly used delivery methods, malware file types and a timeline analysis is conducted. Advanced tools like OpenCTI and Cuckoo Sandbox are utilized to give an overall analysis on Financially motivated threat actors

1.0 Introduction

The financial sector is facing an ever evolving and complex threat landscape in the realm of cybersecurity. In recent years, there has been a rise in the frequency and sophistication of attacks on the financial and banking industry. The financial sector was the second most impacted sector based on the number of breaches last year.

According to the IBM cost of a data breach report 2023,

- The global average cost of a data breach in 2023 was $4.45 million, 15% more than in 2020.
- 51% of organizations are planning to increase security investments because of breach.
- The effect of extensive security AI and automation on the financial impact of a breach is USD1.76M

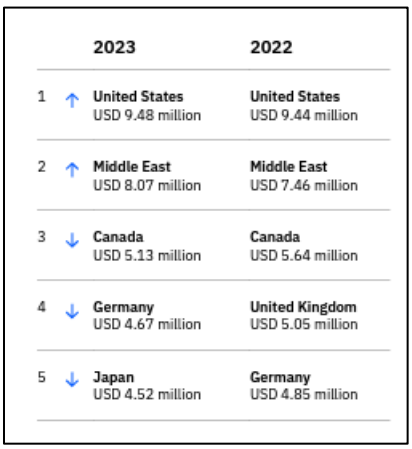


Figure 1: Data breach costs (Top five countries)

The selection of 17 industries has been included in the study for multiple years. Out of 17 industries, the financial industry suffers 14% of data breaches. Refer to the below diagram from the report.

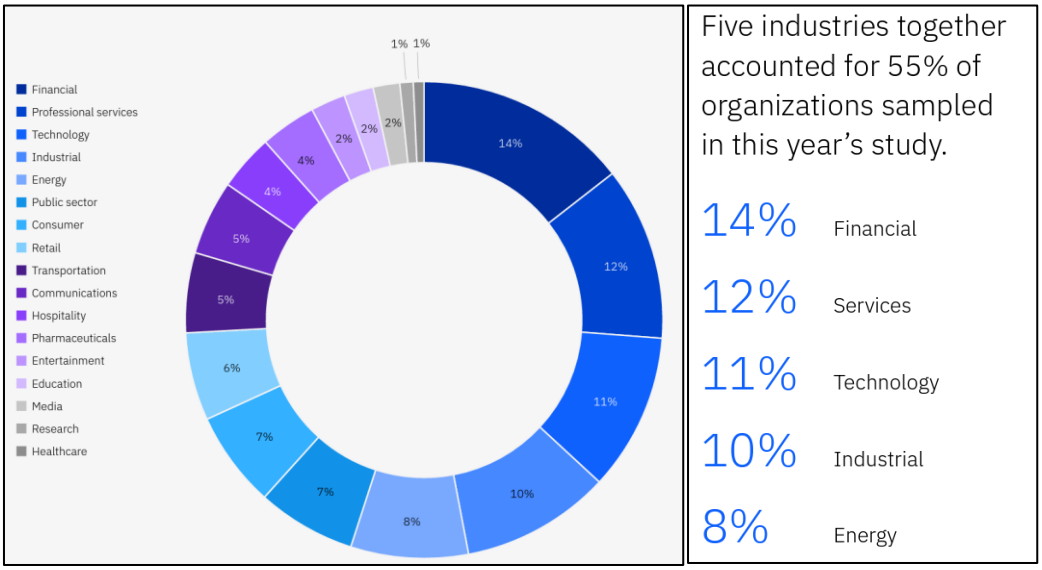


Figure 2: Distribution of the sample by Industry

More information on the data breaches in the year 2023 can be found in the IBM report. [1]

Risks faced by financial sector:

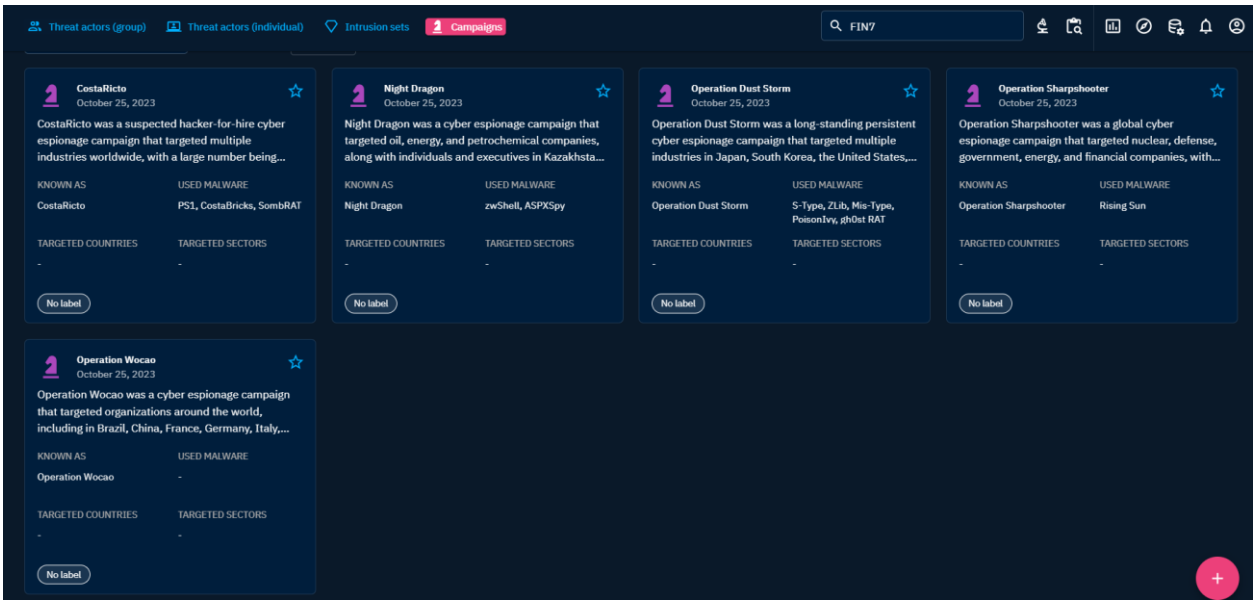
Based on the Cybersecurity and Financial system resilience report, Cybersecurity came up at the top of list as the potential risks and emerging threats that affects the U.S. economy. It was called out RaaS (Ransomware-as-a-Service) and sophisticated DDoS (Distributed-Denial-of-Service) attacks as the biggest risks to financial institutions ability to operate and safeguard customer data.

It was highlighted in the report,

"*The rising number of advanced persistent threats increases the potential for malicious cyber activity within the financial sector. These threats may result in incidents that affect one or more participants in the financial services sector simultaneously and have potentially systemic consequences. Such incidents could affect the ability of targeted firms to provide services and conduct business as usual, presenting a unique challenge to operational resilience. These incidents can also threaten the confidentiality, integrity, and availability of the targeted firm's data.*" [1]

Active Campaigns:

In line with the above reports, our research has identified a lot of active campaigns against financial institutions. The below snapshots show active campaigns.



Our Focus:

The financial sector the financial sector has witnessed a surge in cyber-attacks, necessitating a comprehensive analysis of the factors contributing to this trend. By examining the motivations of cybercriminals, the vulnerabilities inherent in the sector's digital transformation, and the sophisticated attack techniques employed, we can better comprehend the magnitude of the threats faced.

To highlight the significance of this research, we will explore recent high-profile attacks that have impacted the financial sector. These case studies will underscore the importance of proactive security measures and the potential consequences of failing to adequately protect financial institutions and their customers. Through this report, we aim to provide valuable insights into the evolving nature of cyber threats in the financial sector, emphasizing the importance of proactive cybersecurity measures such as threat monitoring and detection and fostering a collective effort to safeguard the integrity and stability of the financial ecosystem.

2.0 Our Research

2.1 APT groups

We have extensively looked at the Advanced Persistent Threats (APT) group which are motivated by financial gains, and we mapped the tactics and techniques of these groups in the MITRE ATT@CK framework.

No	Threat Group	Introduction
1	FIN 4	FIN4 is a financially motivated threat group that has targeted confidential information related to the public financial market, particularly regarding healthcare and pharmaceutical companies, since at least 2013. [2]
2	FIN 5	FIN5 is a financially motivated threat group that has targeted personally identifiable information and payment card information. The group has been active since at least 2008 and has targeted the restaurant, gaming, and hotel industries. [2]

No	Threat Group	Introduction
3	FIN 6	FIN6 is a cybercrime group that has stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors. [2]
4	FIN 7	FIN7 is a financially motivated threat group that has been active since 2013 primarily targeting the U.S. retail, restaurant, and hospitality sectors, often using point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. [2]
5	FIN 8	FIN8 is a financially motivated threat group known to launch tailored spear phishing campaigns targeting the retail, restaurant, and hospitality industries. [2]
6	FIN 10	FIN10 is a financially motivated threat group that has targeted organizations in North America from 2013 through 2016. The group uses stolen data exfiltrated from victims to extort organizations. [2]
7	CARBANK	Carbanak is a cybercriminal group that has used Carbanak malware to target financial institutions since at least 2013. Carbanak may be linked to groups tracked separately as Cobalt Group and FIN7 that have also used Carbanak malware. [2]
8	SILENCE	Silence is a financially motivated threat actor targeting financial institutions in different countries. The group was first seen in June 2016. Their main targets reside in Russia, Ukraine, Belarus, Azerbaijan, Poland, and Kazakhstan. [2]
9	COBALT	Cobalt Group is a financially motivated threat group that has primarily targeted financial institutions since at least 2016. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. Cobalt Group has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. [2]
10	APT38	APT38 is a North Korean state-sponsored threat group that specializes in financial cyber operations; it has been attributed to the Reconnaissance General Bureau. Active since at least 2014, APT38 has targeted banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs [2]
11	APT41	APT41 is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially motivated operations. Active since at least 2012, APT41 has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. [2]
12	BLACKTECH	BlackTech is a suspected Chinese cyber espionage group that has primarily targeted organizations in East Asia--particularly Taiwan, Japan, and Hong Kong--and the US since at least 2013. BlackTech has

No	Threat Group	Introduction
		used a combination of custom malware, dual-use tools, and living off the land tactics to compromise media, construction, engineering, electronics, and financial company networks. [2]
13	DARKVISHNYA	DarkVishnya is a financially motivated threat actor targeting financial institutions in Eastern Europe. In 2017-2018 the group attacked at least 8 banks in this region. [2]
14	EVILNUM	Evilnum is a financially motivated threat group that has been active since at least 2018 [2]
15	EXOTIC LILY	EXOTIC LILY is a financially motivated group that has been closely linked with Wizard Spider and the deployment of ransomware including Conti and Diavol. EXOTIC LILY may be acting as an initial access broker for other malicious actors and has targeted a wide range of industries including IT, cybersecurity, and healthcare since at least September 2021. [2]
16	GOLD SOUTHFIELD	GOLD SOUTHFIELD is a financially motivated threat group active since at least 2018 that operates the REvil Ransomware-as-a Service (RaaS). GOLD SOUTHFIELD provides backend infrastructure for affiliates recruited on underground forums to perpetrate high value deployments. [2]
17	TA551	TA551 is a financially motivated threat group that has been active since at least 2018. The group has primarily targeted English, German, Italian, and Japanese speakers through email-based malware distribution campaigns. [2]
18	WIZARD SPIDER	Wizard Spider is a Russia-based financially motivated threat group originally known for the creation and deployment of TrickBot since at least 2016. Wizard Spider possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals. [2]

Table 1: APT Groups (Financially Motivated)

The information on the Threat groups can be found in [2]

2.2 Heatmap

With many APT groups are financially motivated, we have researched on their Tactics, Techniques and Procedures (TTPs) of these groups mentioned in the *Table 1* and created heatmaps for TTPs used by these groups.

What is TTPs?

Based on NIST, Tactics, Techniques and Procedures (TTPs) means

> *"The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique."* [3]

2.2.1 MITRE ATT@CK Heatmap:

A MITRE ATT&CK heatmap is a visual representation that showcases the tactics, techniques, and procedures (TTPs) used by threat actors. It provides a structured way to understand and analyze cybersecurity threats and defenses by mapping observed behaviors. This heatmap can help organizations assess their security posture and develop strategies to defend against cyber threats. We have used python to generate the heatmap in Excel sheet. Below is the python script to generate the MITRE ATT@CK Heatmap.

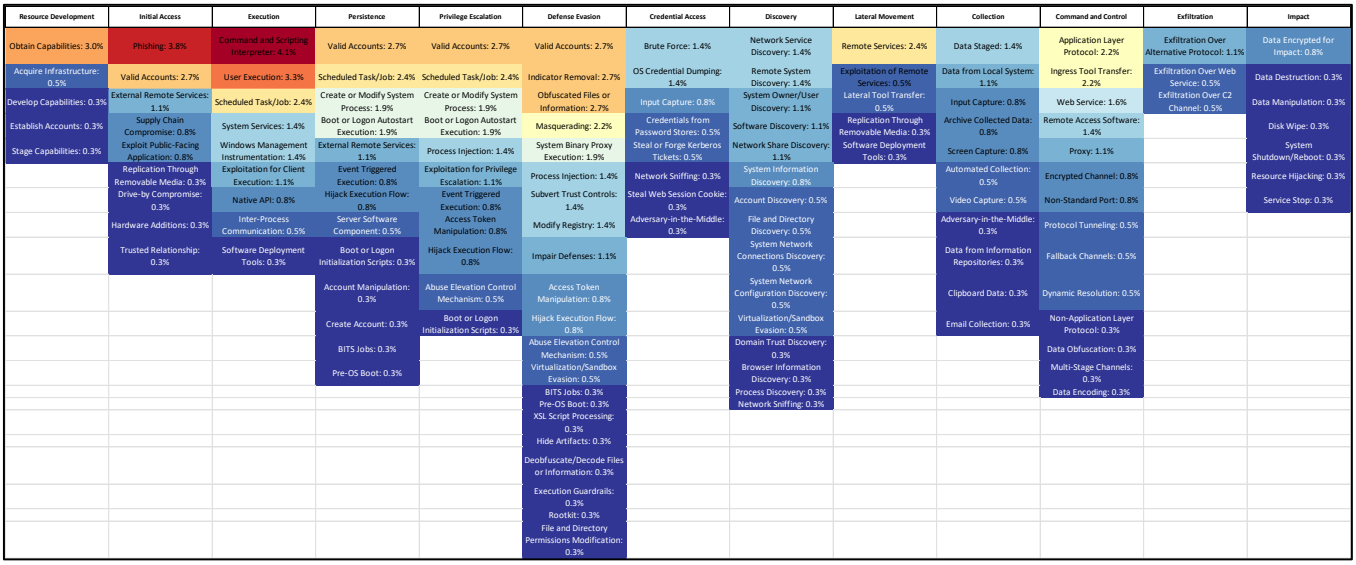
heatMap.py

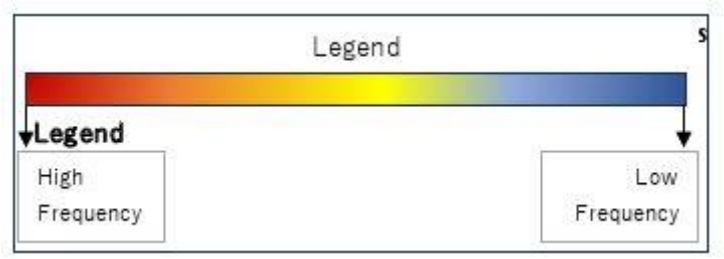
```python
import os
import json
import csv
from collections import Counter
import pandas as pd
import seaborn as sns
import matplotlib.pyplot as plt
# Get the current directory
current_directory = os.getcwd()

# List all files in the directory
file_names = os.listdir(current_directory)

# Filter only JSON files
json_files = [file for file in file_names if file.endswith('.json')]
appended_list = []

# Loop through each JSON file
for json_file in json_files:
    with open(os.path.join(current_directory, json_file), 'r') as file:
        data = json.load(file)
        techniques = data.get('techniques', [])
        appended_list.extend(techniques)

filtered_technique_ids = [entry['techniqueID'] for entry in appended_list if 'techniqueID' in entry and '.' not in entry['techniqueID']]

# Count the frequency of technique IDs
technique_id_counts = Counter(filtered_technique_ids)

# Sort the technique IDs by frequency in decreasing order
sorted_technique_ids = sorted(technique_id_counts.items(), key=lambda item: item[1], reverse=True)
```

```python
# Initialize a list to store the appended data
data = []

# Open the original CSV file
with open('t.csv', 'r') as file:
    reader = csv.reader(file)
    headers = next(reader)  # Get the headers
    data.append([headers[0], headers[1], headers[7]])  # Append headers for the selected columns

    for row in reader:
        data.append([row[0], row[1], row[7]])  # Append the required columns

# Save the appended data to a new CSV file
with open('appended_data.csv', 'w', newline='') as file:
    writer = csv.writer(file)
    writer.writerows(data)



# Save the data to a CSV file
with open('HeatMapData.csv', mode='w', newline='') as file:
    writer = csv.writer(file)
    writer.writerow(['Technique ID', 'Frequency', 'Technique','Tactic'])
    for technique_id, frequency in sorted_technique_ids:
        for total_data in data:
            #print(total_data[0])
            if(technique_id==total_data[0]):
                writer.writerow([technique_id, frequency,total_data[1],total_data[2]])

                print("SHI")

print("Data has been saved to HeatMapData.csv")




# Read the data from the CSV file
df = pd.read_csv('HeatMapData.csv')

# Filter the DataFrame to include only rows with frequency >= 2
df_filtered = df[df['Frequency'] >= 2]

# Pivot the filtered DataFrame to make Technique as subheaders of each Tactic
df_pivot = df_filtered.pivot_table(index='Tactic', columns='Technique', values='Frequency', fill_value=0)

# Create a heatmap
plt.figure(figsize=(12, 8))
sns.heatmap(df_pivot, annot=True, cmap='YlGnBu', fmt='g')
plt.title('Technique Frequency Heatmap (Frequency >= 2)')
plt.show()
```

Figure 3: Heatmap with Python Code

The figure presented below is the output generated by the Python script mentioned earlier. It represents a MITRE ATT&CK heatmap focusing on 18 distinct threat groups. In this heatmap, red signifies a high frequency of occurrence of tactics, techniques, and procedures (TTPs), while blue indicates a lower frequency. This visualization helps in quickly identifying the prevalence and distribution of TTPs among the different threat groups.





The visual representation in the figure below is a column heatmap that offers an organized view of tactics used in cyber threats. It arranges these tactics in descending order of frequency, with the most utilized tactics occupying the upper sections and the less frequently employed tactics located lower down in the heatmap. This arrangement provides a clear and intuitive way to understand the distribution and prevalence of tactics used by threat actors.

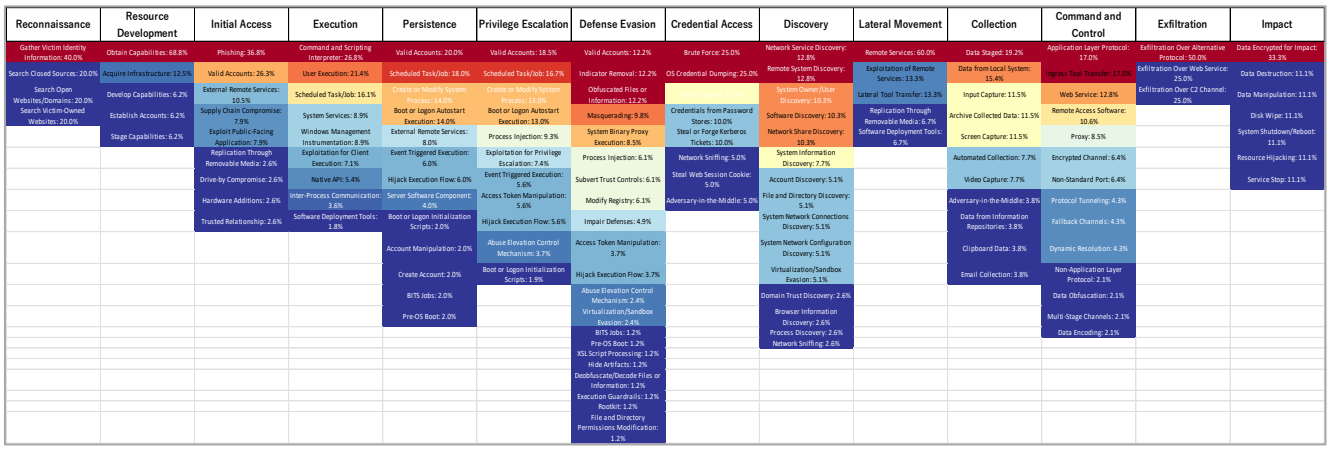


Figure 4: Column wise Heatmap (With Highest Priority)

Based on the MITRE ATT&CK heatmap analysis, we have identified the top 13 techniques that are frequently employed by FIN threat actors in various cyberattacks. These techniques represent the most common strategies and tactics used by malicious actors to compromise systems and networks, highlighting critical areas that organizations should focus on to enhance their cybersecurity defenses.

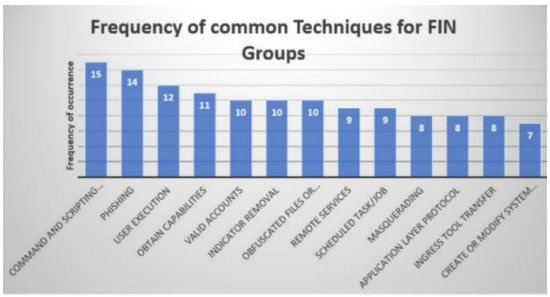


Figure 5: Top* techniques *used by* FIN *groups.

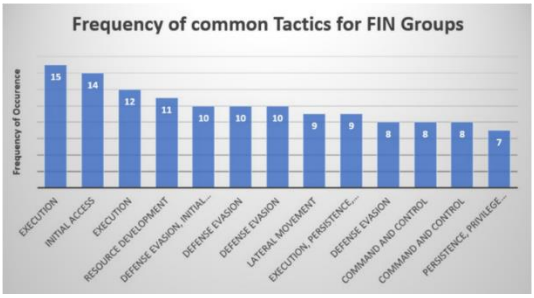


Figure 6: Top tactics used by* FIN *groups.

Our research into the threat actor utilizing these prominent techniques and tactics has led us to identify the threat group FIN 7. This specific threat group extensively employs 11 out of the top 14 tactics and techniques in their malicious activities. The following figure visually represents the mapping of these eleven techniques, showcasing their significance in the operational playbook of the FIN 7 group.

Technique ID	Frequency	Technique	Tactic	FIN7
T1059	15	Command and Scripting Interpret	Execution	Yes
T1566	14	Phishing	Initial Access	Yes
T1204	12	User Execution	Execution	Yes
T1588	11	Obtain Capabilities	Resource Development	No
T1078	10	Valid Accounts	Defense Evasion, Initial Access, Persistence, Privilege Escalation	Yes
T1070	10	Indicator Removal	Defense Evasion	No
T1027	10	Obfuscated Files or Information	Defense Evasion	Yes
T1021	9	Remote Services	Lateral Movement	Yes
T1053	9	Scheduled Task/Job	Execution, Persistence, Privilege Escalation	Yes
T1036	8	Masquerading	Defense Evasion	Yes
T1071	8	Application Layer Protocol	Command and Control	Yes
T1105	8	Ingress Tool Transfer	Command and Control	Yes
T1543	7	Create or Modify System Process	Persistence, Privilege Escalation	Yes

Figure 7: Top* techniques *used by* FIN *7

Based on the previously outlined rationale and findings, we have made the informed decision to prioritize the investigation and detailed analysis of the threat actor known as FIN 7. This selection is based on various factors, including their extensive use of the top tactics and techniques, making them a significant player in the cybersecurity threat landscape. Further research into FIN 7's tactics, strategies, and characteristics will provide valuable insights and contribute to a better understanding of their activities, ultimately enhancing our ability to defend against their threats.

3.0 FIN 7

FIN7 is a financially motivated threat group that has been active since 2013 primarily targeting the U.S. retail, restaurant, and hospitality sectors, often using point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. Since 2020 FIN7 shifted operations to a big game hunting (BGH) approach including use of REvil ransomware and their own Ransomware as a Service (RaaS), Darkside. FIN7 may be linked to the Carbanak Group, but there appears to be several groups using Carbanak malware and are therefore tracked separately.

3.1 Overview of FIN 7

FIN 7 group has been working since 2013. The below figure shows the FIN7 activities in the year 2020-2021. [4]

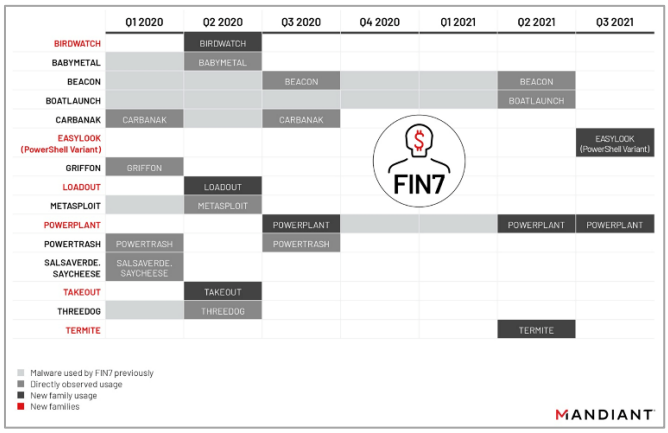


Figure 8: **FIN7 Activity in 2020-2021**

The distribution of relations for FIN 7 is shown in the below figure.

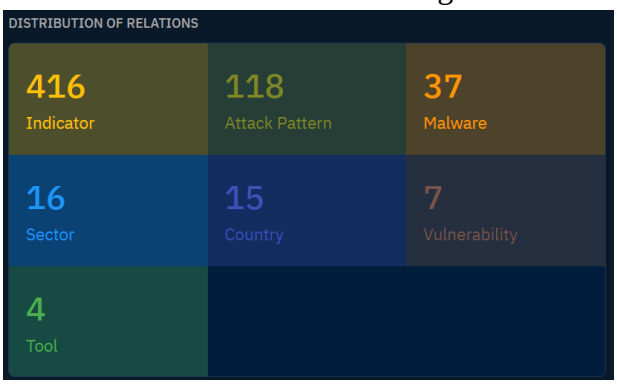


Figure 9: Distribution of Relations

3.2 Geo Victims and Target of FIN 7 team:

Based on the thehackernews. com [5] article published in the year 2022, An exhaustive analysis of FIN7 has unmasked the cybercrime syndicate's organizational hierarchy, alongside unraveling its role as an affiliate for mounting ransomware attacks. It has also exposed deeper associations between the group and the larger threat ecosystem comprising the now-defunct ransomware DarkSide, REvil, and LockBit families.

The highly active threat group, also known as Carbanak, is known for employing an extensive arsenal of tools and tactics to expand its "cybercrime horizons," including adding ransomware to its playbook and setting up fake security companies to lure researchers into conducting ransomware attacks under the guise of penetration testing.

More than 8,147 victims have been compromised by the financially motivated adversary across the world, with most of the entities located in the U.S. Other prominent countries include China, Germany, Canada, Italy, and the U.K. FIN7's intrusion techniques, over the years, have further diversified beyond traditional social engineering to include infected USB drives, software supply chain compromise, and the use of stolen credentials purchased from underground markets.

3.3 Tools and Malwares and Vulnerabilities used by FIN7:

FIN7 uses various tools such as Powersploit, Mimikalz, Crack MapExec are some of the tools mainly used by this group.

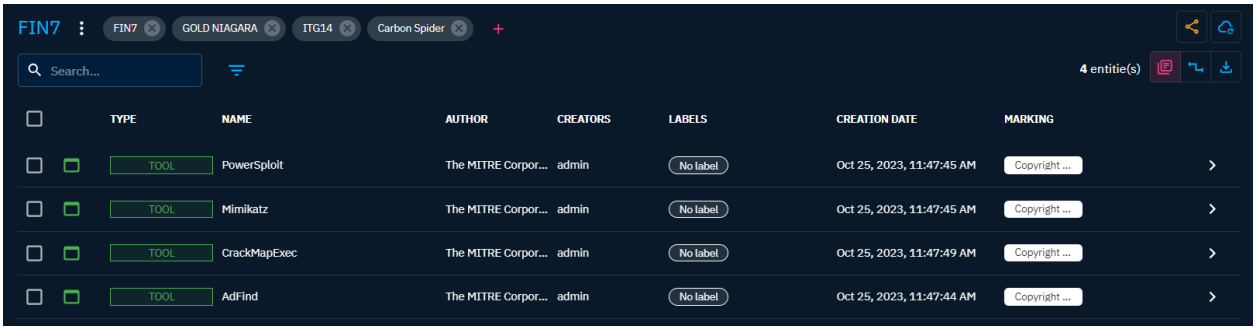
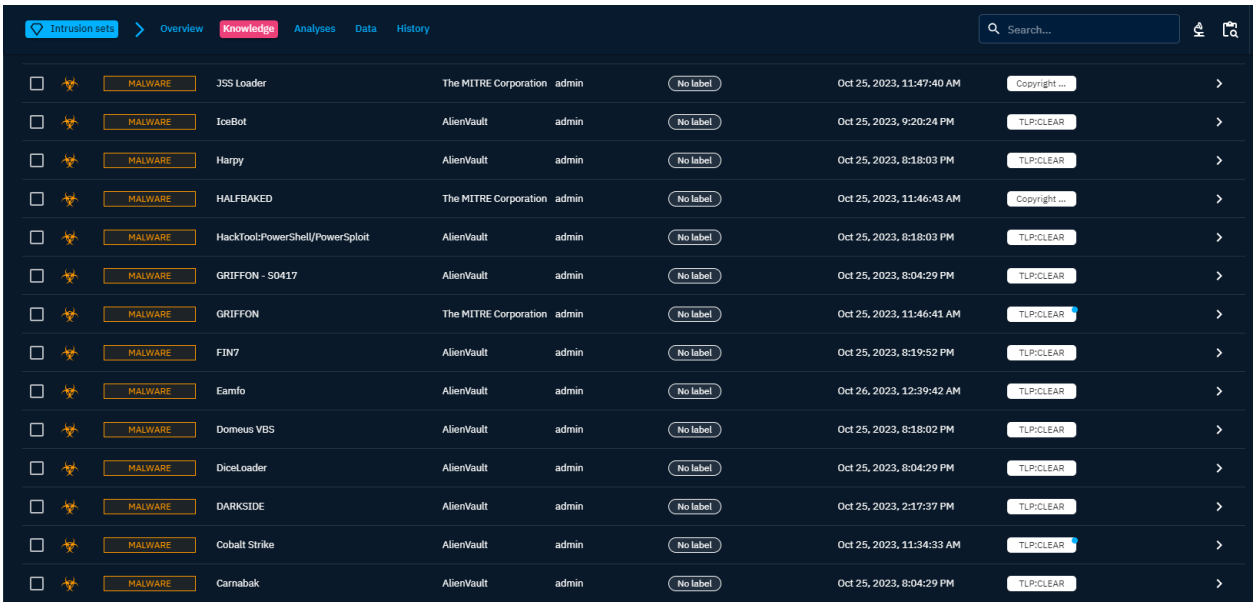
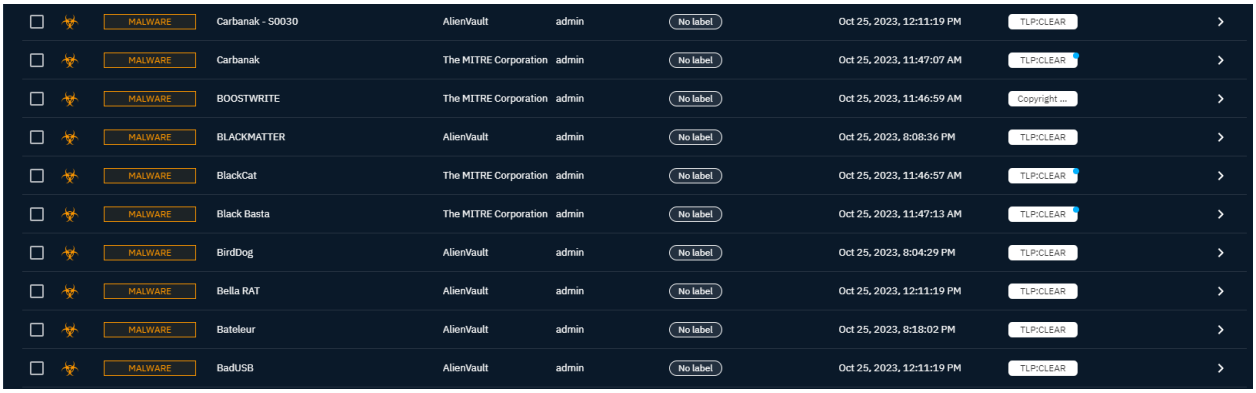
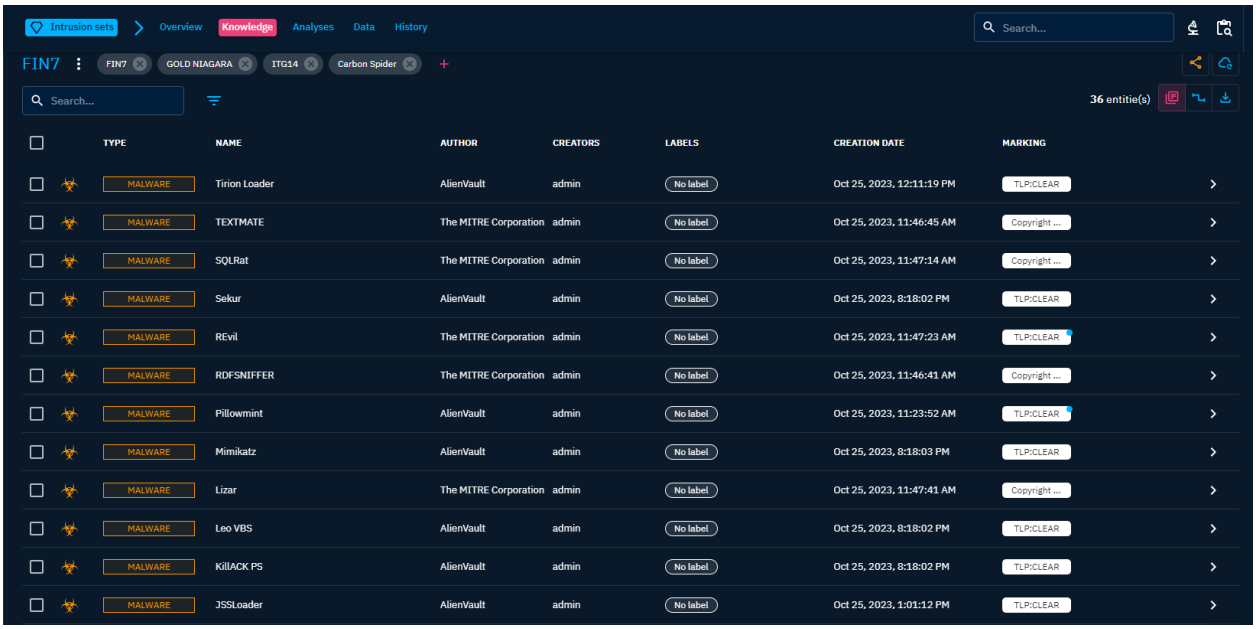


Figure 10: Tools used by FIN 7

Similarly, multiple malwares were used by this group are listed down in the below figure


Intrusion sets
Overview
Knowledge
Analyses
Data
History
Search...
MALWARE JSS Loader The MITRE Corporation admin No label Oct 25, 2023, 11:47:40 AM Copyright ...
MALWARE IceBot AlienVault admin No label Oct 25, 2023, 9:20:24 PM TLP:CLEAR
MALWARE Harpy AlienVault admin No label Oct 25, 2023, 8:18:03 PM TLP:CLEAR
MALWARE HALFBAKED The MITRE Corporation admin No label Oct 25, 2023, 11:46:43 AM Copyright ...
MALWARE HackTool:PowerShell/PowerSploit AlienVault admin No label Oct 25, 2023, 8:18:03 PM TLP:CLEAR
MALWARE GRIFFON - S0417 AlienVault admin No label Oct 25, 2023, 8:04:29 PM TLP:CLEAR
MALWARE GRIFFON The MITRE Corporation admin No label Oct 25, 2023, 11:46:41 AM TLP:CLEAR
MALWARE FIN7 AlienVault admin No label Oct 25, 2023, 8:19:52 PM TLP:CLEAR
MALWARE Eamfo AlienVault admin No label Oct 26, 2023, 12:39:42 AM TLP:CLEAR
MALWARE Domeus VBS AlienVault admin No label Oct 25, 2023, 8:18:02 PM TLP:CLEAR
MALWARE DiceLoader AlienVault admin No label Oct 25, 2023, 8:04:29 PM TLP:CLEAR
MALWARE DARKSIDE AlienVault admin No label Oct 25, 2023, 2:17:37 PM TLP:CLEAR
MALWARE Cobalt Strike AlienVault admin No label Oct 25, 2023, 11:34:33 AM TLP:CLEAR
MALWARE Carnabak AlienVault admin No label Oct 25, 2023, 8:04:29 PM TLP:CLEAR


MALWARE Carbanak - S0030 AlienVault admin No label Oct 25, 2023, 12:11:19 PM TLP:CLEAR
MALWARE Carbanak The MITRE Corporation admin No label Oct 25, 2023, 11:47:07 AM TLP:CLEAR
MALWARE BOOSTWRITE The MITRE Corporation admin No label Oct 25, 2023, 11:46:59 AM Copyright ...
MALWARE BLACKMATTER AlienVault admin No label Oct 25, 2023, 8:08:36 PM TLP:CLEAR
MALWARE BlackCat The MITRE Corporation admin No label Oct 25, 2023, 11:46:57 AM TLP:CLEAR
MALWARE Black Basta The MITRE Corporation admin No label Oct 25, 2023, 11:47:13 AM TLP:CLEAR
MALWARE BirdDog AlienVault admin No label Oct 25, 2023, 8:04:29 PM TLP:CLEAR
MALWARE Bella RAT AlienVault admin No label Oct 25, 2023, 12:11:19 PM TLP:CLEAR
MALWARE Bateleur AlienVault admin No label Oct 25, 2023, 8:18:02 PM TLP:CLEAR
MALWARE BadUSB AlienVault admin No label Oct 25, 2023, 12:11:19 PM TLP:CLEAR


Intrusion sets
Overview
Knowledge
Analyses
Data
History
Search...
FIN7
FIN7
GOLD NIAGARA
ITG14
Carbon Spider
Search...
36 entitie(s)
TYPE NAME AUTHOR CREATORS LABELS CREATION DATE MARKING
MALWARE Tirion Loader AlienVault admin No label Oct 25, 2023, 12:11:19 PM TLP:CLEAR
MALWARE TEXTMATE The MITRE Corporation admin No label Oct 25, 2023, 11:46:45 AM Copyright ...
MALWARE SQLRat The MITRE Corporation admin No label Oct 25, 2023, 11:47:14 AM Copyright ...
MALWARE Sekur AlienVault admin No label Oct 25, 2023, 8:18:02 PM TLP:CLEAR
MALWARE REvil The MITRE Corporation admin No label Oct 25, 2023, 11:47:23 AM TLP:CLEAR
MALWARE RDFSNIFFER The MITRE Corporation admin No label Oct 25, 2023, 11:46:41 AM Copyright ...
MALWARE Pillowmint AlienVault admin No label Oct 25, 2023, 11:23:52 AM TLP:CLEAR
MALWARE Mimikatz AlienVault admin No label Oct 25, 2023, 8:18:03 PM TLP:CLEAR
MALWARE Lizar The MITRE Corporation admin No label Oct 25, 2023, 11:47:41 AM Copyright ...
MALWARE Leo VBS AlienVault admin No label Oct 25, 2023, 8:18:02 PM TLP:CLEAR
MALWARE KillACK PS AlienVault admin No label Oct 25, 2023, 8:18:02 PM TLP:CLEAR
MALWARE JSSLoader AlienVault admin No label Oct 25, 2023, 1:01:12 PM TLP:CLEAR

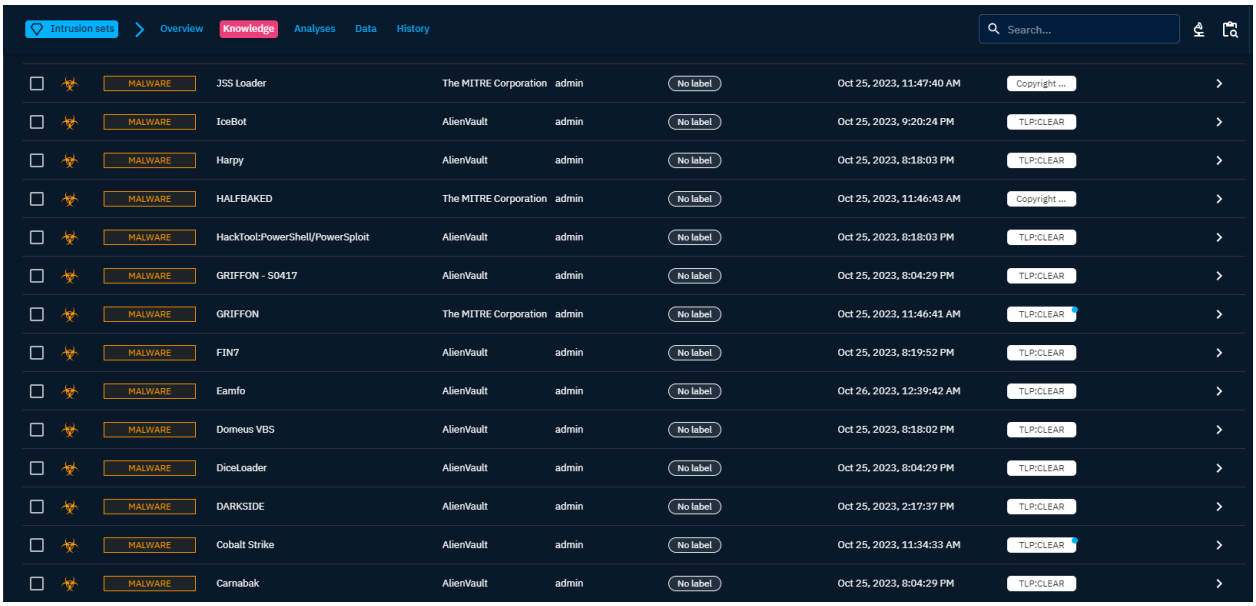


Figure 11: Malwares used by FIN 7

Some of the vulnerabilities used by this group FIN 7 are shown in the below figure.

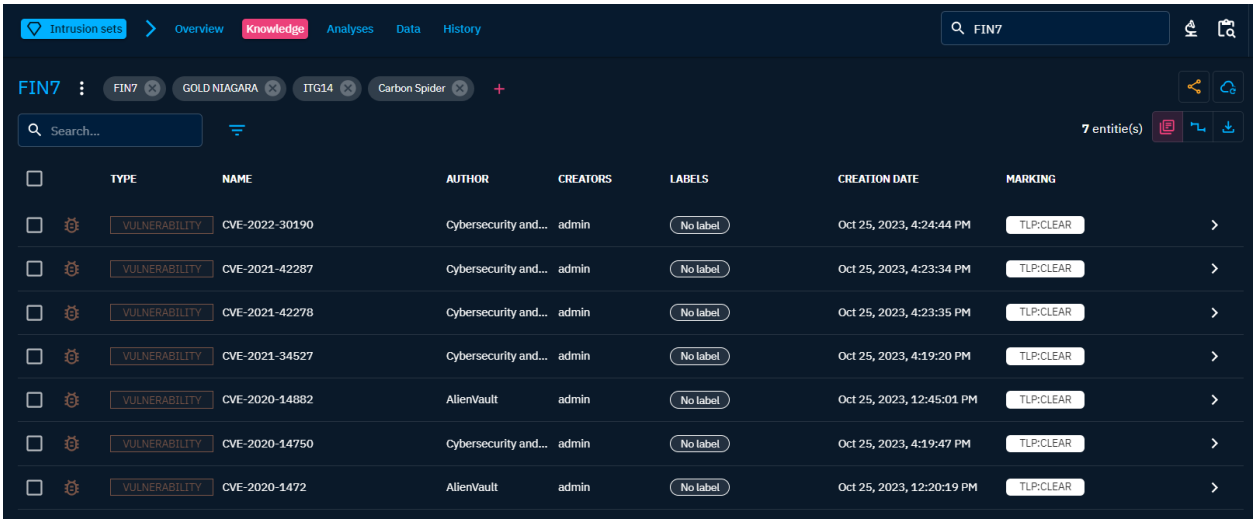


Figure 12: Vulnerabilities used by FIN 7

Some of the vulnerabilities used by the FIN 7 group are referenced in the below table.

CVE	Description
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190 [6]
CVE-2021-42278	Active Directory Domain Services Elevation of Privilege Vulnerability https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42278 [6]
CVE-2021-34527	Windows Print Spooler Remote Code Execution Vulnerability https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34527 [6]
CVE-2020-14882	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware. Easily exploitable vulnerability allows unauthenticated attacker

CVE	Description
	with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14882 [6]
CVE-2020-14750	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14750 [6]
CVE-2020-1472	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472 [6]

Table 2: CVEs used by FIN 7 group.

Based on the tactics, techniques and procedures used by this group FIN 7, we have identified some of the notable attacks carried out by FIN7 group. These attacks are sophisticated and far-reaching cyberattacks and are listed below.

Attack	Brief Description
Attack Disguised as Brown-Forman Inc.	In June 2021, FIN7 attacked a law firm with a fake complaint that appeared to belong to Brown-Forman Inc., a prominent American company in the wine and spirits industry known for Jack Daniels whisky. This deceptive complaint served as bait to trick a law firm into downloading a version of the JSSLoader Remote Access Trojan (RAT) that was hidden within an Excel file attachment.
Clever Phishing Lure in the Form of a Gift Card Exchange	In 2020, one of its attacks, FIN7 sent out physical letters purportedly from Best Buy, with a $50 gift card and a USB drive, claiming to contain a list of items to spend on. The USB was identified as a "BadUSB Leonardo USB ATMEGA32U4" device, programmed to emulate a USB keyboard, allowing it to automatically inject malicious commands once plugged in.
Exploiting Veeam Vulnerability	A recent report highlighted FIN7's targeting of Veeam servers. The group has been seen exploiting a vulnerability (CVE-2023-27532) in the Veeam Backup & Replication software. Using a PowerShell script, Powertrash, the group deployed a backdoor called Diceloader to perform various post-exploitation operations. The attacks involved the theft and exfiltration of credentials, network reconnaissance, and lateral movement within the compromised systems.

Table 3: FIN 7 Attacks

Other than the above known attacks, FIN7 (AKA Carbanak) threat actor is linked to Black Basta. Black Basta is a ransomware operator and Ransomware-as-a-Service (Raas) criminal enterprise that emerged in early 2022 and immediately became one of the most active RaaS threat actors in the world. This intrigued us and we wanted to explore the Black Basta, and we chose this as our incident for our research and started working on this incident.

4.0 Black Basta

4.1 Introduction on Black Basta

The Black Basta operator(s) use the double extortion technique, meaning that in addition to encrypting files on the systems of targeted organizations and demanding ransom to make decryption possible, they also maintain a dark web leak site where they threaten to post sensitive information if an organization chooses not to pay ransom.

Based on Unit 42 report, The ransomware is written in C++ and impacts both Windows and Linux operating systems. It encrypts users' data using a combination of ChaCha20 and RSA-4096, and to speed up the encryption process, the ransomware encrypts in chunks of 64 bytes, with 128 bytes of data remaining unencrypted between the encrypted regions. [7]

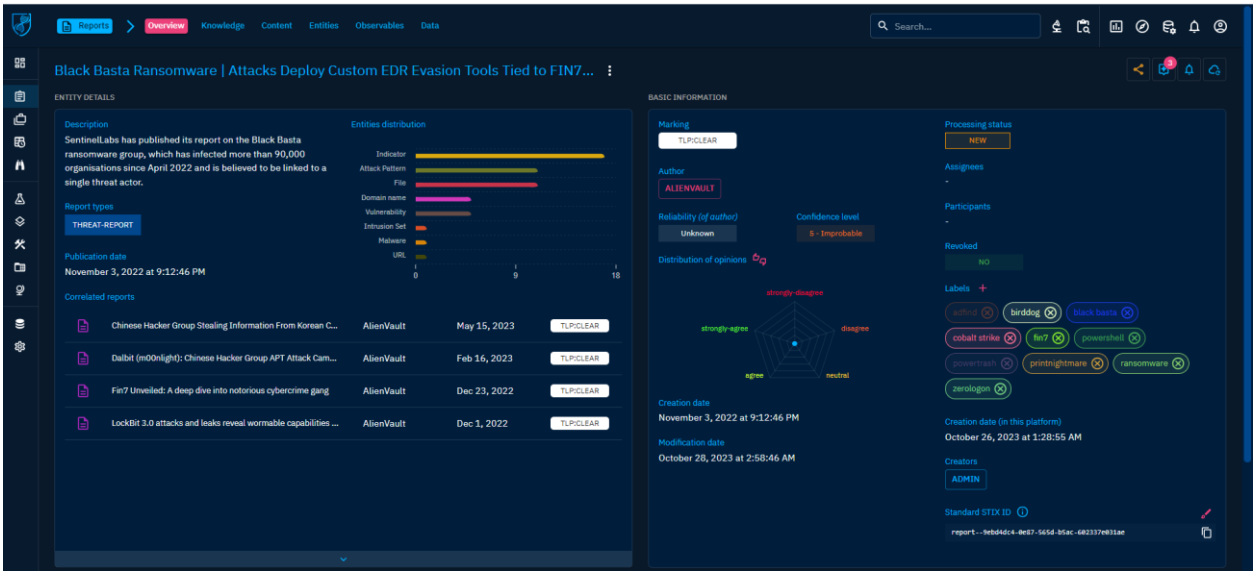


Figure 13: Black Basta Ransomware Info

The black basta ransomware using QBot as an initial point of entry and to move laterally in compromised networks. QBot, also known as Qakbot, is a Windows malware strain that started as a banking trojan and evolved into a malware dropper. Along with other researchers, we noted that Black Basta infections began with Qakbot delivered by email and macro-based MS Office documents, ISO+LNK droppers and .docx documents exploiting the MSDTC remote code execution vulnerability, CVE-2022-30190. The Black Basta group was observed using Qakbot for both initial access and to spread laterally throughout the network.

The sample of Black Basta file can be downloaded from MalwareBazaar. The link to download the sample is provided here Black Basta Malware Sample Download [8]. The Black Basta file information is as shown in the below figure:

File Information (time: 0:00:03.112371)

filename	723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224.exe
filetype	PE32 executable (GUI) Intel 80386, for MS Windows
filesize	1489920
hash sha256	723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224
virustotal	/
imagebase	0x400000
entrypoint	0x237d9
imphash	e7481059b799ac586859298d4788584d
datetime	2016-04-20 18:01:43
dll	False
directories	import, debug, tls, resources, relocations
sections	.rsrc, .text *, .rdata *, .data *, .reloc *
features	mutex, antidbg, packer, crypto

File		Import function	
UxTheme.dll	Library	SHLWAPI.dll	35
SHLWAPI.dll	Library	PSAPI.DLL	2
PSAPI.DLL	Library	USER32.dll	136
USER32.dll	Library	KERNEL32.dll	155
KERNEL32.dll	Library	GDI32.dll	10
GDI32.dll	Library	COMDLG32.dll	3
COMDLG32.dll	Library	ADVAPI32.dll	3
ADVAPI32.dll	Library	SHELL32.dll	18
SHELL32.dll	Library	ole32.dll	8
ole32.dll	Library	ntdll.dll	1
ntdll.dll	Library	COMCTL32.dll	8
COMCTL32.dll	Library		

Figure 14: Black Basta file information

There are many research conducted on the Black Basta, and the below figure shows Black Basta Attack Lifecycle as explained in Unit42 report.

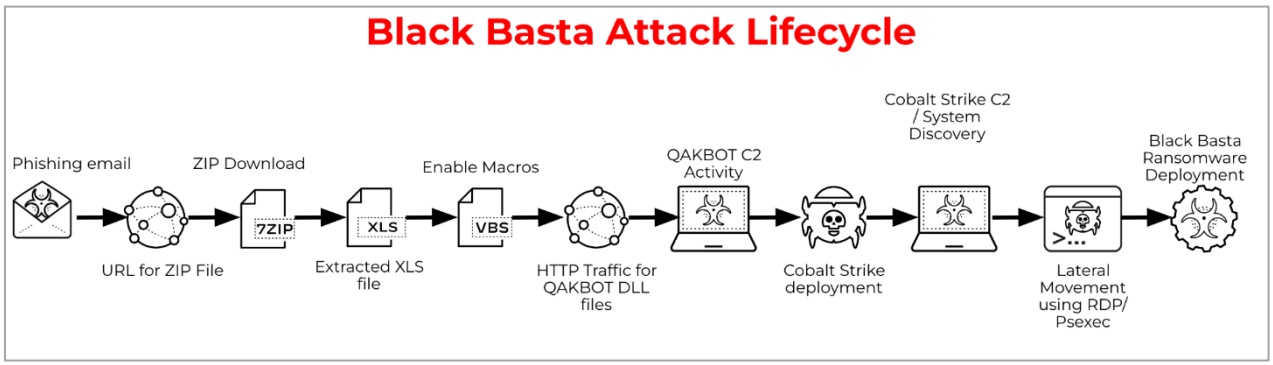


Figure 15: Black Basta Attack Lifecycle

4.2 Qakbot/QBot

QBot is a modular information stealer also known as Qakbot or Pinkslipbot. It has been active for years since 2007. It has historically been known as a banking Trojan, meaning that it steals financial data from infected systems, and a loader using C2 servers for payload targeting and download.

4.2.1 Reference

Qakbot/QBot reference available based on our research is from the year 2009 to the year 2023 (October). All along the Qakbot are used various attacks to deliver payloads, connect to C2 servers and in some cases, it helped lateral movement as well. The consolidated reference can be found in the https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot [9]

4.2.2 Qakbot Malware sample

Qakbot/QBot malware sample can be downloaded from the following link.
https://bazaar.abuse.ch/sample/3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa/ [10]

The malware sample is a .zip folder which contains an “Adobe Acrobat Document”. The below figure shows the snapshot of the .pdf file.

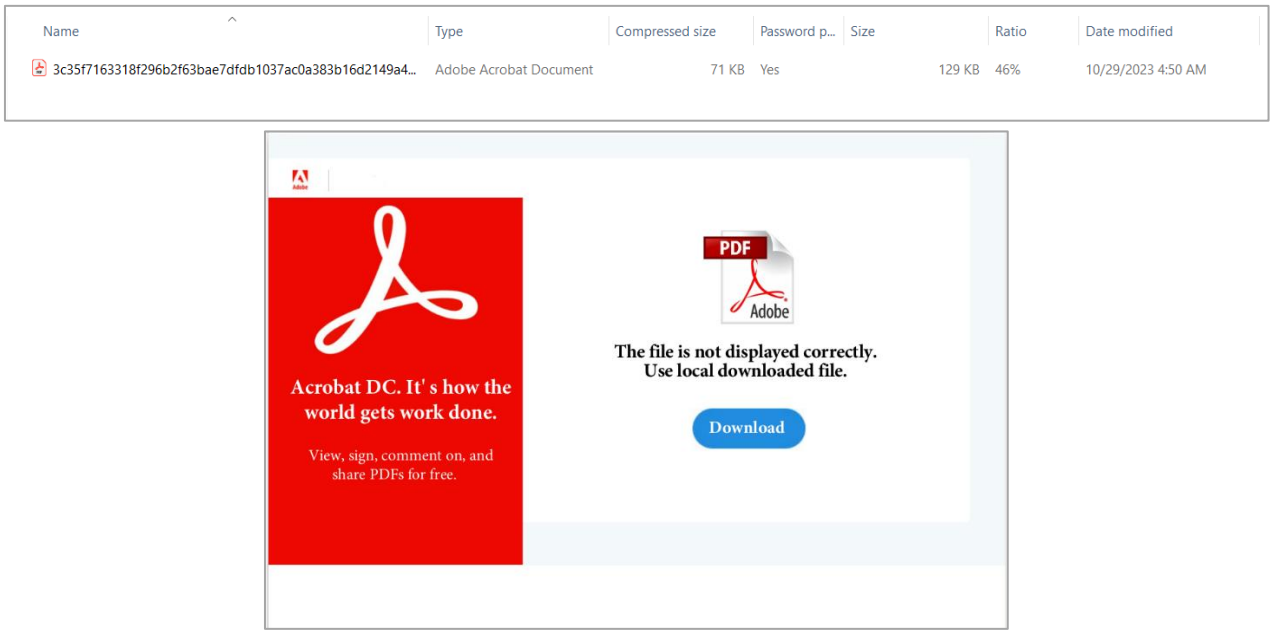


Figure 16: Qakbot Malware Sample

4.2.3 Qakbot/QBot Infection chain

QBot's infection chain is described in the following flow-chart.

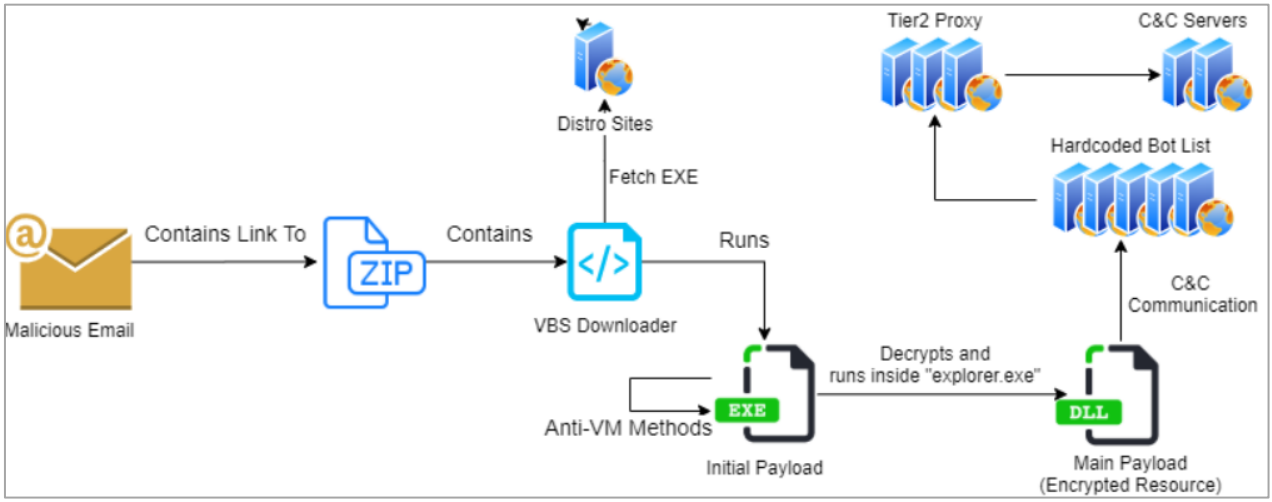


Figure 17: Qakbot infection chain

4.2.4 Qakbot/QBot Initial Access

The initial infection chain starts by sending specially crafted emails to the target organizations. The method is less sophisticated than spear-phishing techniques but has additional attributes which add to its credibility. One of these is called "Hijacked Email Threads" – capturing archived email conversations and replying to the sender with the malicious content. Those conversations could be captured using Qbot's Email Collector module. Some examples of crafted phishing emails are as shown below.

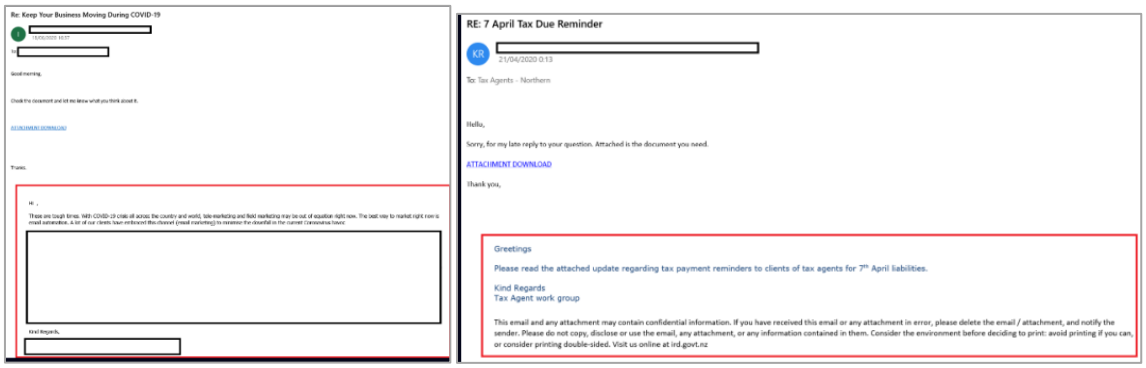


Figure 18: Qakbot Initial Access – Phishing emails.

4.2.5 Qakbot/QBot Analysis

We have used remnux tool to start the analysis of the downloaded Qakbot malware sample (*.pdf) file. Below is the step-by-step analysis we have conducted on the .pdf file.

1. To understand the sample PDF related information's, we have used "pdfid.py" tool. The below snapshot shows the command executed and information gathered from the pdf file.

```
remnux@remnux:~/Downloads$ ls
3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa.pdf
3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa.zip
7z2301-x64.exe
malware_samples
malware_samples.zip
Unit42-Wireshark-tutorials-main
Unit42-Wireshark-tutorials-main.zip
remnux@remnux:~/Downloads$ pdfid.py 3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa.pdf
PDFiD 0.2.8 3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa.pdf
 PDF Header: %PDF-1.4
 obj                    90
 endobj                 90
 stream                 35
 endstream              35
 xref                    1
 trailer                 1
 startxref               1
 /Page                   9
 /Encrypt                0
 /ObjStm                 0
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             0
 /AcroForm               0
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /URI                    2
 /Colors > 2^24          0
```

Figure 19: pfdid.py information

2. We found there are "/URI" in the pdf and we used "strings" command to see the URI embedded in the pdf file. Below snapshot shows the command executed and found the URI path https://ourloverlyday.us/xuenxavleu/xuenxavleu.gif

```
remnux@remnux:~/Downloads$ strings 3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa.pdf
%PDF-1.4
<</S/URI/URI(https://ourlovelyday.us/xuenxavleu/xuenxavleu.gif)>>
3 0 obj
<</A 4 0 R/BS<</S/S/Type/Border/W 0>>/Border[0 0 0]/C[1.0 1.0 1.0]/H/N/Rect[421.013 178.676 671.064 307.214]/Subtype/Link/Type/Annot>>
endobj
2 0 obj
[3 0 R]
endobj
5 0 obj
<</Filter/FlateDecode/Length 930>>stream
,v??
4=j;
,1e{H
q>B9
```

```
remnux@remnux:~/Downloads$ pdf-parser.py --search uri 3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa.pdf
obj 4 0
 Type:
 Referencing:

  <<
    /S /URI
    /URI (https://ourlovelyday.us/xuenxavleu/xuenxavleu.gif)
  >>


remnux@remnux:~/Downloads$
```

Figure 20: Qakbot URL from PDF.

3. We have done analysis on the identified URL through https://urlhaus.abuse.ch/url/2669875/. [11]. Below snapshot shows the information gathered from the above link

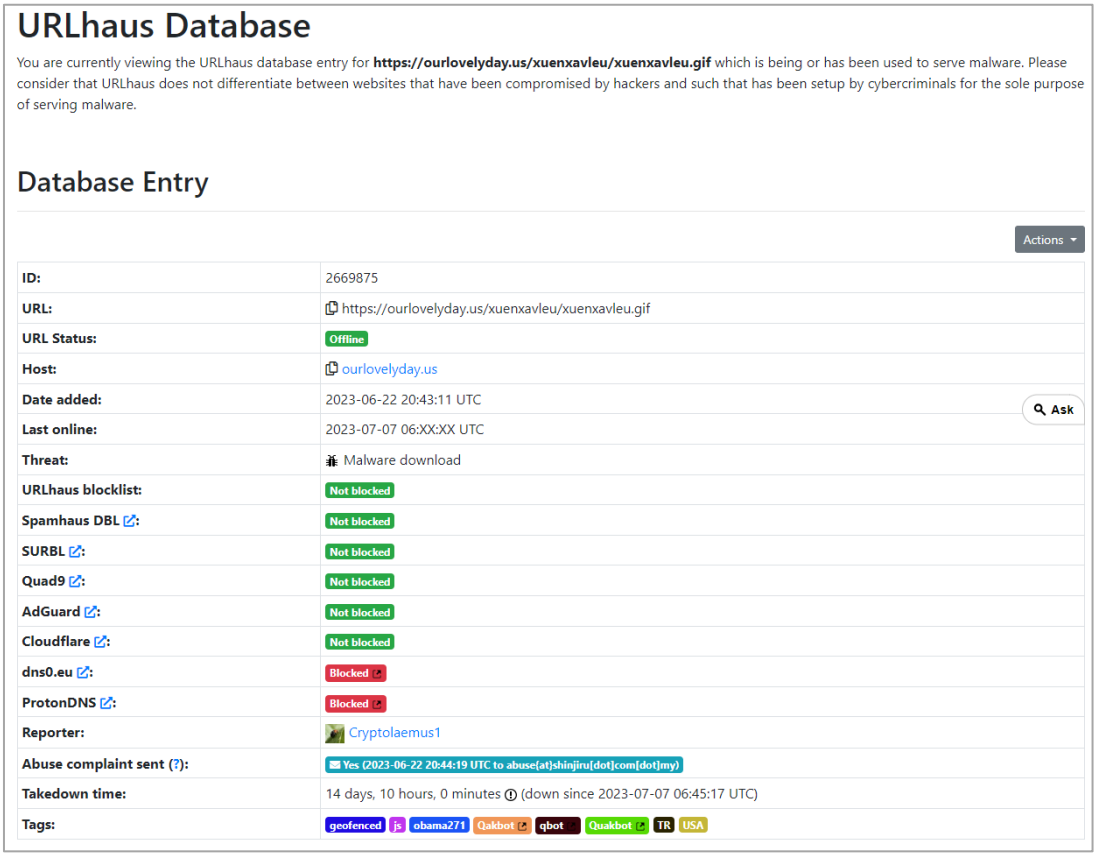


Figure 21: Qakbot Information based on URL.

From the above figure, we can understand, this PDF is related to Qakbot/QBot related and host is "Online" until 07th July 2023. Also, it was identified that the URL is used for Malware download as well. The related payloads associated with this URL are also available in the location. The below figure shows the information of payloads associated with this URL.

Payload delivery

The table below documents all payloads that URLhaus retrieved from this particular URL.

Firstseen	Filename	File Type	Payload (SHA256)	VT	Bazaar	Signature
2023-07-06	BSN-934795990.zip	zip	ad2cb77b1cd7dad4c151f3514a808b31f57caef96a7253089e3e2f96590847cc	n/a		Quakbot
2023-07-06	BSN-1525063912.zip	zip	749699a9a6198e917dd0b9dbb3769324cffe1f7bb570a8540c06b229ec0909c6	28.33%		Quakbot
2023-07-05	BSN-648582479.zip	zip	0d24ce0a34460f5a2ef82eeec406ee7defceb35a0aabc01ca5a24e8a09cfd967	n/a		Quakbot
2023-07-05	BSN-501648987.zip	zip	5e8e7b6687497d6f8aa278bfef0f825927759060d6955f0496be228a7f944a26	n/a		Quakbot
2023-07-04	BSN-1646570560.zip	zip	32542ff40271e16e3fee7b484bab79f13759aa0e0b73fb06286c76ccfcec4e53	n/a		Quakbot
2023-07-04	BSN-388349023.zip	zip	d5cb0c5110b5d15b4e70a494268a468f739767f250b41846e31593285b4e7e6c	n/a		Quakbot
2023-07-03	BSN-885602820.zip	zip	3b9029f13d804539bc6c9074c6356efe9285577811d1b35e99874b12fd727efe	n/a		Quakbot
2023-07-03	BSN-1609781407.zip	zip	897e6afd069d468269a4c493952e2b414cd83d49712c1f928fb18bbb91ceca9d	n/a		Quakbot
2023-07-02	BSN-1701353900.zip	zip	9303ead5e015215f7bb5bbd62595e9aa926f3f79763613ac9397afde05dad3af	n/a		Quakbot
2023-07-02	BSN-767584426.zip	zip	9377387fa10ba478568eb091ca5cf7007ac07af17b0820061b79963bfa1ddb14	n/a		Quakbot
2023-07-01	BSN-21000639.zip	zip	d51cec9cf3e00f2a38dc7f3a7afe7b75aeaaadb76498ab6b2b90cf6b8a0bf26e	n/a		Quakbot
2023-07-01	BSN-1624316576.zip	zip	2733aa9575463971d80efeb74d101eefbfa42e601f4d4e8b828f2d19f0593903	25.81%		Quakbot
2023-06-30	BSN-346589395.zip	zip	df24c34de63f32f2de58eec0712aae10a0a05eb392ba334e4c36ab1811aa07af	n/a		Quakbot
2023-06-30	BSN-2095055196.zip	zip	96eae5116f28ada38fc9796683c0a3761ac11007850e257121d8a7e4a4bb7e5c	n/a		Quakbot
2023-06-29	BSN-360970421.zip	zip	324ecc452159dc7251b19ef7bbd02d1b0113334b004d5894621877757570e6e5	n/a		Quakbot
2023-06-29	BSN-1078355438.zip	zip	d826265925f1704175d602a2315f0b862ebff91b8fa416da05447326ebde83d6	n/a		Quakbot
2023-06-28	BSN-659637643.zip	zip	e7cf94c3f525b788bb52722aa6f61767cdbd1ec6b44a8ae7a1fb5956f4bdd488	n/a		Quakbot
2023-06-28	BSN-989333913.zip	zip	d6b059997486a426cce9cf8dcb366a95770d48d1d1d4c163129a05fa722e8264	n/a		
2023-06-27	BSN-476442748.zip	zip	d8c2a47f3a6a5fdb853d01862fc40fa8a9adf5a750ffb31aca0d6db6891a8e43	n/a		Quakbot
2023-06-26	BSN-1010883072.zip	zip	fed906e95625c311117bd5258ebc9669a85ba2b7830e2d69a1b38d2ce6a62d16	n/a		Quakbot
2023-06-26	BSN-1445863482.zip	zip	f469f796392ba10987bb447c6a249bf9b395849ee82f5248e5448fcef3f4f065	n/a		Quakbot
2023-06-25	BSN-964842713.zip	zip	5b35ec8c3277149d86353a3407414ec33d715d9a18881a5838011b1f913d3cf4	8.06%		Quakbot
2023-06-25	BSN-1403099197.zip	zip	4832606a5235277811f9243f036885c41825a0f74309c249a664f3a7cdf6b8e2	n/a		Quakbot
2023-06-24	BSN-100766691.zip	zip	ea70bb3993e40bd39029f71440b3ecfc251f6313579f0a8dec608bac8fdf48b5	n/a		Quakbot
2023-06-24	BSN-2107257244.zip	zip	91973073c084e89b8aa29a941ceac6862d67807deacf28b88f33a195065ac383	n/a		Quakbot
2023-06-23	BSN-39797926.zip	zip	be4fcaf606d0ba10b0c03e0a79d22e624eca1f0958eba5d7060c07a657312061	n/a		Quakbot
2023-06-23	BSN-1841259078.zip	zip	b4a0534e0a42375e79ccbb498a0bde268be57940c9bf8d33a99407e18cadb02f	n/a		Quakbot
2023-06-22	BSN-2019472077.zip	zip	d88c59f211f2dd86edbcef5bbc53e683841d87a9239ab95357f63f77a66021c0	n/a		Quakbot
2023-06-22	BSN-1834448915.zip	zip	89e81455c7ec32a9944763fadbc41f8f3ef401f58ceee1677f313ec2279f6ee9	n/a		Quakbot

Figure 22: Qakbot/Qbot - Payloads associated with the URL.

4.2.6 Qakbot Execution:

After the initial analysis, we start exploring the PDF file and how QBot is executing in our test environment. Below are the steps we have identified during our analysis.

1. html drops .zip via html smuggling.
2. zip contains iso file.
3. iso contains .lnk.
4. Lnk file launches calc.exe,
5. calc.exe sideloads windowscodecs.dll
6. windowscodecs.dll executes the malicious payload dll (102755.dll).

Stage 1: Analysis of HTML

1. We downloaded the malware sample file earlier, which contains HTML page. We have analyzed the HTML page and found the variable as shown in the below figure.

Figure 23: Stage 1- HTML File Analysis

2. Based on ChatGPT query [12], we understood the variable started with the text "UEsDB". This is a common starting sequence in the Base64 representation of a ZIP file. Below is the information gathered from ChatGPT.
   - A ZIP file typically starts with a specific byte sequence known as a "magic number" that helps identify it. The magic number for a ZIP file is "PK" (0x50 0x4B in hexadecimal). The base64 representation of these bytes is "UEsD" in ASCII.
   - If you have a ZIP file and you want to encode the starting sequence "PK" in base64, you can do so by encoding these bytes as follows:
     - Convert "PK" to its hexadecimal representation: 0x50 0x4B.
     - Encode these bytes in base64: "UEs="
   - "UEs=" is the base64 encoding of the ZIP file starting sequence "PK." Please note that this base64 encoding only represents the initial bytes of the ZIP file and not the entire file.
3. We downloaded the ZIP file from the from the text by decoding Base64 to file. Refer the below snapshot on how to download the ZIP file from the HTML page variable.

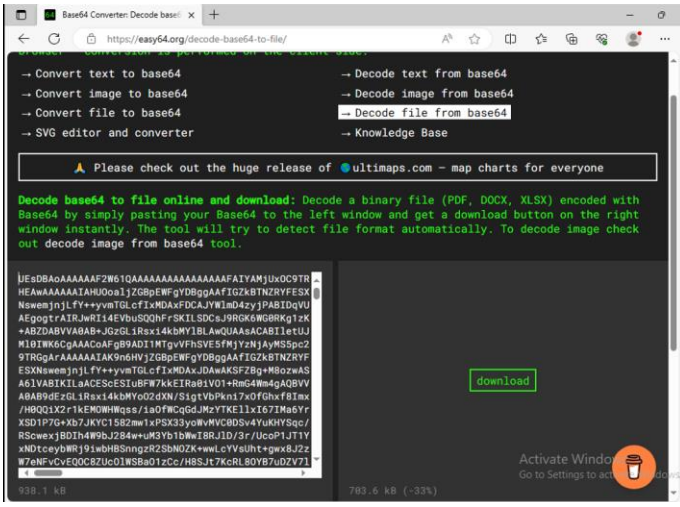


Figure 24: Stage 1- Download ZIP file

4. When we tried to extract the zip file, it required the password. We were able to find the password in the HTML page. Refer the below figure for extracted password.

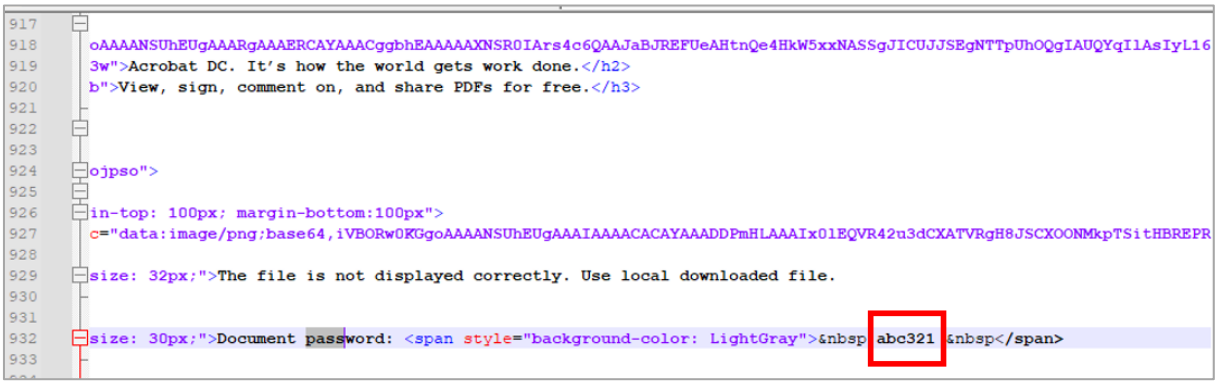


Figure 25: Stage 1- Identifying the Password

Stage 2: ZIP contains iso file.

1. We were able to extract the content from zip file, using the identified password (abc321). Refer the below figure.

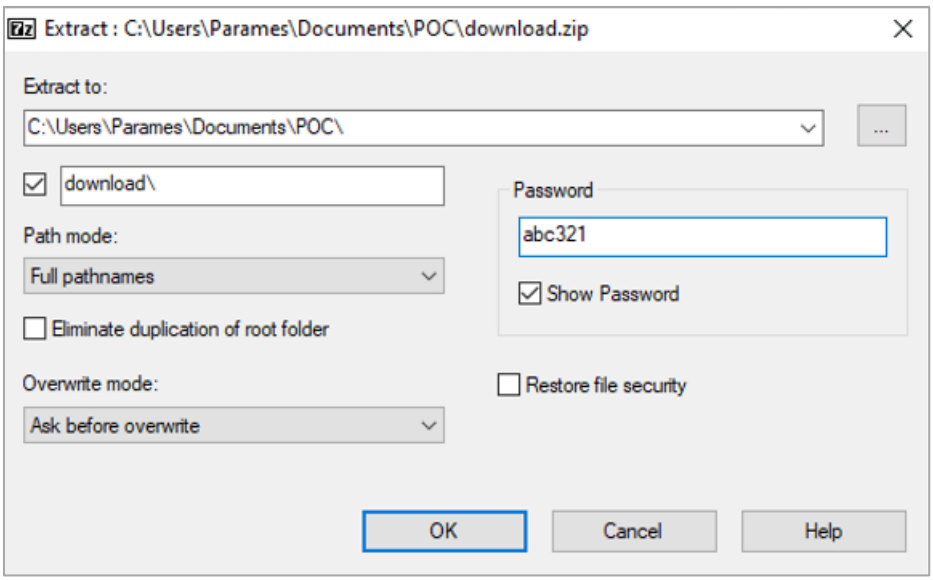


Figure 26: Stage 2- Extracting the files from the ZIP folder.

2. After extracting the ZIP file, we can extract the files using 7z using the following commands. The below figure shows the extraction of files from the ISO file.

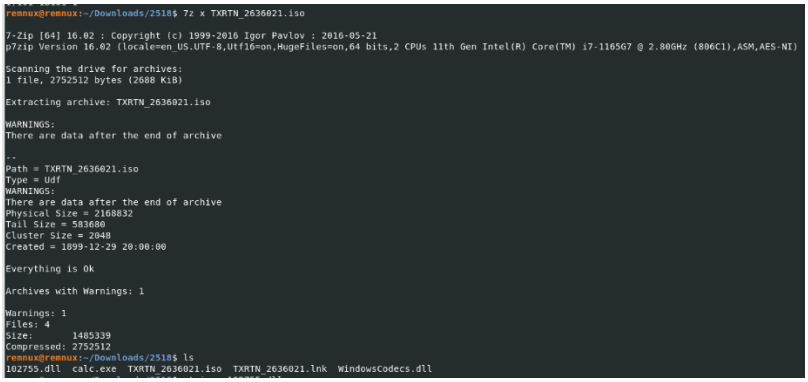


Figure 27: Stage 2- Extracting the files from the ISO.

Stage 3: ISO contains .lnk

1. As you can see, the extracted folder has multiple files such as calc.exe, dll files, Lnk files. The below figure shows the extracted files.

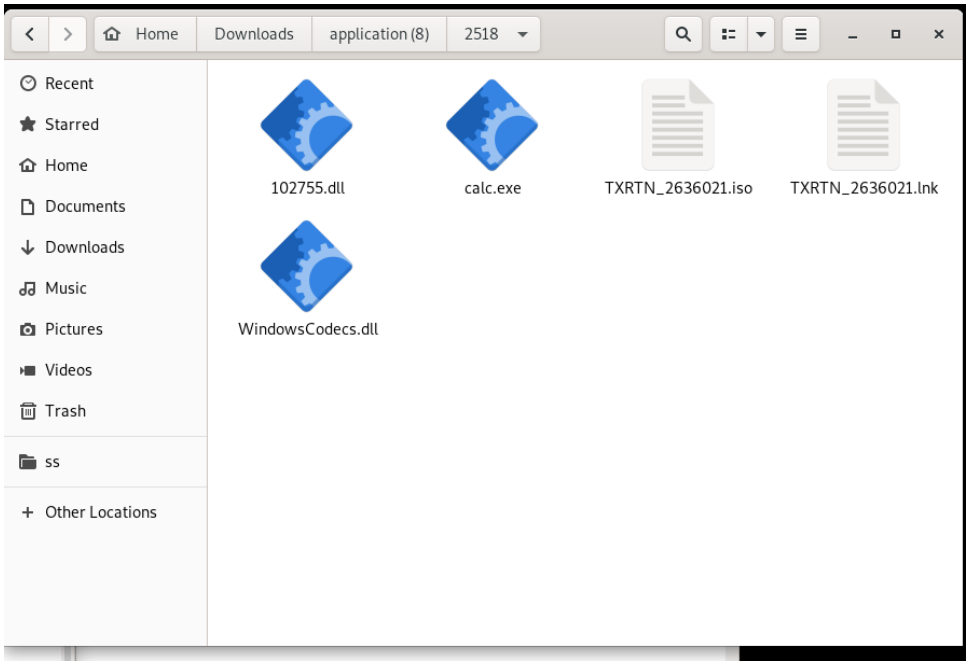


Figure 28: Stage 3- Extracted files from the ISO.

```
Metadata
-------------------------------------------------------------------------------
CompanyName       Microsoft Corporation
FileDescription   Windows Calculator
FileVersion       6.1.7601.17514 (win7sp1_rtm.101119-1850)
InternalName      CALC
LegalCopyright    © Microsoft Corporation. All rights reserved.
OriginalFilename  CALC.EXE
ProductName       Microsoft® Windows® Operating System
ProductVersion    6.1.7601.17514
```

```
File
-------------------------------------------------------------------------------
SHELL32.dll       Library
SHLWAPI.dll       Library
gdiplus.dll       Library
ADVAPI32.dll      Library
ntdll.DLL         Library
OLEAUT32.dll      Library
UxTheme.dll       Library
ole32.dll         Library
COMCTL32.dll      Library
KERNEL32.dll      Library
USER32.dll        Library
RPCRT4.dll        Library
WINMM.dll         Library
VERSION.dll       Library
GDI32.dll         Library
msvcrt.dll        Library
WindowsCodecs.dll Library
```

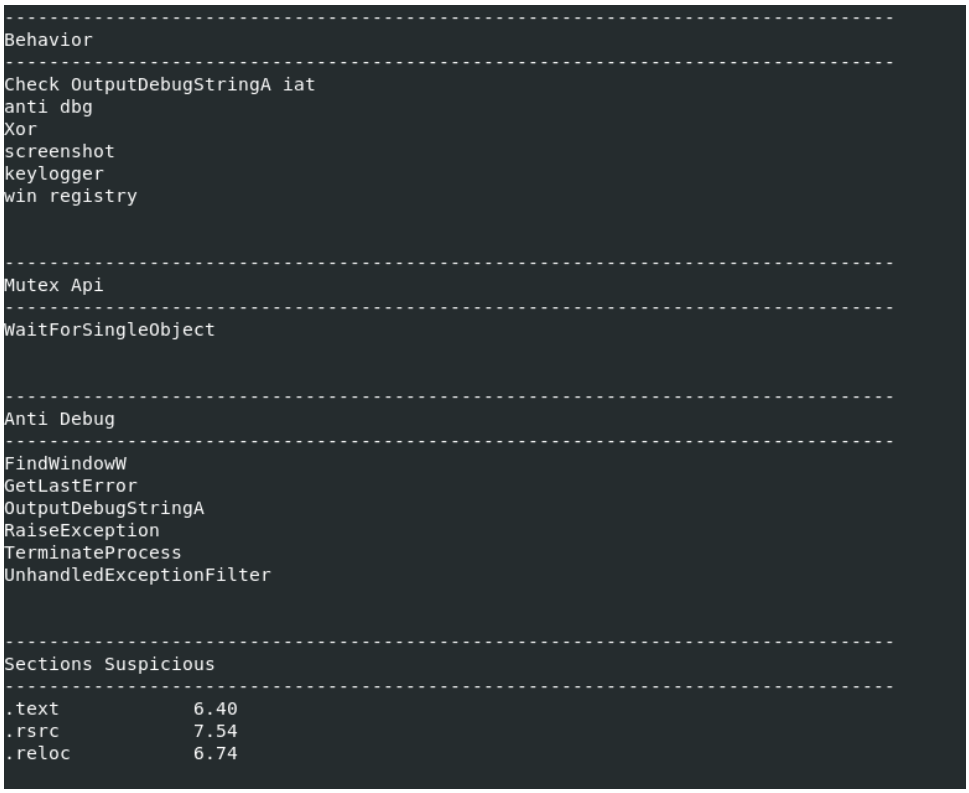


Figure 29: Stage 3- Analysis of files.

Stage 4: .lnk files executes calc.exe.

1. When we analyzed the file "Txrtn_2636021.lnk", we identified the "calc.exe" is being executed in the behind. Refer the below figure for analysis of .lnk file.

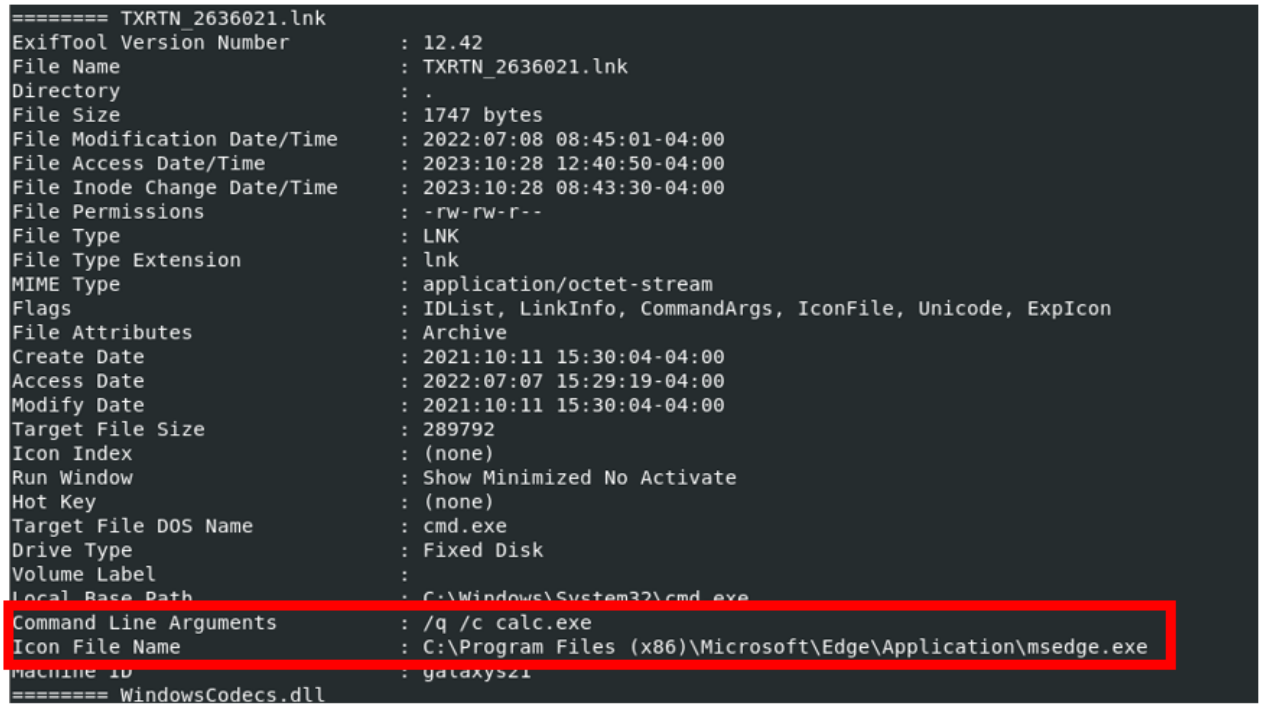


Figure 30: Stage 4- Analysis of Txrtn_2636021.lnk.

Stage 5: calc.exe sideloads windowscodecs.dll

1. When the calc.exe is executed, the windowscodecs.dll file as well. Refer the below figure how the process is executed in the process monitor.

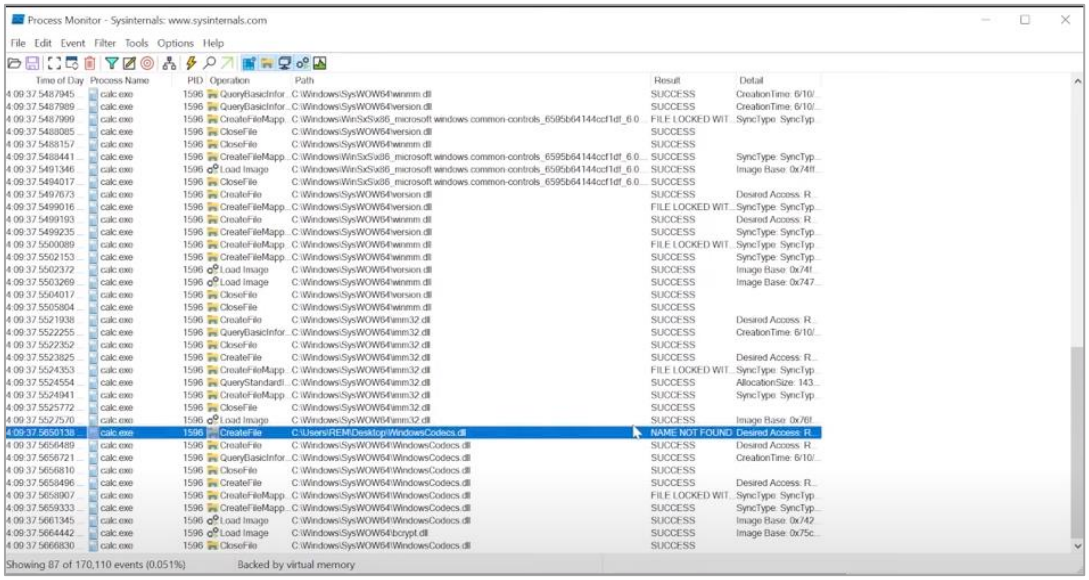


Figure 31: Stage 5- windowscodecs.dll sideloaded when calc.exe executed.

2. Analyzing the windowscodecs.dll file, refer to the below figures for information.

```
remnux@remnux:~/Downloads/application (8)/2518$ peframe WindowsCodecs.dll
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)


-------------------------------------------------------------------------------
File Information (time: 0:00:00.968403)
-------------------------------------------------------------------------------
filename          WindowsCodecs.dll
filetype          PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
filesize          4608
hash sha256       6e3661049bde832369781afa1d9034315442b1e4b87aa92d571cbe73186997c5
virustotal        /
imagebase         0x10000000 *
entrypoint        0x1080
imphash           87a1f1c5766b04416c137412a6152760
datetime          2022-07-11 14:15:55
dll               True
directories       import, export, tls, resources, relocations
sections          .text, .rdata, .data, .rsrc, .reloc
features          antidbg, packer
```


```
-------------------------------------------------------------------------------
Import function
-------------------------------------------------------------------------------
KERNEL32.dll      9
USER32.dll        1
```

Figure 32: Stage 5- Analysis of windowscodecs.dll file

3. The windowscodecs.dll file is registered using DllRegisterServer and its entries are included in the system registry. This enables other applications to recognize and utilize the functionality provided by the dll.

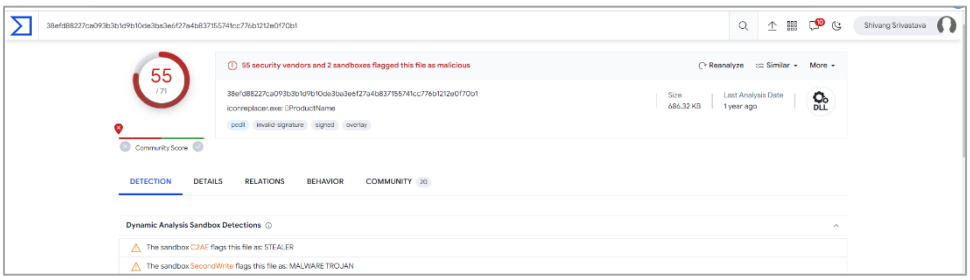
```
=== EXPORTS ===

# module "dll_helper.dll"
# flags=0x0  ts="2106-02-07 06:28:15"  version=0.0  ord_base=1
# nFuncs=2  nNames=2

  ORD ENTRY_VA  NAME
    1     1030  DllInstall
    2     1000  DllRegisterServer
remnux@remnux:~/Downloads/2518$
```

Figure 33: Stage 5- dll registration in DllRegisterServer.

Stage 6: windowscodecs.dll executes the malicious payload dll (102755.dll)

1. When Windowscodecs.dll is loaded, it will execute the malicious payload 102755.dll as well.
2. Analyzing the 102755.dll file, refer to the below figures for information.

```
remnux@remnux:~/Downloads/application (8)/2518$ peframe 102755.dll
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)


-------------------------------------------------------------------------------
File Information (time: 0:00:02.521666)
-------------------------------------------------------------------------------
filename          102755.dll
filetype          PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
filesize          702792
hash sha256       38efd88227ca093b3b1d9b10de3ba3e6f27a4b837155741cc776b1212e0f70b1
virustotal        /
imagebase         0x400000
entrypoint        0x5a60c
imphash           05ed4a07fc9a6a7112c8cd9c50f474b3
datetime          1992-06-19 22:22:17
dll               True
directories       import, tls, resources, relocations, sign
sections          DATA, BSS, .idata, .rsrc, CODE *, .reloc *
features          mutex, antidbg, packer, crypto
```




```
-------------------------------------------------------------------------------
Anti Debug
-------------------------------------------------------------------------------
FindWindowA
GetLastError
GetWindowThreadProcessId
RaiseException
UnhandledExceptionFilter
```

Figure 34: Stage 6- 102755.dll Analysis.

3. 102755.dll file will connect to the C2 to download the payloads. Refer the below figures for more information.

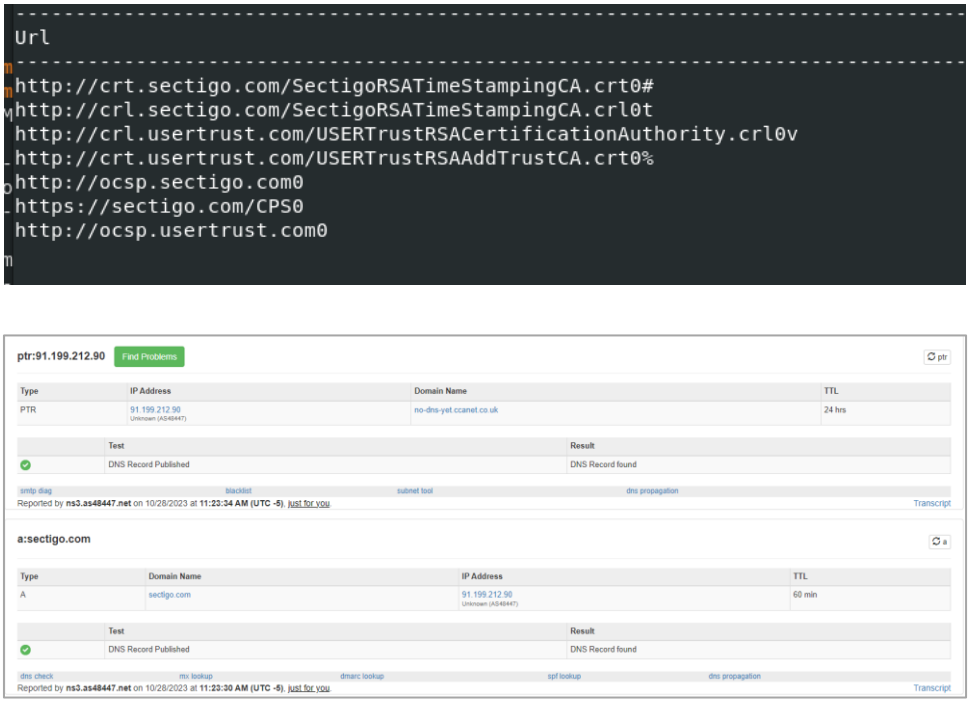


Figure 35: Stage 6- 102755.dll connect with C2.

5.0 Diamond Model

To analyze and understand the cyberthreats and incidents by Qakbot/Qbot, we can use the diamond model. The four components of diamond model Adversary, Infrastructure, Victim and Capability are explained below for Qakbot/Qbot malware.

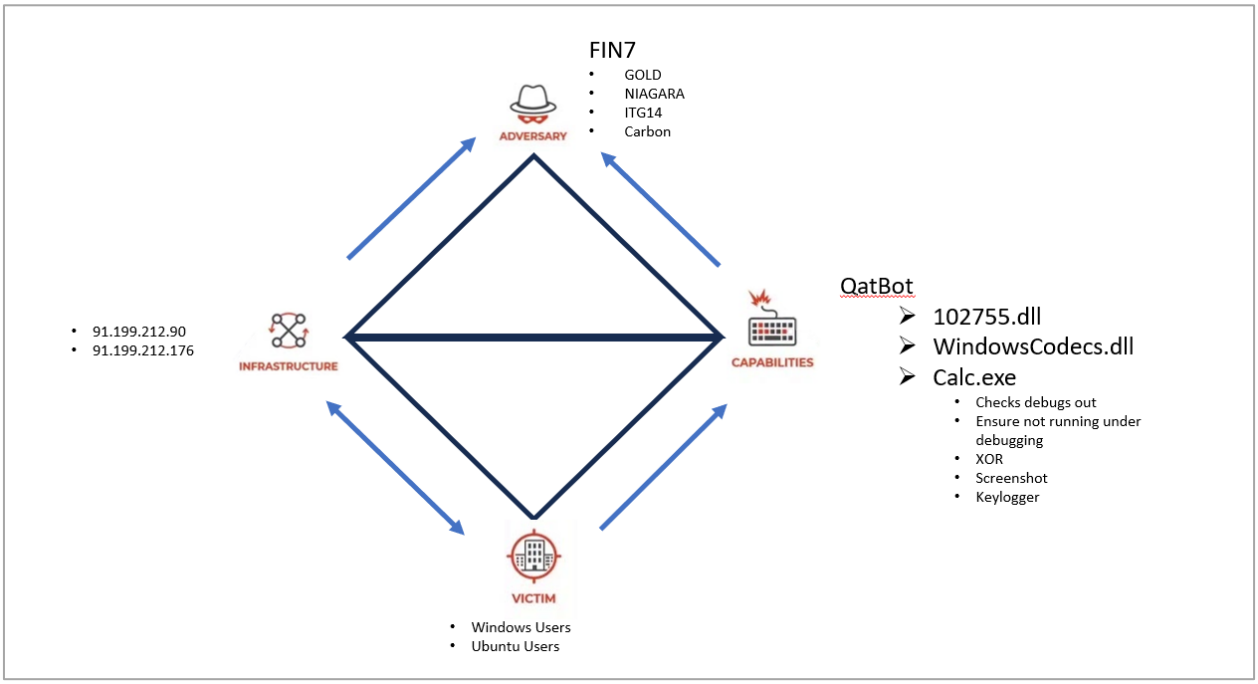


Figure 36: Qakbot Diamond Model

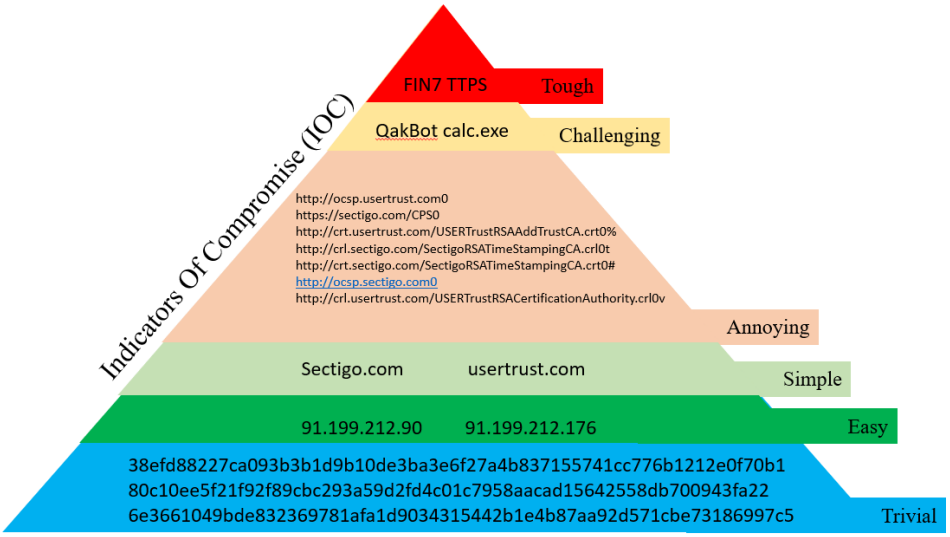


Figure 37: Pyramid Of Pain

Tactic	Technique	Sub Technique	Description
TA0002 - Execution	T1204 - User Execution	T1204.001 - Malicious Link	QakBot leverages malicious hyperlinks to initiate the execution of its payload.
TA0002 - Execution	T1204 - User Execution	T1204.002 - Malicious File	QakBot can be delivered through malicious file attachments, exploiting vulnerabilities upon execution.
TA0005 - Defense Evasion	T1218 - System Binary Proxy Execution	T1218.007 - System Binary Proxy Execution: Msiexec	QakBot uses the Windows Installer (msiexec) for evasion purposes, blending into legitimate processes.
TA0004 - Privilege-Escalation	T1055 - Process Injection		QakBot utilizes process injection to run malicious code within legitimate processes, evading detection.
TA0004 - Privilege-Escalation	T1574 - Hijack Execution Flow	T1574.002 - DLL Side-Loading	QakBot may load malicious DLLs into legitimate processes to escalate privileges.
TA0004 - Privilege-Escalation	T1543 - Create or Modify System Process	T1543.003 - Create or Modify System Process: Windows Service	QakBot may establish persistence by creating a Windows service with malicious functionality.

Table 4: Mapping of TTPs to QakBot

6.0 Detection for Qakbot/QBot – Yara Rules

YARA is a popular open-source tool and a rule-based language used for identifying and classifying files based on patterns, attributes, and characteristics. YARA rules are essentially a set of defined patterns and conditions that help you search for and identify files or data that match specific criteria. They are widely used in cybersecurity for malware detection, threat hunting, and intrusion detection. Here's an overview of YARA rules: To detect the malicious dll of Qakbot/Qbot, we can create YARA rules as below.

```
rule Detect_102755_DLL {
   meta:
      description = "YARA rule for detecting multiple strings in 102755.dll"
   strings:
      $string_list = "win_hook"
      $string_list = "network_udp_sock"
      $string_list = "network_tcp_listen"
      $string_list = "network_tcp_socket"
      $string_list = "network_dns"
      $string_list = "screenshot"
      $string_list = "keylogger"
      $string_list = "win_registry"
      $string_list = "win_files_operation"
      $string_list = "Str_Win32_Winsock2_Library"
      $string_list = "Delphi_FormShow"
      $string_list = "Delphi_CompareCall"
      $string_list = "Delphi_Copy"
      $string_list = "Delphi_StrToInt"
      $string_list = "Delphi_DecodeDate"
      $string_list = "Borland"
      $string_list = "IsPE32"
      $string_list = "IsDLL"
      $string_list = "IsWindowsGUI"
      $string_list = "HasOverlay"
      $string_list = "HasDigitalSignature"
      $string_list = "borland_delphi_dll"
      $string_list = "Borland_Delphi_40_additional"
      $string_list = "Microsoft_Visual_Cpp_v50v60_MFC"
      $string_list = "Borland_Delphi_30_additional"
      $string_list = "Borland_Delphi_30_"
      $string_list = "Borland_Delphi_Setup_Module"
      $string_list = "Borland_Delphi_40"
      $string_list = "Borland_Delphi_v40_v50"
      $string_list = "Borland_Delphi_v30"
      $string_list = "Borland_Delphi_DLL"
```

```
    condition:
        any of them
}

rule Detect_Calc_EXE {
    meta:
        description = "YARA rule for detecting multiple strings in calc.exe"
    strings:
        $string_list = "SEH_Save"
        $string_list = "SEH_Init"
        $string_list = "Check_OutputDebugStringA_iat"
        $string_list = "anti_dbg"
        $string_list = "screenshot"
        $string_list = "keylogger"
        $string_list = "win_registry"
        $string_list = "IsPE32"
        $string_list = "IsWindowsGUI"
        $string_list = "IsPacked"
        $string_list = "HasDebugData"
        $string_list = "HasRichSignature"

    condition:
        any of them
}
rule Detect_WindowsCodecs_DLL {
    meta:
        description = "YARA rule for detecting multiple strings in WindowsCodecs.dll"
    strings:
        $string_list = "anti_dbg"
        $string_list = "IsPE32"
        $string_list = "IsDLL"
        $string_list = "IsWindowsGUI"
        $string_list = "HasDebugData"
        $string_list = "HasRichSignature"
        $string_list = "Microsoft_Visual_Cpp_v50v60_MFC"

    condition:
        any of them
}
```

7.0 Understanding the Science behind the Qakbot

After the analysis we started researching the science behind the Qakbot. We tried to get knowledge on Qakbot from the database of Malware Bazaar through API.

1. We send a request to the API, specifically asking for the 1000 "latest" malware SHA-256 samples with the tag "Qakbot." This gives us access to the most recent instances of this malware strain. Each sample is identified by its unique SHA-256 hash. Refer the below figure for the Python code to import the data,

```
@author: shiva
"""

import requests

API_ENDPOINT = "https://mb-api.abuse.ch/api/v1/"
headers = {'API-KEY': '12ecb62a793113ef0478bc9f3180317c'}  # Replace 'YOUR_API_KEY' w

data = {
    'query': 'get_taginfo',
    'tag': 'Quakbot',
    'limit': 1000
}

response = requests.post(API_ENDPOINT, data=data, headers=headers)

if response.status_code == 200:
    results = response.json()
    if 'data' in results:
        sha256_hashes = [entry.get('sha256_hash') for entry in results['data']]
        with open('quakbot_hashes.txt', 'w') as file:
            for hash_value in sha256_hashes:
                file.write(hash_value + '\n')
        print("SHA-256 hashes saved to 'quakbot_hashes.txt'.")
    else:
        print("No data found in the response.")
else:
    print(f"Request failed with status code {response.status_code}.")
```

2. Run the above code to get the 1000 Hash values (latest samples) to get the information about the samples and save them in excel namely First seen, Last seen, Delivery Method, File Type and the corresponding SHA value for the malware.

```
import requests
import pandas as pd
API_ENDPOINT = "https://mb-api.abuse.ch/api/v1/"
API_KEY = "-api.abuse.ch/api/v1/"
headers = {'API-KEY': '12ecb62a793113ef0478bc9f3180317c'}  # Replace with your actual API key



with open('quakbot_hashes.txt', 'r') as file:
    data = file.read()

# Split the data into individual lines (assuming each line contains one hash)
hash_list = data.strip().split('\n')
hashes=hash_list
#hashes = ["0b6e3977e1e40cba19d5be5bbc194fd72131e019febae55ba82e91ea3ca28d19","775ca69b395e7d228e5326cfbbd6a47b2456e743c6840503177 49cff6eec9150"]
first_seen_list = []
last_seen_list=[]
file_type_list = []
delivery_method= []
sha256_hash=[]
i=1
for hash_value in hashes:
    data = {
        "query": "get_info",
        "hash": hash_value,
    }
    headers = {"API-KEY": API_KEY}

    response = requests.post(API_ENDPOINT, data=data, headers=headers)

    if response.status_code == 200:
        result = response.json()
        # Process the result as needed
        #print(result)
        print(i)
        i+=1
        for item in result['data']:
            first_seen_list.append(item['first_seen'])
            last_seen_list.append(item['last_seen'])

            file_type_list.append(item['file_type'])
            delivery_method.append(item['delivery_method'])
            sha256_hash.append(item['sha256_hash'])

    else:
        print(f"Request failed with status code {response.status_code}.")
df = pd.DataFrame({'First Seen': first_seen_list,'Last Seen': last_seen_list, 'File Type': file_type_list, 'Delivery Method': delivery_method, 'Hash': sha256_

# Save to Excel
df.to_excel('output.xlsx', index=False)
```

3. Downloaded intelligence about 1000 latest malware samples from Qakbot malware are in the format shown below.

First Seen	Last Seen	File Type	ivery M	Hash
2023-10-19	15:28:43	lnk	web_dow	9b6e3977e1e40cba19d5be5bbc194fd72131e019febae55ba82e91ea3ca28d19
2023-10-1	2023-10-2	zip	web_dow	775ca69b395e7d228e5326cfbbd6a47b2456e743c684050317749cff6eec9150
2023-09-07	18:32:30	lnk		8f5fa78c2b92c3f4b0ce7ae1b4adca6e895d6bf32e3c11a8a604ca48bbdab112
2023-08-25	01:11:58	7z		3f004293165057ac40d7d2dc663cc62c877ebe29601251dcca24b6aa1062b7af
2023-08-18	10:40:24	js	email_att	eec3dce6ca41b66570a08433a5a9b9b2a1cffb037b5255bd589ccf089c12e8ac
2023-08-18	03:26:20	dll		7ee6095ba8c4ed9fe11fbf5e703823e1aeae7f5443027738f55979b27ca57171
2023-07-11	10:43:21	js		66f6ac4a4950397df2f012b7eb4d6576d1dff9629a175677786c44596715b9f9
2023-07-10	09:31:25	dll		4c7d5ae6fefb8f53e0f557a241f95a677482bc4219c1d91573425ebc0cb44830
2023-07-10	09:31:17	js		cf5295f7c653e106bcf8367feb1daa26144f94e7721f0840d2c61f0ec7bd33c4
2023-07-10	09:31:11	zip	web_dow	749699a9a6198e917dd0b9dbb3769324cffe1f7bb570a8540c06b229ec0909c6
2023-06-25	07:05:26	dll		7619db1cbeef2ec38d180fdd9fecb8dd8776c90b6c1941e4f685c0a9b03b1343
2023-06-23	19:35:13	js		88590eb81c23e50c1a52a49e48b37b5bc72ead1868ca45adc4ffe5c8485a9626
2023-06-23	19:34:52	js		be26c5d7a70cc3ea46138c2ef3b589a381d61a9aaabd50ad9b8095d80f8260d9
2023-06-23	19:34:31	js		dbc198139b9f4ecbe0170b51d2e802873ac2e98db5d0f8fef6913c2f01e82e41
2023-06-23	19:34:05	js		c68f65405594431595c84bc345c28a7d73b797ae8b007352ccb48ddaecf03fee
2023-06-23	19:33:41	js		2270d9b08ecb65e01b8a490dede9b1480431bdfaa052cecc54a1231fe56e655a
2023-06-23	19:32:05	dll		457c622ba31de68f44d01c63de335b32cc7ef2cbbf6c48a2acdd868a28ddba97
2023-06-23	19:31:24	dll		8386c26ef88062db37966613ac32debe4ec5be1e44ea42ae89d8ad7fbf3f83e5
2023-06-23	19:30:51	dll		90d800f250c1951c9f015b95bd590263b550af0ba56b0719325af093f184839d

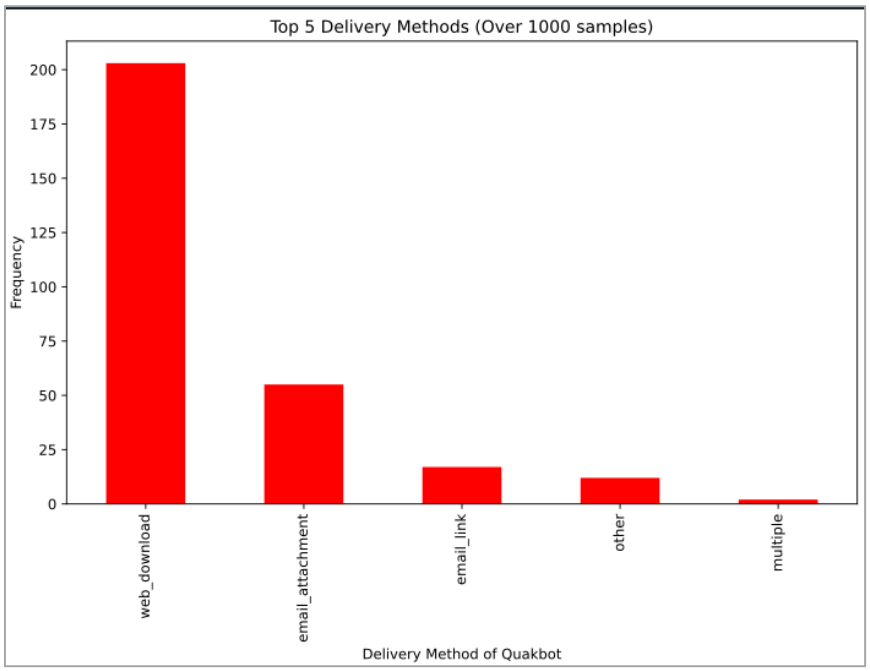
4. With the information gathered in excel, we plotted the common delivery method for Qakbot. The below figure shows the code used to plot the chart.

```
# -*- coding: utf-8 -*-
"""
Created on Sun Oct 29 03:15:36 2023

@author: shiva
"""

import pandas as pd
import matplotlib.pyplot as plt

# Reading the CSV
df = pd.read_excel('output.xlsx')
# Extracting the 'Delivery Method' column
delivery_methods = df.iloc[:, 3]

# Counting frequencies
delivery_counts = delivery_methods.value_counts().nlargest(5)

# Plotting the bar chart
plt.figure(figsize=(10, 6))
delivery_counts.plot(kind='bar', color='red')
plt.title('Top 5 Delivery Methods')
plt.xlabel('Delivery Method of Quakbot')
plt.ylabel('Frequency')
plt.show()
```

The most used delivery method of Qakbot is “Web_download”. The below is the top delivery methods.

1. Web_download
2. email_attachment
3. email_link
4. other
5. multiple

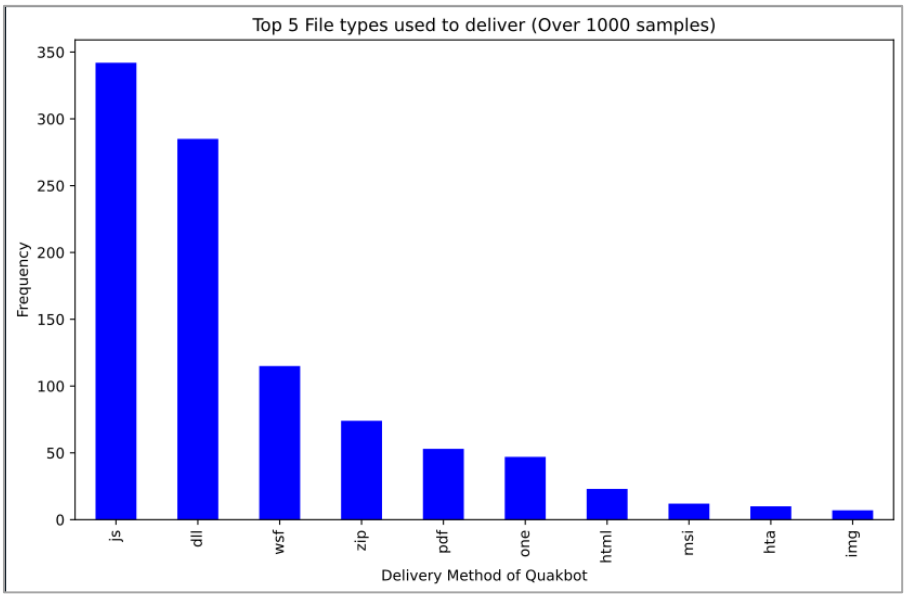
Refer the below figure for the generated chart.



5. With the information gathered in excel, we plotted the delivery method for Qakbot. The below figure shows the code used to plot the chart.

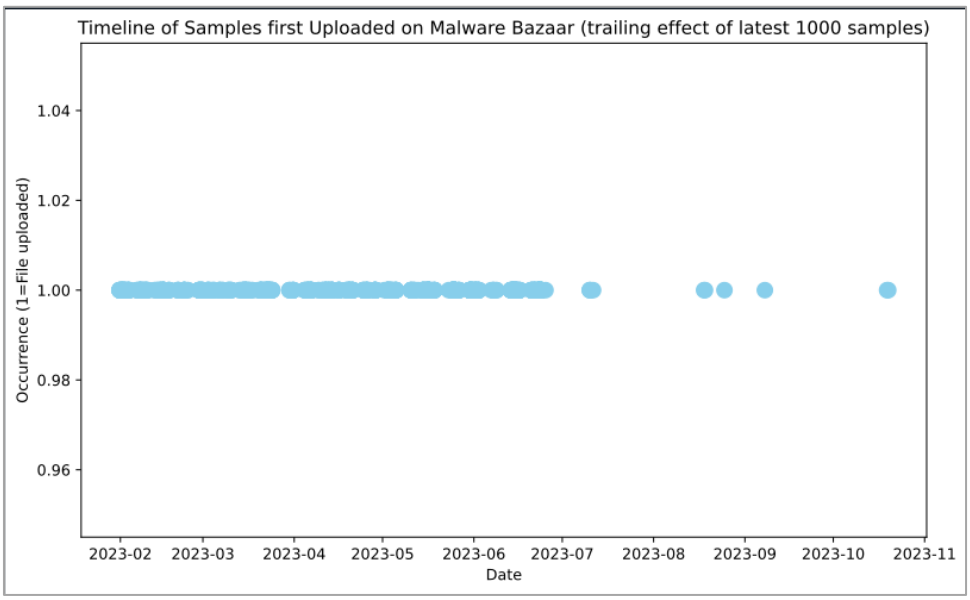
```
import pandas as pd
import matplotlib.pyplot as plt
from datetime import datetime
# Reading the CSV
df = pd.read_excel('output.xlsx')
# Extracting the 'Delivery Method' column
delivery_methods = df.iloc[:, 2]

# Counting frequencies
delivery_counts = delivery_methods.value_counts().nlargest(10)

# Plotting the bar chart
plt.figure(figsize=(10, 6))
delivery_counts.plot(kind='bar', color='blue')
plt.title('Top 5 File types used to deliver (Over 1000 samples)')
plt.xlabel('Delivery Method of Quakbot')
plt.ylabel('Frequency')
plt.show()
```

The most common file types used to deliver Qakbot are represented in the below chart.



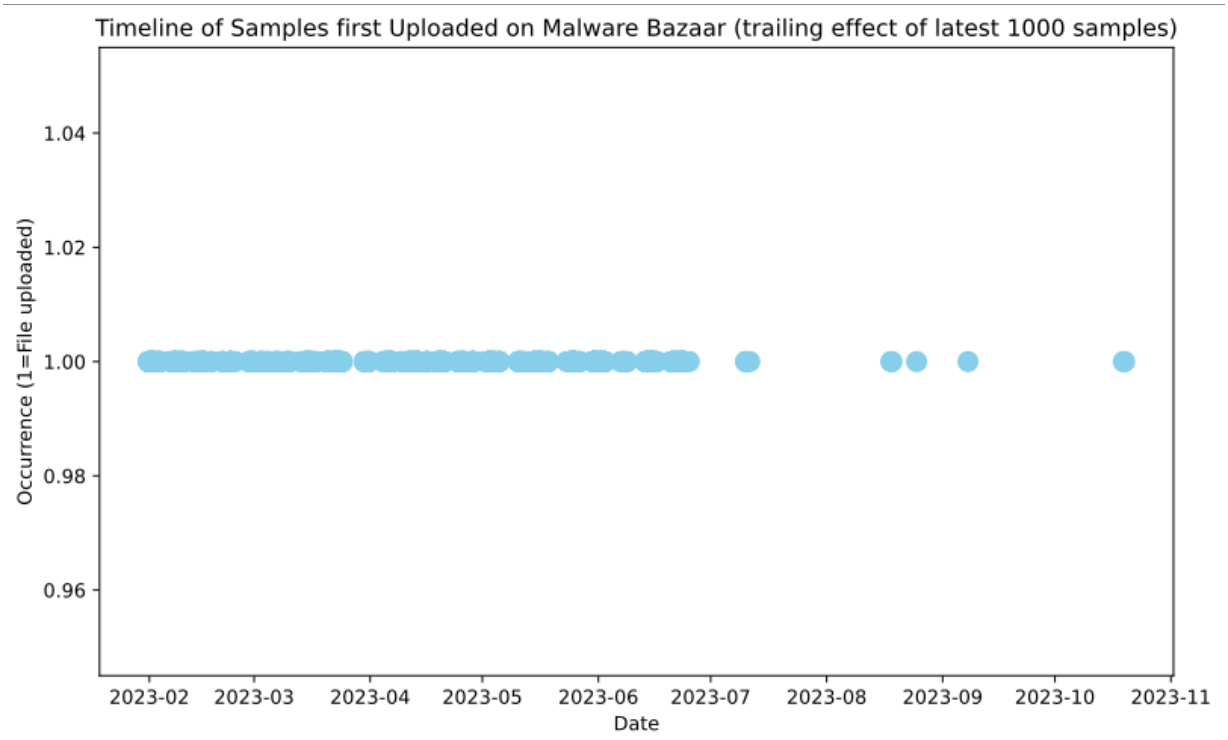
6. Timeline of samples first seen on malware bazaar for Qakbot (entry effect). It is important to note that we picked the latest 1000 samples. So, it is easy to see that after 2023-07, the sample is not being uploaded anymore, indicating likely that it is patched and isn't functional, and the CCs are dow

```
df = pd.read_excel('output.xlsx')

# Extracting the dates from the first column
dates = pd.to_datetime(df.iloc[:, 0])

# Creating a list of 1s to represent the presence of an entry on that date
values = [1] * len(dates)

# Creating scatter plot
plt.figure(figsize=(10, 6))
plt.scatter(dates, values, color='skyblue', s=100)

# Setting the title and labels
plt.title('Timeline of Samples first Uploaded on Malware Bazaar (entry effect)')
plt.xlabel('Date')
plt.ylabel('Occurrence (1=File uploaded)')
plt.show()
```



7. Timeline of samples last seen on malware bazaar for Qakbot (trailing effect). It is important to note that we picked the latest 1000 samples. So, it is easy to see that after 2023-06/7, the sample is not being uploaded anymore, indicating likely that it is patched and isn't functional, and the CCs are down.

```
df = pd.read_excel('output.xlsx')

# Extracting the dates from the first column
dates = pd.to_datetime(df.iloc[:, 1])

# Creating a list of 1s to represent the presence of an entry on that date
values = [1] * len(dates)

# Creating scatter plot
plt.figure(figsize=(10, 6))
plt.scatter(dates, values, color='skyblue', s=100)

# Setting the title and labels
plt.title('Timeline of Samples last Uploaded on Malware Bazaar (trailing effect')
plt.xlabel('Date')
plt.ylabel('Occurrence (1=File uploaded)')
plt.show()
```



8.0 Mitigations for the identified Techniques

Technique ID	Frequency	Technique	Tactic	Mitigations [2]						
T1059	15	Command and Scripting Interpreter	Execution	Quarantine using Antimalware	Enable Attack Surface Reduction rules to prevent Visual Basic and JS scripts from malicious download	Allow running of signed scripts only	Disable unnecessary scripts	Use application control for execution prevention	Restrict Web Based content	Manage privileged accounts
T1566	14	Phishing	Initial Access	Quarantine using Antimalware	Use Network Intrusion Detection systems to scan and remove malicious attachments and block activity	Restrict or block web-based content. Ex: exe files over emails	Use SPF (sender validity) and DKIM (integrity) for authentication and integrity of email messages	User Training		
T1204	12	User Execution	Execution	Enable Attack Surface Reduction rules to prevent executable files from running unless they meet a certain age or trust to prevent Office Apps from creating malicious content	Prevent running of executable files masquerading as other files	Use Network IPS to scan and remove malicious downloads	If a link is visited by a user, unknown files should not be downloaded, especially from suspicious sites	User Training		
T1078	10	Valid Accounts	Defense Evasion, Initial Access, Persistence, Privilege Escalation	To prevent logins from non-compliant devices or from outside of specified company IP ranges, use conditional access controls.	Disable legacy authentication which does not support MFA	Make sure that no private information or login credentials are stored by apps in an unsafe manner.	Before being deployed to a production environment, applications and appliances that use the default login and password should be changed right away following installation.	Regularly audit domain and local accounts, together with their permission levels to look for possible breaches	Remove accounts that are not needed (Audit)	Train users to only accept valid push notifications and to report suspicious push notifications. (MFA)

Technique ID	Frequency	Technique	Tactic	Mitigations [2]						
T1070	10	Indicator Removal	Defense Evasion	Obfuscate/encrypt event files locally and in transit to avoid giving feedback to an adversary.	Immediately forward events to a data repository or log server to avoid situations where an adversary could find and alter data on the local system.	Protect generated event files that are stored locally with proper permissions and authentication				
T1027	10	Obfuscated Files or Information	Defense Evasion	Using antivirus software, questionable files can be automatically identified and quarantined. Use the Antimalware Scan Interface (AMSI)	It is advisable to conduct routine examinations of frequently used fileless storage locations (like the Registry) to detect any unusual or malicious data.	On Windows 10+, enable Attack Surface Reduction (ASR) rules to prevent execution of potentially obfuscated payloads				
T1021	9	Remote Services	Lateral Movement	Use multi-factor authentication on remote service logons where possible.	Restrict which accounts can use remote services. Restrict the permissions of accounts that are more likely to be compromised; for instance, set up SSH so users can only execute applications.					
T1053	9	Scheduled Task/Job	Execution, Persistence, Privilege Escalation	Toolkits like the Powerspolit framework contain Powerup modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges.	Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM.	Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process.	Restrict user account privileges and fix Privilege Escalation vectors so that only authorized administrators can establish scheduled tasks on remote systems.			

Technique ID	Frequency	Technique	Tactic	Mitigations [2]						
T1036	8	Masquerading	Defense Evasion	Anti-virus can be used to automatically quarantine suspicious files.	Implement security controls on the endpoint, such as a Host Intrusion Prevention System (HIPS), to identify and prevent execution of potentially malicious files (such as those with mismatching file signatures).	Require signed binaries.	Use tools that restrict program execution via application control by attributes other than file name for common operating system utilities that are needed.	Use file system access controls to protect folders such as C:¥Windows¥System32.		
T1071	8	Application Layer Protocol	Command and Control	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level.						
T1105	8	Ingress Tool Transfer	Command and Control	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known protocols like FTP can be used to mitigate activity at the network level.	Implement security controls on the endpoint, such as a Host Intrusion Prevention System (HIPS), to identify and prevent execution of potentially malicious files (such as those with mismatching file signatures).	Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions.	Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[493]	-		

The mitigation for various techniques were derived from mitre.org. The reference [2] can be found under section **Error! Reference source not found.**

9.0 Conclusion:

The QBOT malware family is highly active and still part of the threat landscape in mid-2023 due to its features and its powerful modular system. While initially characterized as an information stealer in 2007, this family has been leveraged as a delivery mechanism for additional malware and post-compromise activity.

However, with recent samples received in Malware Bazaar, the number of samples received is “null” and this explains most of the vulnerabilities used by this malware are already patched.

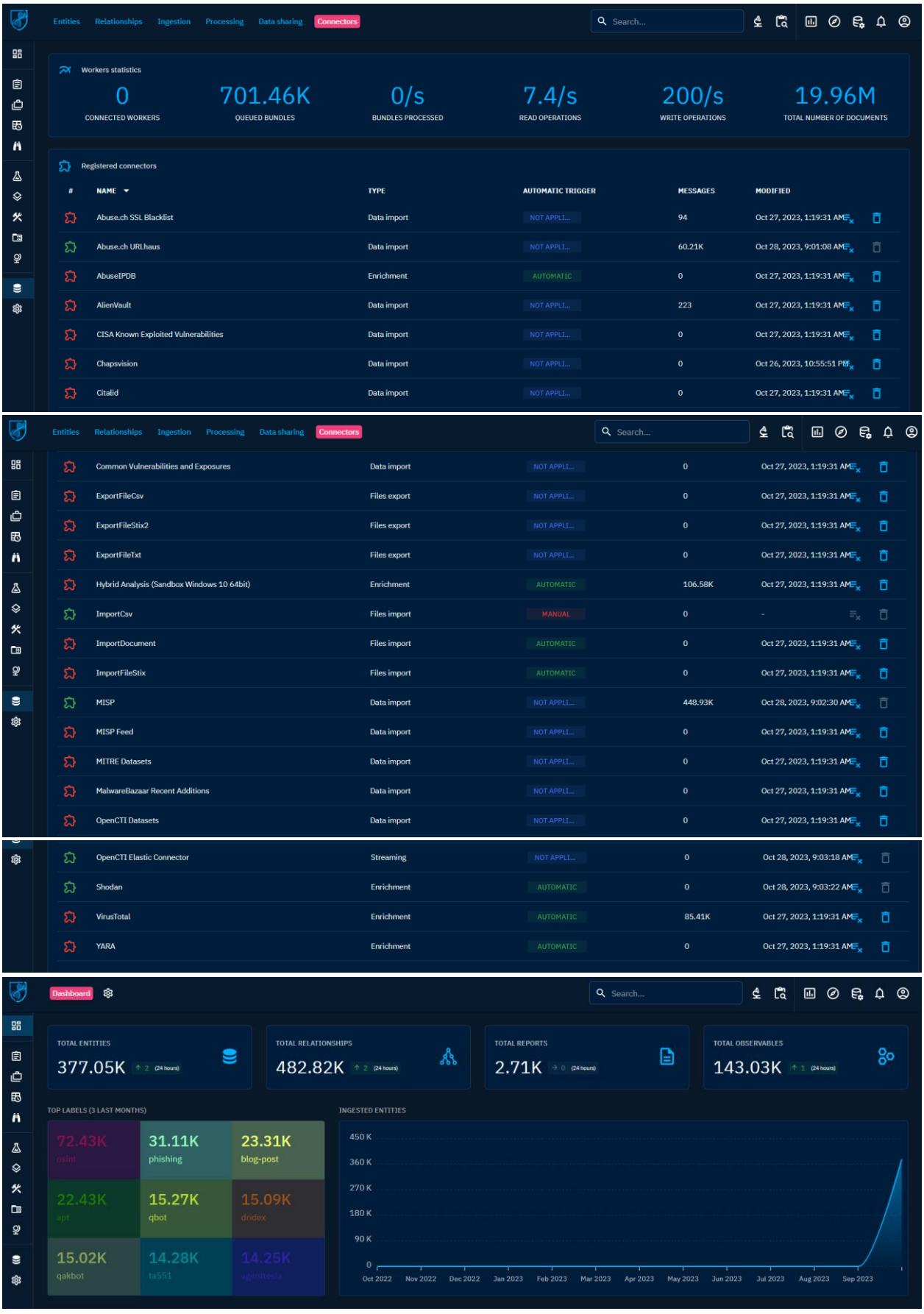
10.0 Appendix

We have utilized OpenCTI as threat intelligence platform to understand better on the Qakbot/Qbot malwares.

10.1 OpenCTI

OpenCTI is an open-source platform allowing organizations to manage their cyber threat intelligence knowledge and observables. It has been created to structure, store, organize and visualize technical and non-technical information about cyber threats.

Below are some of the snapshots of the OpenCTI platform. (We will demonstrate OpenCTI during our presentation)


Entities
Relationships
Ingestion
Processing
Data sharing
Connectors
Search...
Workers statistics
0
CONNECTED WORKERS
701.46K
QUEUED BUNDLES
0/s
BUNDLES PROCESSED
7.4/s
READ OPERATIONS
200/s
WRITE OPERATIONS
19.96M
TOTAL NUMBER OF DOCUMENTS
Registered connectors
NAME TYPE AUTOMATIC TRIGGER MESSAGES MODIFIED
Abuse.ch SSL Blacklist Data import NOT APPLI... 94 Oct 27, 2023, 1:19:31 AM
Abuse.ch URLhaus Data import NOT APPLI... 60.21K Oct 28, 2023, 9:01:08 AM
AbuseIPDB Enrichment AUTOMATIC 0 Oct 27, 2023, 1:19:31 AM
AlienVault Data import NOT APPLI... 223 Oct 27, 2023, 1:19:31 AM
CISA Known Exploited Vulnerabilities Data import NOT APPLI... 0 Oct 27, 2023, 1:19:31 AM
Chapsvision Data import NOT APPLI... 0 Oct 26, 2023, 10:55:51 PM
Citalid Data import NOT APPLI... 0 Oct 27, 2023, 1:19:31 AM
Common Vulnerabilities and Exposures Data import NOT APPLI... 0 Oct 27, 2023, 1:19:31 AM
ExportFileCsv Files export NOT APPLI... 0 Oct 27, 2023, 1:19:31 AM
ExportFileStix2 Files export NOT APPLI... 0 Oct 27, 2023, 1:19:31 AM
ExportFileTxt Files export NOT APPLI... 0 Oct 27, 2023, 1:19:31 AM
Hybrid Analysis (Sandbox Windows 10 64bit) Enrichment AUTOMATIC 106.58K Oct 27, 2023, 1:19:31 AM
ImportCsv Files import MANUAL 0 -
ImportDocument Files import AUTOMATIC 0 Oct 27, 2023, 1:19:31 AM
ImportFileStix Files import AUTOMATIC 0 Oct 27, 2023, 1:19:31 AM
MISP Data import NOT APPLI... 448.93K Oct 28, 2023, 9:02:30 AM
MISP Feed Data import NOT APPLI... 0 Oct 27, 2023, 1:19:31 AM
MITRE Datasets Data import NOT APPLI... 0 Oct 27, 2023, 1:19:31 AM
MalwareBazaar Recent Additions Data import NOT APPLI... 0 Oct 27, 2023, 1:19:31 AM
OpenCTI Datasets Data import NOT APPLI... 0 Oct 27, 2023, 1:19:31 AM
OpenCTI Elastic Connector Streaming NOT APPLI... 0 Oct 28, 2023, 9:03:18 AM
Shodan Enrichment AUTOMATIC 0 Oct 28, 2023, 9:03:22 AM
VirusTotal Enrichment AUTOMATIC 85.41K Oct 27, 2023, 1:19:31 AM
YARA Enrichment AUTOMATIC 0 Oct 27, 2023, 1:19:31 AM
Dashboard
TOTAL ENTITIES
377.05K
TOTAL RELATIONSHIPS
482.82K
TOTAL REPORTS
2.71K
TOTAL OBSERVABLES
143.03K
TOP LABELS (3 LAST MONTHS)
72.43K
31.11K phishing
23.31K blog-post
22.43K
15.27K qbot
15.09K
15.02K qakbot
14.28K
INGESTED ENTITIES
450 K
360 K
270 K
180 K
90 K
0
Oct 2022
Nov 2022
Dec 2022
Jan 2023
Feb 2023
Mar 2023
Apr 2023
May 2023
Jun 2023
Jul 2023
Aug 2023
Sep 2023

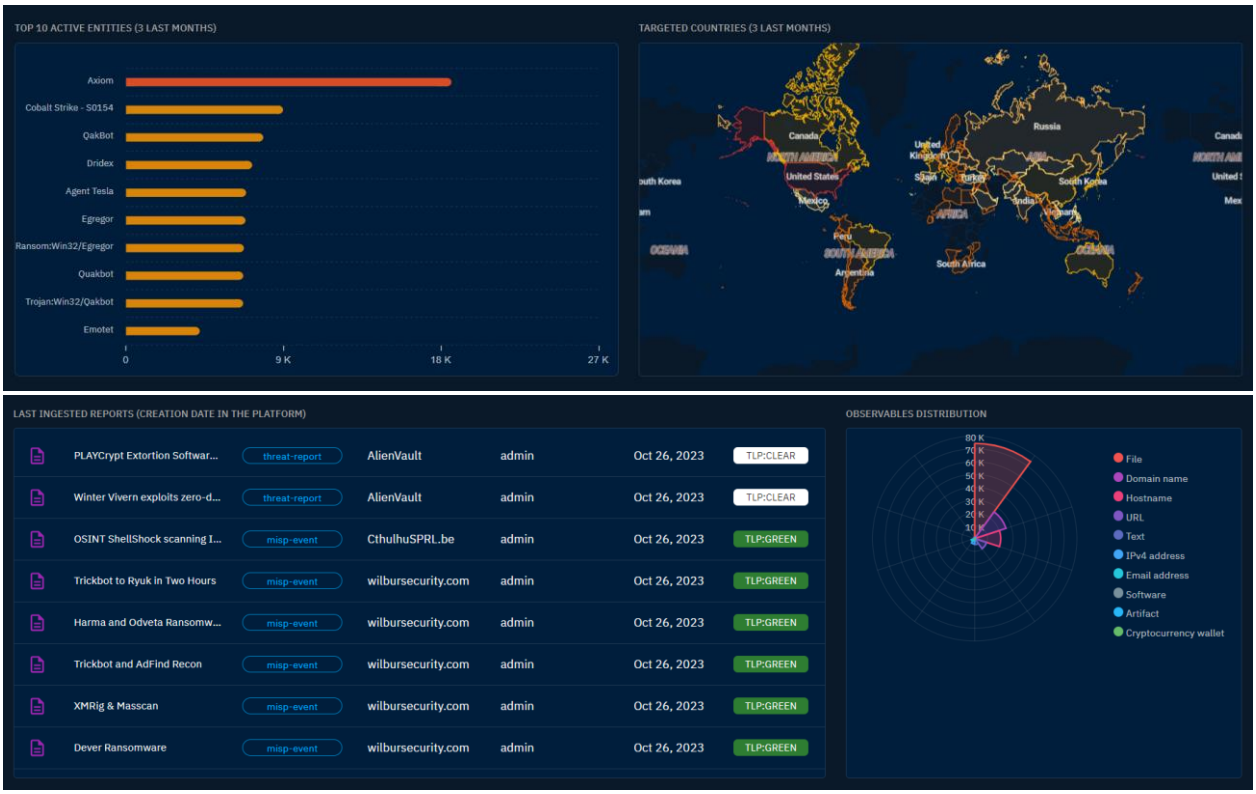
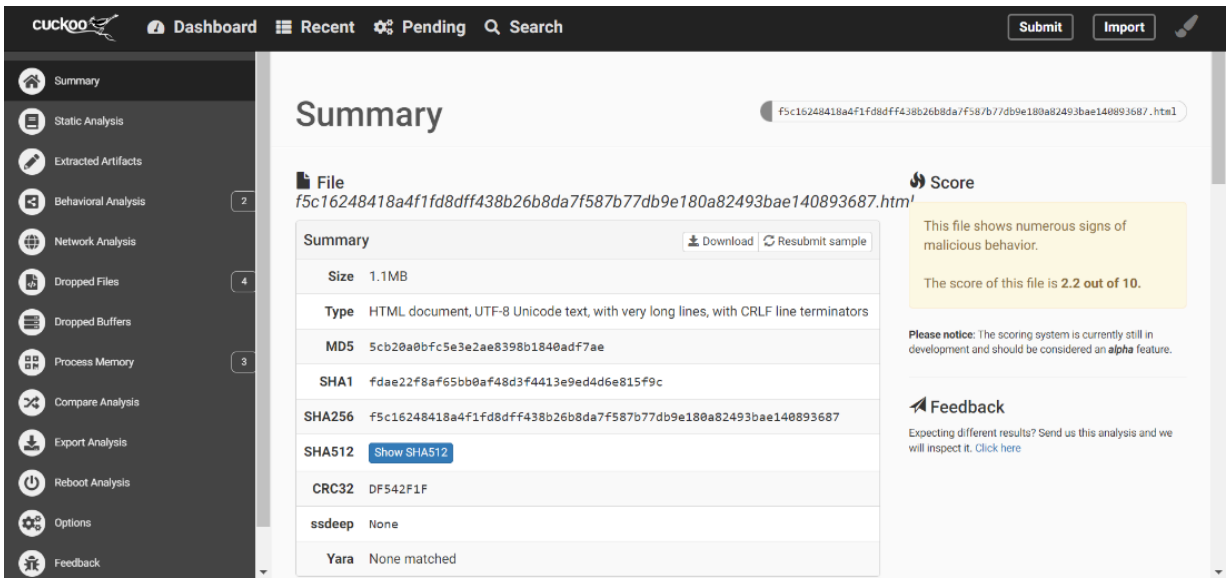


Figure 38: Snapshots of OpenCTI

10.2 Cuckoo

Cuckoo Sandbox is free software that automated the task of analyzing any malicious file under Windows, macOS, Linux, and Android. Below are some of the snapshots of the Cuckoo platform. (We will demonstrate Cuckoo during our presentation). [13]



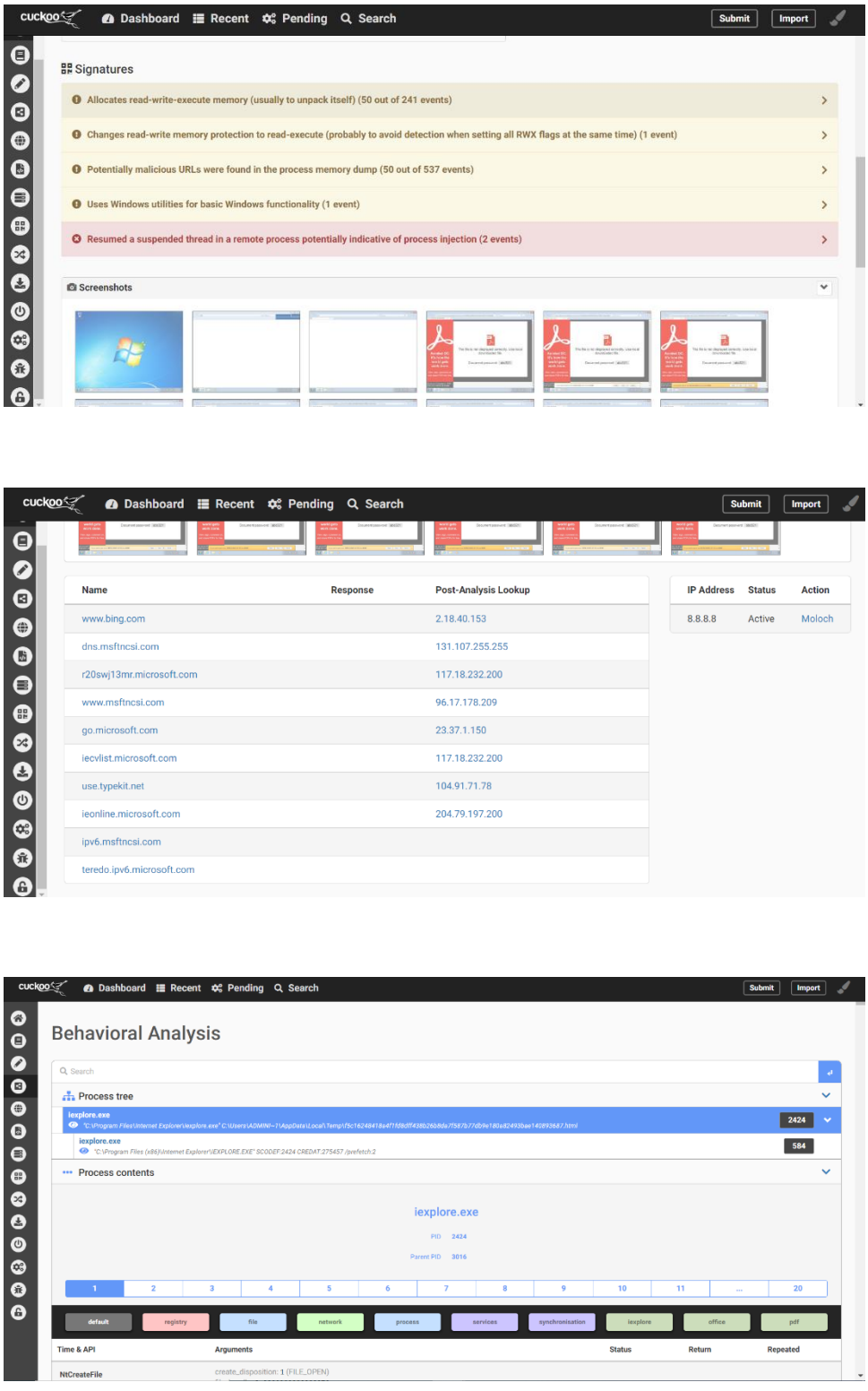


Figure 39: Snapshots of Cuckoo Sandbox

1. "https://securityintelligence.com," https://securityintelligence.com, [Online]. Available: https://securityintelligence.com/articles/cost-of-a-data-breach-2023-financial-industry/. [Accessed 13 11 2023].

2. "www.federalreserve.gov/aboutthefed.htm.," Federalreserve, 2022. [Online]. Available: https://www.federalreserve.gov/publications/files/cybersecurity-report-202207.pdf. [Accessed 13 11 2023].
3. "https://attack.mitre.org/," mitre.org, [Online]. Available: https://attack.mitre.org/groups/. [Accessed 13 11 2023].
4. "https://csrc.nist.gov," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures. [Accessed 13 11 2023].
5. "https://www.mandiant.com," https://www.mandiant.com, [Online]. Available: https://www.mandiant.com/resources/blog/evolution-of-fin7. [Accessed 13 11 2023].
6. "https://thehackernews.com," thehackernews.com, [Online]. Available: https://thehackernews.com/2022/12/fin7-cybercrime-syndicate-emerges-as.html. [Accessed 13 11 2023].
7. "https://cve.mitre.org/," https://cve.mitre.org/, [Online]. Available: https://cve.mitre.org/. [Accessed 13 11 2023].
8. "https://unit42.paloaltonetworks.com," https://unit42.paloaltonetworks.com, [Online]. Available: https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/. [Accessed 13 11 2023].
9. "https://bazaar.abuse.ch," https://bazaar.abuse.ch, [Online]. Available: https://bazaar.abuse.ch/download/723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224/. [Accessed 13 11 2023].
10. "https://malpedia.caad.fkie.fraunhofer.de/," https://malpedia.caad.fkie.fraunhofer.de/details, [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot. [Accessed 13 11 2023].
11. "https://bazaar.abuse.ch/," https://bazaar.abuse.ch/, [Online]. Available: https://bazaar.abuse.ch/sample/3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139daa/. [Accessed 13 11 2023].
12. "https://urlhaus.abuse.ch/," https://urlhaus.abuse.ch/, [Online]. Available: https://urlhaus.abuse.ch/url/2669875/. [Accessed 13 11 2023].
13. "ChatGPT query," ChatGPT query, [Online]. Available: https://chat.openai.com/. [Accessed 31 10 2023].
14. "https://cuckoosandbox.org/," https://cuckoosandbox.org/, [Online]. Available: https://cuckoosandbox.org/. [Accessed 13 11 2023]