



- E-ISSN: 2582-2160 Website: www.jifmr.com

Email: editor@iifmr.com

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

Srivastava Shivang¹, Chinnuswamy Tamizhselvan², Parameswaran Ganesan³, Rengabashyam Asha⁴

^{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

		2023	2022
1	↑	United States USD 9.48 million	
2	↑	Middle East USD 8.07 million	
3	¥	Canada USD 5.13 million	Canada USD 5.64 million
4	¥	Germany USD 4.67 million	United Kingdom USD 5.05 million
5	Ŷ	Japan USD 4.52 million	Germany USD 4.85 million

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.

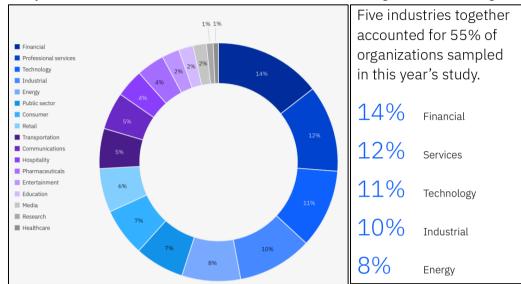


Figure 2: Distribution of the sample by Industry

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.



E-IS

E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u>

• Email: editor@ijfmr.com

2 CostaRicto October 25, 2023		Night Dragon October 25, 2023		2 Operation Dust St October 25, 2023		Operation Sharpsl October 25, 2023	hooter 🖌
spionage campaign tha	ted hacker-for-hire cyber t targeted multiple th a large number being	targeted oil, energy, and	er espionage campaign that I petrochemical companies, nd executives in Kazakhsta	cyber espionage campa	as a long-standing persistent ign that targeted multiple th Korea, the United States,		was a global cyber t targeted nuclear, defense, financial companies, with
NOWN AS	USED MALWARE	KNOWN AS	USED MALWARE	KNOWN AS	USED MALWARE	KNOWN AS	USED MALWARE
lostaRicto	PS1, CostaBricks, SombRAT	Night Dragon	zwShell, ASPXSpy	Operation Dust Storm	S-Type, ZLib, Mis-Type, PoisonIvy, ghOst RAT	Operation Sharpshooter	Rising Sun
ARGETED COUNTRIES	TARGETED SECTORS	TARGETED COUNTRIES	TARGETED SECTORS	TARGETED COUNTRIES	TARGETED SECTORS	TARGETED COUNTRIES	TARGETED SECTORS
No label		No label		No label		No label	
2 Operation Wocao October 25, 2023							
hat targeted organizatio	cyber espionage campaign ons around the world, I, France, Germany, Italy,						
NOWN AS	USED MALWARE						
peration Wocao							
ARGETED COUNTRIES	TARGETED SECTORS						

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]								



E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com

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 Asiaparticularly Taiwan,
		Japan, and Hong Kongand the US since at least 2013. BlackTech has
	1	1 / 0 0 0



E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com

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	GOLD SOUTHFIELD is a financially motivated threat group active
	SOUTHFIELD	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]
	Те	able 1: APT Groups (Financially Motivated)

 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 lowerlevel, 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.

		hard for an
	mport	heatMap.py
	mport	
	mport	csv illections import Counter
		pandas as pd
		seaborn as sns
		matplotlib.pyplot as plt the current directory
		<pre>smes = os.listdir(current_directory)</pre>
		iles = [file for file in file_names if file.endswith('.json')]
a	ppende	d_list = []
		n_file in json_files: :h open(os. <mark>path</mark> .join(current_directory, json_file), 'r') as file:
		<pre>techniques = data.get('techniques', []) appended_list.extend(techniques)</pre>
	iltere	<pre>ed_technique_ids = [entry['techniqueID'] for entry in appended_list if 'techniqueID' in entry and '.' not in entry['techniqueID']</pre>
		<pre>ue_id_counts = Counter(filtered_technique_ids)</pre>
s	orted_	<pre>technique_ids = sorted(technique_id_counts.items(), key=lambda item: item[1], reverse=True)</pre>
	37	# Initialize a list to store the appended data
	38 39	data = []
	40	# Open the original CSV file
	41	with open('t.csv', 'r') as file:
	42 43	<pre>reader = csv.reader(file) headers = next(reader) # Get the headers</pre>
	44	<pre>data.append([headers[0], # Get the headers data.append([headers[0], headers[1], headers[7]]) # Append headers for the selected columns</pre>
	45	
	46 47	for row in reader:
	48	<pre>data.append([row[0], row[1], row[7]]) # Append the required columns</pre>
	49	# Save the appended data to a new CSV file
	50	with open('appended_data.csv', 'w', newline='') as file:
	51 52	<pre>writer = csv.writer(file) writer.writerows(data)</pre>
	53	··· ···· ()
	54	
	55 56	# Save the data to a CSV file
	57	with open('HeatMapData.csv', mode='w', newline='') as file:
	58 59	writer = csv.writer(file)
	59 60	<pre>writer.writerow(['Technique ID', 'Frequency', 'Technique','Tactic']) for technique_id, frequency in sorted_technique_ids:</pre>
	61	for total_data in data:
	62	<pre>#print(total_data[0])</pre>
	63 64	<pre>if(technique_id==total_data[0]): writer.writerow([technique_id, frequency,total_data[1],total_data[2]])</pre>
	65	
	66	print("SHI")
	67 68	print("Data has been saved to HeatMapData.csv")
	69	
	70	
	71	
	73	
	74	# Read the data from the CSV file
	75	df = pd.read_csv('HeatMapData.csv')
	77	# Filter the DataFrame to include only rows with frequency >= 2
	78	<pre>df_filtered = df[df['Frequency'] >= 2]</pre>
	79 80	# Pivot the filtered DataFrame to make Technique as subheaders of each Tactic
	81	<pre>df_pivot = df_filtered.pivot_table(index='Tactic', columns='Technique', values='Frequency', fill_value=0)</pre>
	82	
	83 84	<pre># Create a heatmap plt.figure(figsize=(12, 8))</pre>
	85	<pre>sns.heatmap(df_pivot, annot=True, cmap='YlGnBu', fmt='g')</pre>
	86	<pre>plt.title('Technique Frequency Heatmap (Frequency >= 2)')</pre>
	87	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.

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Obtain Capabilities: 3.0%	Phishing: 3.8%	Command and Scripting Interpreter: 4.1%	Valid Accounts: 2.7%	Valid Accounts: 2.7%	Valid Accounts: 2.7%	Brute Force: 1.4%	Network Service Discovery: 1.4%	Remote Services: 2.4%	Data Staged: 1.4%	Application Layer Protocol: 2.2%	Exfiltration Over Alternative Protocol: 1.1%	Data Encrypted for Impact: 0.8%
Acquire Infrastructure: 0.5%	Valid Accounts: 2.7%	User Execution: 3.3%	Scheduled Task/Job: 2.4%	Scheduled Task/Job: 2.4%	Indicator Removal: 2.7%	OS Credential Dumping: 1.4%	Remote System Discovery: 1.4%	Exploitation of Remote Services: 0.5%	Data from Local System: 1.1%	Ingress Tool Transfer: 2.2%	Exfiltration Over Web Service: 0.5%	Data Destruction: 0.3%
Develop Capabilities: 0.3%	1.1%	Scheduled Task/Job: 2.4%	Create or Modify System Process: 1.9%	Create or Modify System Process: 1.9%	Obfuscated Files or Information: 2.7%	Input Capture: 0.8%	System Owner/User Discovery: 1.1%	Lateral Tool Transfer: 0.5%	Input Capture: 0.8%	Web Service: 1.6%	Exfiltration Over C2 Channel: 0.5%	Data Manipulation: 0.3%
Establish Accounts: 0.3%	Supply Chain Compromise: 0.8%	System Services: 1.4%	Boot or Logon Autostart Execution: 1.9%	Boot or Logon Autostart Execution: 1.9%	Masquerading: 2.2%	Credentials from Password Stores: 0.5%	Software Discovery: 1.1%	Removable Media: 0.3%	Archive Collected Data: 0.8%	Remote Access Software: 1.4%		Disk Wipe: 0.3%
Stage Capabilities: 0.3%	Exploit Public-Facing Application: 0.8%	Instrumentation: 1.4%	External Remote Services: 1.1%	Process Injection: 1.4%	System Binary Proxy Execution: 1.9%	Steal or Forge Kerberos Tickets: 0.5%	Network Share Discovery: 1.1%	Software Deployment Tools: 0.3%	Screen Capture: 0.8%	Proxy: 1.1%		System Shutdown/Reboot: 0.3%
	Replication Through Removable Media: 0.3%	Exploitation for Client Execution: 1.1%	Event Triggered Execution: 0.8%	Exploitation for Privilege Escalation: 1.1%	Process Injection: 1.4%	Network Sniffing: 0.3%	System Information Discovery: 0.8%		Automated Collection: 0.5%	Encrypted Channel: 0.8%		Resource Hijacking: 0.3%
	Drive-by Compromise: 0.3%	Native API: 0.8%	Hijack Execution Flow: 0.8%	Event Triggered Execution: 0.8%	Subvert Trust Controls: 1.4%	Steal Web Session Cookie: 0.3%				Non-Standard Port: 0.8%		Service Stop: 0.3%
	Hardware Additions: 0.3%	Inter-Process Communication: 0.5%	Server Software Component: 0.5%	Access Token Manipulation: 0.8%	Modify Registry: 1.4%	Adversary-in-the-Middle: 0.3%	File and Directory Discovery: 0.5% System Network		Adversary-in-the-Middle: 0.3%			
	Trusted Relationship: 0.3%	Software Deployment Tools: 0.3%	Boot or Logon Initialization Scripts: 0.3%	Hijack Execution Flow: 0.8%	Impair Defenses: 1.1%		Connections Discovery: 0.5%		Data from Information Repositories: 0.3%	Fallback Channels: 0.5%		
			Account Manipulation: 0.3%	Abuse Elevation Control Mechanism: 0.5%	Access Token Manipulation: 0.8%		System Network Configuration Discovery: 0.5%		Clipboard Data: 0.3%			
			Create Account: 0.3%	Boot or Logon Initialization Scripts: 0.3%	Hijack Execution Flow: 0.8%		Virtualization/Sandbox Evasion: 0.5%		Email Collection: 0.3%	Non-Application Layer Protocol: 0.3%		
			BITS Jobs: 0.3%		Abuse Elevation Control Mechanism: 0.5%		Domain Trust Discovery: 0.3%			Data Obfuscation: 0.3%		
			Pre-OS Boot: 0.3%		Virtualization/Sandbox Evasion: 0.5%		Browser Information Discovery: 0.3%			Multi-Stage Channels: 0.3%		
					BITS Jobs: 0.3% Pre-OS Boot: 0.3%		Process Discovery: 0.3% Network Sniffing: 0.3%			Data Encoding: 0.3%		
					XSL Script Processing: 0.3% Hide Artifacts: 0.3%							
					Deobfuscate/Decode Files or Information: 0.3%							
					Execution Guardrails: 0.3%							
					Rootkit: 0.3% File and Directory Permissions Modification: 0.3%							



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.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information: 40.0%	Obtain Capabilities: 68.8%		Command and Scripting Interpreter: 26.8%					Network Service Discovery: 12.8%	Remote Services: 60.0%	Data Staged: 19.2%	Application Layer Protocol: 17.0%	Exfiltration Over Alternative Protocol: 50.0%	Data Encrypted for Impa 33.3%
	Acquire Infrastructure: 12.5%	Valid Accounts: 26.3%	User Execution: 21.4%			Indicator Removal: 12.2%	OS Credential Dumping: 25.0%	Remote System Discovery: 12.8%	Exploitation of Remote Services: 13.3%	Data from Local System: 15.4%	Ingress Tool Transfer: 17.0%	Exfiltration Over Web Service: 25.0%	
Search Open Websites/Domains: 20.0%	Develop Capabilities: 6.2%	External Remote Services: 10.5%	Schedul ed Task/Job: 16.1%			Obfuscated Files or Information: 12.2%	Input Capture: 15.0%		Lateral Tool Transfer: 13.3%	Input Capture: 11.5%	Web Service: 12.8%	Exfiltration Over C2 Channel: 25.0%	
Search Victim Owned Websites: 20.0%		Supply Chain Compromise: 7.9%	System Services: 8.9%	Boot or Logon Autostart Execution: 14.0%	Boot or Logon Autostart Execution: 13.0%	Masquerading: 9.8%	Credentials from Password Stores: 10.0%	Software Discovery: 10.3%	Replication Through Removable Media: 6.7%	Archive Collected Data: 11.5%	Remote Access Software: 10.6%		
	Stage Capabilities: 6.2%	Exploit Public-Facing Application: 7.9%	Windows Management Instrumentation: 8.9%	External Remote Services: 8.0%	Process Injection: 9.3%	System Binary Proxy Execution: 8.5%	Steal or Forge Kerberos Tickets: 10.0%	Network Share Discovery: 10.3%	Software Deployment Tools: 6.7%	Screen Capture: 11.5%	Praxy: 8.5%		System Shutdown/Rebo 11.1%
		Replication Through Removable Media: 2.6%	Exploitation for Client Execution: 7.1%	Event Triggered Execution: 6.0%	Exploitation for Privilege Escalation: 7.4%	Process Injection: 6.1%	Network Sniffing: 5.0%	System Information Discovery: 7.7%		Automated Collection: 7.7%	Encrypted Channel: 6.4%		
			Native API: 5.4%	Hijack Execution Flow: 6.0%	Event Triggered Execution: 5.6%	Subvert Trust Controls: 6.1%	Steal Web Session Cookie: 5.0%	Account Discovery: 5.1%		Video Capture: 7.7%	Non-Standard Port: 6.4%		
			Inter-Process Communication: 3.6%	Server Software Component: 4.0%	Access Token Manipulation: 5.6%	Modify Registry: 6.1%	Adversary-in-the-Middle: 5.0%	File and Directory Discovery: 5.1%		Adversary-In-the-Middle: 3.8%			
		Trusted Relationship: 2.6%	Software Deployment Tools: 1.8%	Boot or Logon Initialization Scripts: 2.0%	Hijack Execution Flow: 5.6%	Impair Defenses: 4.9%		System Network Connections Discovery: 5.1%		Data from Information Repositories: 3.8%			
					Abuse Elevation Control Mechanism: 3.7%	Access Token Manipulation: 3.7%		System Network Configuration Discovery: 5.1%		Clipboard Data: 3.8%			
					Boot or Logon Initialization Scripts: 1.9%	Hijack Execution Flow: 3.7%		Virtualization/Sandbox Evasion: 5.1%			Non-Application Layer Protocol: 2.1%		
						Abuse Elevation Control Mechanism: 2.4%		Domain Trust Discovery: 2.6%					
				Pre-OS Boot: 2.0%		Virtualization/Sandbox Evasion: 2.4%		Browser Information Discovery: 2.6%			Multi-Stage Channels: 2.1%		
						BITS Jobs: 1.2% Pre-OS Boot: 1.2%		Process Discovery: 2.6% Network Sniffing: 2.6%			Data Encoding: 2.1%		
						XSL Script Processing: 1.2% Hide Artifacts: 1.2%							
						Deobfuscate/Decode Files or Information: 1.2%							
						Execution Guardrails: 1.2% Rootkit: 1.2%							
						File and Directory Permissions Modification: 1.2%							



E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com

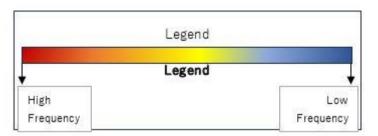


Figure 4: Column wise Heatmap (With Highest Priority)

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.

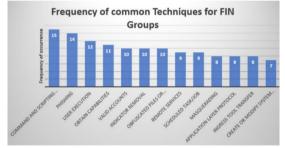


Figure 5: Top techniques used by FIN groups.

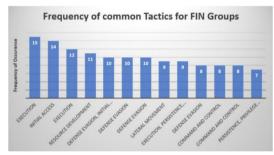


Figure 6: Top tactics used by FIN groups.

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	FrequencyTechnique	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]

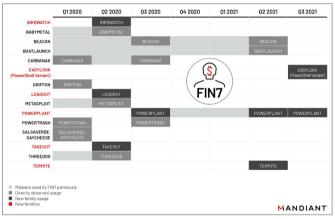


Figure 8: FIN7 Activity in 2020-2021

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

DISTRIBUTION OF RELATIONS								
416 Indicator	118 Attack Pattern	37 Malware						
16 Sector		7 Vulnerability						
4 Tool								

Figure 9: Distribution of Relations



3.2 Geo Victims and Target of FIN 7 team:



Based on the <u>thehackernews. com [5]</u> 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.

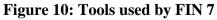
The highly active threat group, also known as Carbanak, is known for employing an extensive arsenal of tools and tactics to expand its "cybercrime horizons," including adding ransomware to its playbook and setting up fake security companies to lure researchers into conducting ransomware attacks under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

C	·	1								
FIN7	:	FIN7 SGOLD	NIAGARA 🗙 ITG14 🗙 Carbon Spide	er 😣 🕂					~	G
Q 56								4 entitie(s)		ᆂ
		ТҮРЕ	NAME	AUTHOR	CREATORS	LABELS	CREATION DATE	MARKING		
			PowerSploit	The MITRE Corpor	admin	No label	Oct 25, 2023, 11:47:45 AM	Copyright	;	>
			Mimikatz	The MITRE Corpor	admin	No label	Oct 25, 2023, 11:47:45 AM	Copyright	;	>
			CrackMapExec	The MITRE Corpor	admin	No label	Oct 25, 2023, 11:47:49 AM	Copyright	;	>
			AdFind	The MITRE Corpor	admin	No label	Oct 25, 2023, 11:47:44 AM	Copyright	;	>



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



E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u>

• Email: editor@ijfmr.com

V Intrus	sion sets	> Overview	Knowledge Analyses Data History					Q Search	⊈ [ੈ
			JSS Loader	The MITRE Corporation	admin	No label	Oct 25, 2023, 11:47:40 AM	Copyright	>
			IceBot	AlienVault	admin	(No label	Oct 25, 2023, 9:20:24 PM	TLP:CLEAR	>
			Нагру	AlienVault	admin	No label	Oct 25, 2023, 8:18:03 PM	TLP:CLEAR	>
			HALFBAKED	The MITRE Corporation	admin	No label	Oct 25, 2023, 11:46:43 AM	Copyright	
🗆 👳			HackTool:PowerShell/PowerSploit	AlienVault	admin	No label	Oct 25, 2023, 8:18:03 PM	TLP:CLEAR	>
			GRIFFON - S0417	AlienVault	admin	No label	Oct 25, 2023, 8:04:29 PM	TLP:CLEAR	>
□ 👳			GRIFFON	The MITRE Corporation	admin	No label	Oct 25, 2023, 11:46:41 AM	TLP:CLEAR	>
			FIN7	AlienVault	admin	No label	Oct 25, 2023, 8:19:52 PM	TLP:CLEAR	>
			Eamfo	AlienVault	admin	No label	Oct 26, 2023, 12:39:42 AM	TLP:CLEAR	>
□ 👳			Domeus VBS	AlienVault	admin	No label	Oct 25, 2023, 8:18:02 PM	TLP:CLEAR	>
			DiceLoader	AlienVault	admin	No label	Oct 25, 2023, 8:04:29 PM	TLP:CLEAR	>
□ 👳			DARKSIDE	AlienVault	admin	No label	Oct 25, 2023, 2:17:37 PM	TLP:CLEAR	
			Cobalt Strike	AlienVault	admin	(No label)	Oct 25, 2023, 11:34:33 AM	TLP:CLEAR	
□ 👳			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	>
৵		Carbanak	The MITRE Corporation	admin	No label	Oct 25, 2023, 11:47:07 AM	TLP:CLEAR	>
*		BOOSTWRITE	The MITRE Corporation	admin	(No label	Oct 25, 2023, 11:46:59 AM	Copyright	>
ঁ≹		BLACKMATTER	AlienVault	admin	No label	Oct 25, 2023, 8:08:36 PM	TLP:CLEAR	>
♦		BlackCat	The MITRE Corporation	admin	(No label)	Oct 25, 2023, 11:46:57 AM	TLP:CLEAR	>
♦		Black Basta	The MITRE Corporation	admin	No label	Oct 25, 2023, 11:47:13 AM	TLP:CLEAR	>
♦		BirdDog	AlienVault	admin	(No label)	Oct 25, 2023, 8:04:29 PM	TLP:CLEAR	>
\∳		Bella RAT	AlienVault	admin	No label	Oct 25, 2023, 12:11:19 PM	TLP:CLEAR	>
*		Bateleur	AlienVault	admin	No label	Oct 25, 2023, 8:18:02 PM	TLP:CLEAR	>
♦		BadUSB	AlienVault	admin	No label	Oct 25, 2023, 12:11:19 PM	TLP:CLEAR	>

V Intrusion	sets > Overview	Knowledge Analyses Data History					Q Search	\$ Ca
FIN7 :	FIN7 GOLD NIA	ITG14 Carbon Spider						< C
Q Search								36 entitie(s) 🔳 🔽 🛃
	түре	NAME	AUTHOR	CREATORS	LABELS	CREATION DATE	MARKING	
□ 😾		Tirion Loader	AlienVault	admin	No label	Oct 25, 2023, 12:11:19 PM	TLP:CLEAR	
		TEXTMATE	The MITRE Corporation	admin	No label	Oct 25, 2023, 11:46:45 AM	Copyright	
□ 😾		SQLRat	The MITRE Corporation	admin	No label	Oct 25, 2023, 11:47:14 AM	Copyright	
		Sekur	AlienVault	admin	No label	Oct 25, 2023, 8:18:02 PM	TLP:CLEAR	
		REvil	The MITRE Corporation	admin	No label	Oct 25, 2023, 11:47:23 AM	TLP:CLEAR	
□ 🔆		RDFSNIFFER	The MITRE Corporation	admin	No label	Oct 25, 2023, 11:46:41 AM	Copyright	
□ 😾		Pillowmint	AlienVault	admin	No label	Oct 25, 2023, 11:23:52 AM	TLP:CLEAR	
□ 😾		Mimikatz	AlienVault	admin	No label	Oct 25, 2023, 8:18:03 PM	TLP:CLEAR	
□ 👳		Lizar	The MITRE Corporation	admin	No label	Oct 25, 2023, 11:47:41 AM	Copyright	
□ 😾		Leo VBS	AlienVault	admin	No label	Oct 25, 2023, 8:18:02 PM	TLP:CLEAR	
□ 😾		KILIACK PS	AlienVault	admin	No label	Oct 25, 2023, 8:18:02 PM	TLP:CLEAR	
		JSSLoader	AlienVault	admin	No label	Oct 25, 2023, 1:01:12 PM	TLP:CLEAR	



E-ISSN: 2582-2160 • Website: www.ijfmr.com

• Email: editor@ijfmr.com

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

	sets > Overvie	ew Knowledge Analyses Data					Q FIN7		\$	Ê
FIN7 :	FIN7 S GOLD	NIAGARA 🗙 ITG14 🛞 Carbon Spid	er 🛞 🕂						٢	G
Q Search								7 entitie(s)		
	түре	NAME	AUTHOR	CREATORS	LABELS	CREATION DATE	MARKING			
o 🕺		CVE-2022-30190	Cybersecurity and	admin	No label	Oct 25, 2023, 4:24:4	4 PM TLP:CLEAR			>
o o		CVE-2021-42287	Cybersecurity and	admin	No label	Oct 25, 2023, 4:23:3	4 PM TLP:CLEAR			>
0		CVE-2021-42278	Cybersecurity and	admin	No label	Oct 25, 2023, 4:23:3	5 PM TLP:CLEAR			>
0		CVE-2021-34527	Cybersecurity and	admin	No label	Oct 25, 2023, 4:19:2	0 PM TLP:CLEAR			>
□ Ŭ		CVE-2020-14882	AlienVault	admin	No label	Oct 25, 2023, 12:45	01 PM TLP:CLEAR			>
□ Ŭ		CVE-2020-14750	Cybersecurity and	admin	No label	Oct 25, 2023, 4:19:4	7 PM TLP:CLEAR			>
□ ŭ		CVE-2020-1472	AlienVault	admin	No label	Oct 25, 2023, 12:20	19 PM TLP:CLEAR			>

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



E-ISSN: 2582-2160 • Website: www.ijfmr.com • Email: editor@ijfmr.com

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-	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion				
14750	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	In June 2021, FIN7 attacked a law firm with a fake complaint that appeared			
Brown-Forman Inc.	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	In 2020, one of its attacks, FIN7 sent out physical letters purportedly from			
Lure in the Form of	Best Buy, with a \$50 gift card and a USB drive, claiming to contain a list			
a Gift Card	of items to spend on. The USB was identified as a "BadUSB Leonardo			
Exchange	USB ATMEGA32U4" device, programmed to emulate a USB keyboard,			
	allowing it to automatically inject malicious commands once plugged in.			
Exploiting Veeam	A recent report highlighted FIN7's targeting of Veeam servers. The group			
Vulnerability	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 <u>Unit 42 report</u>, 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]

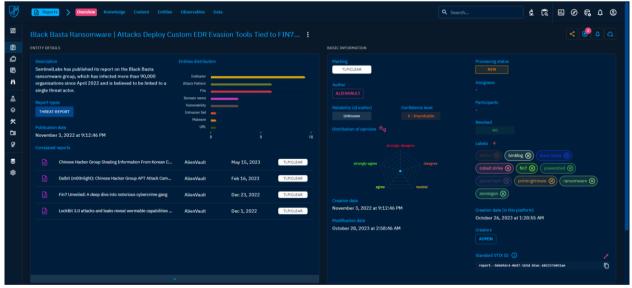


Figure 13: Black Basta Ransomware Info

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 <u>Black Basta Malware Sample Download</u> [8]. The Black Basta file information is as shown in the below figure:



E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> •

• Email: editor@ijfmr.com

ile Information (time: 0:00:03.112371)		File		Import function	
filename filetype filesize hash sha256 virustotal magebase entrypoint mphash latetime Hll lirectories sections features	723dlcf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224.exe PE32 executable (GUI) Intel 80386, for MS Windows 1489920 723dlcf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224 / 0x400000 0x237d9 e7481059b799ac586859298d4788584d 2016-04-20 18:01:43 False import, debug, tls, resources, relocations .rsrc, .text *, .rdata *, .data *, .reloc * mutex, antidbg, packer, crypto	UxTheme.dll SHLWAPI.dll PSAPI.DLL USER32.dll GDI32.dll COMDLG32.dll ADVAPI32.dll SHELL32.dll ole32.dll ntdll.dll COMTL32.dll	Library Library Library Library Library Library Library Library Library Library Library Library	SHLWAPI.dll PSAPI.DLL USER32.dll GDI32.dll COMDLG32.dll ADVAPI32.dll SHELL32.dll ole32.dll ntdll.dll COMCTL32.dll	35 2 136 155 10 3 18 8 1 8 1 8

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.

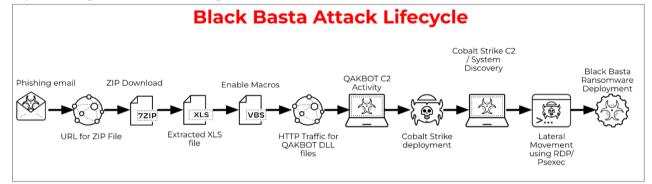


Figure 15: Black Basta Attack Lifecycle

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. <u>https://bazaar.abuse.ch/sample/3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e139</u> <u>daa/ [10]</u>

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



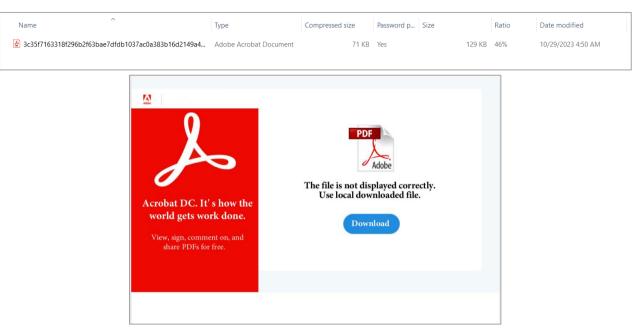


Figure 16: Qakbot Malware Sample

4.2.3 Qakbot/QBot Infection chain

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

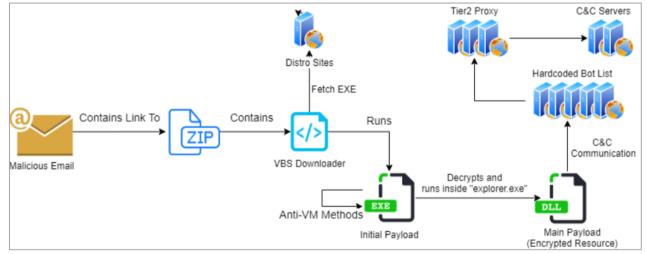


Figure 17: Qakbot infection chain

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.



	1
Re: Keep Your Business Moving During COVID-19	RE: 7 April Tax Due Reminder
100000000000000000000000000000000000000	
	KR 21/04/2020 0.13
Good menning,	Tax Tax Agents - Northern
Ondithe desirent and let no large which you think about it.	
A SUBJURIT BURNLOND	Hella,
	Sorry, for my late reply to your question. Attached is the document you need.
Tans	ATTACIMENT DOWNLOAD
	Bhaok you,
н,	
These are break threa. With COMD-10 crisis all across the country and work, tole marketing and field marketing may be out of equation right new. The best way to market right new is email automation. A list of our cleans have entered this channel (small marketing) to market the downful in the current Commanus have:	
	Greetings
	Please read the attached update regarding tax payment reminders to clients of tax agents for 7th April liabilities.
	Kind Regards Tax Agent work group
mitopol.	This email and any attachment may contain confidential information. If you have received this email or any attachment in error, please dotes the email / attachment, and rotify the senders. Please do not copy, dickise or use the email, any attachment, or any information constained in them. Consider the environment before deciding to print: avoid printing if you can, or consider printing adveloariable, which is consist end ingo dura.

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.

1				0	1
remnux@remnux:~/Dov					
3c35f7163318f296b21					
3c35f7163318f296b21					
7z2301-x64.exe					
malware_samples					
<pre>malware_samples.zip</pre>					
Unit42-Wireshark-tu					
Unit42-Wireshark-tu					
				b1037ac0a383b16d2149a	455970a8e139daa.pdf
PDFiD 0.2.8 3c35f7		63bae7dfdb1037ac	0a383b16d2149a455	970a8e139daa.pdf	
PDF Header: %PDF-:					
obj	90				
endobj	90				
stream	35				
endstream	35				
xref	1				
trailer	1				
startxref	1				
/Page	9				
/Encrypt	Θ				
/ObjStm	0				
/JS	0				
/JavaScript	0				
/AA	0				
/OpenAction	0				
/AcroForm	0				
/JBIG2Decode	0				
/RichMedia	0				
/Launch /EmbeddedFile	0 0				
/EmbeddedFile /XFA	0				
/VRI	2				
/Colors > 2^24	0				
700015 > 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 <u>https://ourloverlyday.us/xuenxavleu/xuenxavleu.gif</u>

Strings: "3C35171653181296627636827610618378C9838301602149845597088 [remnux2emnux:-/Downloads\$ strings 3C35f7163318f29662f63bae7dfdb103 %PDF-1.4	
<>	
<pre>cmousy 3 0 obj <>/Border[0 0 0]/C[1.0 1.0 1.0]/ endobj [3 0 R] endobj 5 0 obj <>stream ,v?? 4=j; ,le(H</pre>	H/N/Rect[421.013 178.676 671.064 307.214]/Subtype/Link/Type/Annot>>
q>B9	



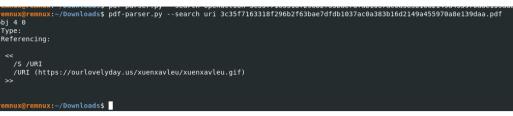


Figure 20: Qakbot URL from PDF.

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

URLhaus Datab	ase
	database entry for https://ourlovelyday.us/xuenxavleu/xuenxavleu.gif which is being or has been used to serve malware. Please ntiate between websites that have been compromised by hackers and such that has been setup by cybercriminals for the sole purpos
Database Entry	
	Actions ~
ID:	2669875
URL:	🗘 https://ourlovelyday.us/xuenxavleu/xuenxavleu.gif
URL Status:	Offline
Host:	🗘 ourlovelyday.us
Date added:	2023-06-22 20:43:11 UTC
Last online:	2023-07-07 06:XX:XX UTC
Threat:	兼 Malware download
URLhaus blocklist:	Not blocked
Spamhaus DBL 🔀:	Not blocked
SURBL 🔁:	Not blocked
Quad9 🔀:	Not blocked
AdGuard 🔀:	Not blocked
Cloudflare 🖄	Not blocked
dns0.eu 🔀:	Blocked in
ProtonDNS 🗹:	Blocked u
Reporter:	Cryptolaemus1
Abuse complaint sent (?):	■ Yes (2023-06-22 20:44:19 UTC to abuss{at}shinjiru[dot]com[dot]my)
Takedown time:	14 days, 10 hours, 0 minutes () (down since 2023-07-07 06:45:17 UTC)
Tags:	geofenced js obama271 Qakbot @ gbot @ Quakbot @ TR USA

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.



E-ISSN: 2582-2160 • Website: www.ijfmr.com

• Email: editor@ijfmr.com

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	C 749699a9a6198e917dd0b9dbb3769324cffe1f7bb570a8540c06b229ec0909c6	▶ 28.33%		Quakbot
2023-07-05	BSN-648582479.zip	zip	D024ce0a34460f5a2ef82eeec406ee7defceb35a0aabc01ca5a24e8a09cfd967	n/a		Quakbot
2023-07-05	BSN-501648987.zip	zip	C 5e8e7b6687497d6f8aa278bfef0f825927759060d6955f0496be228a7f944a26	n/a		Quakbot
2023-07-04	BSN-1646570560.zip	zip	D 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	B97e6afd069d468269a4c493952e2b414cd83d49712c1f928fb18bbb91ceca9d	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	C 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	D 324ecc452159dc7251b19ef7bbd02d1b0113334b004d5894621877757570e6e5	n/a		Quakbot
2023-06-29	BSN-1078355438.zip	zip	🖞 d826265925f1704175d602a2315f0b862ebff91b8fa416da05447326ebde83d6	n/a		Quakbot
2023-06-28	BSN-659637643.zip	zip	C e7cf94c3f525b788bb52722aa6f61767cdbd1ec6b44a8ae7a1fb5956f4bdd488	n/a		Quakbot
2023-06-28	BSN-989333913.zip	zip	D 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	t469f796392ba10987bb447c6a249bf9b395849ee82f5248e5448fcef3f4f065	n/a		Quakbot
2023-06-25	BSN-964842713.zip	zip	C 5b35ec8c3277149d86353a3407414ec33d715d9a18881a5838011b1f913d3cf4	▶ 8.06%		Quakbot
2023-06-25	BSN-1403099197.zip	zip	4832606a5235277811f9243f036885c41825a0f74309c249a664f3a7cdf6b8e2	n/a		Quakbot
2023-06-24	BSN-100766691.zip	zip	Dea70bb3993e40bd39029f71440b3ecfc251f6313579f0a8dec608bac8fdf48b5	n/a		Quakbot
2023-06-24	BSN-2107257244.zip	zip	91973073c084e89b8aa29a941ceac6862d67807deacf28b88f33a195065ac383	n/a		Quakbot
2023-06-23	BSN-39797926.zip	zip	D be4fcaf606d0ba10b0c03e0a79d22e624eca1f0958eba5d7060c07a657312061	n/a		Quakbot
2023-06-23	BSN-1841259078.zip	zip	D 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.



	Keep your software <a awsapmhyutwltjelmzpfbag="" class="white Y3GPJvUizL0gfOmqkXgk" col-lg-9="" href="https</p></th></tr><tr><td>-</td><td></div></td></tr><tr><td>-</td><td></div></td></tr><tr><td></td><td><pre><div class=" pmyfkrlvm_2tciao82al"=""> <div class="ps-2 mt-2"></div>
- <scrip< td=""><td>t language="javascript"></td></scrip<>	t language="javascript">
</td <td></td>	
docume //>	nt.write(decodeURIComponent('\$20\$20\$20\$20\$20\$20\$20\$20\$20\$20\$20\$20\$20\$
- <td>pt></td>	pt>
- <scrip< td=""><td>t type="text/javascript"></td></scrip<>	t type="text/javascript">
doguma	nt artDiementBuild/Manuell stule misibility - Meisibie//
docume	<pre>nt.getElementById("app").style.visibility = "visible";</pre>
-	
var te	xt = 'UEsDBA0AAAAAAA2W61QAAAAAAAAAAAAAAAAAAAAAAAJUXOC9TRHEAwAAAAAAIAHUOoa1jZGBpEWFgYDBggAAfIGZkBTNZRYFESXNsu
var te var co	<pre>xt = 'UEsDBAoAAAAAAA2W61QAAAAAAAAAAAAAAAAAAAAAAAJUxOC9TRHEAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>
var te var co var ta	<pre>xt = 'UEsDBAAAAAAAA2W61QAAAAAAAAAAAAAAAAAAAAAAAAJUxOC9TRHEAwAAAAAAAAAAAAAAAAAAA mtent_type = 'application/zip'; rget_file_name = 'IXRN_2636021.zip';</pre>
var te var co var ta jf(!na	<pre>xt = 'UEsDBAAAAAAAF2W61QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>
var te var co var ta -if(!na ta	<pre>xt = 'UEsDBAAAAAAAA2W61QAAAAAAAAAAAAAAAAAAAAAAAIYAMjUxOC9TRHEAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>
var te var co var ta jf(!na	<pre>xt = 'UEsDBAAAAAAAF2W61QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>
var te var co var ta -if(!na ta	<pre>xt = 'UEsDBAAAAAAAF2W61QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>
var te var co var ta if(!na ta -}	<pre>xt = 'UEsDBAAAAAAAF2W61QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>
var te var co var ta if(!na ta -}	<pre>xt = 'UEsDBAAAAAAAF2W61QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>
var te var co var ta if(!na ta -}	<pre>xt = 'UEsDBAAAAAAAF2W61QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>
var te var co var ta if(!na ta -} var _0 - <td><pre>xt = 'UEsDBAAAAAAAF2W61QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre></td>	<pre>xt = 'UEsDBAAAAAAAF2W61QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>
var te var co var ta if(!na ta -} var _0	<pre>xt = 'UEsDBAAAAAAAF2W61QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>
var te var co var ta if(!na ta -} var _0 - <td><pre>xt = 'UEsDBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre></td>	<pre>xt = 'UEsDBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>

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.

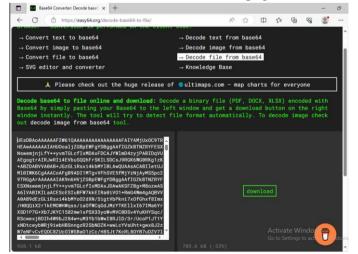


Figure 24: Stage 1- Download ZIP file



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.

917	
918	oAAAANSUhEUgAAARgAAAERCAYAAACggbhEAAAAAXNSR0IArs4c6QAAJaBJREFUeAHtnQe4HkW5xxNASSgJICUJJSEgNTTpUhOQgIAUQYqI1AsIyL16
919	3w">Acrobat DC. It's how the world gets work done.
920	b">View, sign, comment on, and share PDFs for free.
921	-
922	
923	
924	Gojpso">
925	
926	in-top: 100px; margin-bottom:100px">
927	c="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAIAAACACAYAAADDPmHLAAAIx01EQVR42u3dCXATVRgH8JSCXOONMkpTSitHBREPR
928	
929	size: 32px;">The file is not displayed correctly. Use local downloaded file.
930	-
931	
932	size: 30px;">Document password: abc321
933	

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.

Extract : C:\Users\Parames\Documents\P	OC\download.zip X
Extract to:	
C:\Users\Parames\Documents\POC\	×
download\	Password
Path mode:	abc321
Full pathnames	Show Password
Eliminate duplication of root folder	
Overwrite mode:	Restore file security
Ask before overwrite	×
	OK Cancel Help

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.

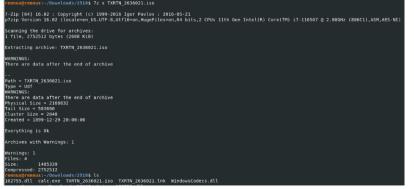


Figure 27: Stage 2- Extracting the files from the ISO.



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.

< > ☆ Home	Downloads application (8)	2518 👻	۹ 🗉 🔹	≡ _ □ ×
⊘ Recent				
🗙 Starred				
🔂 Home	102755.dll	calc.exe	TXRTN_2636021.iso	TXRTN_2636021.lnk
Documents	102/ 55.44	cute.exe	1711112030021.30	TARTN_2050021.00K
↓ Downloads				
J Music				
Pictures	WindowsCodecs.dll			
▶ Videos				
🔟 Trash				
🖿 ss				
+ Other Locations				

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.dl	ll Library



E-ISSN: 2582-2160 • Website: www.ijfmr.com • Email: editor@ijfmr.com

Behavior	
Check OutputDebug anti dbg Xor screenshot keylogger win registry	gStringA iat
Mutex Api	
WaitForSingleObje	
Anti Debug	
FindWindowW GetLastError OutputDebugString RaiseException TerminateProcess UnhandledExceptio	
Sections Suspicio	bus
.text .rsrc .reloc	6.40 7.54 6.74

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.

======= TXRTN_2636021.lnk ExifTool Version Number File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Type File Type Extension MIME Type Flags File Attributes Create Date Access Date Modify Date Target File Size Icon Index Run Window Hot Key Target File DOS Name Drive Type Volume Label	<pre>: 2023:10:28 12:40:50-04:00 : 2023:10:28 08:43:30-04:00 : -rw-rw-r : LNK : application/octet-stream : IDList, LinkInfo, CommandArgs, IconFile, Unicode, ExpIcon : Archive : 2021:10:11 15:30:04-04:00 : 2022:07:07 15:29:19-04:00 : 2021:10:11 15:30:04-04:00 : 289792 : (none) : Show Minimized No Activate : (none) : cmd.exe : Fixed Disk :</pre>
Local Rase Path	: · C·\Windows\Svstem32\cmd_eye
Command Line Arguments Icon File Name	: /q /c calc.exe : C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
======= WindowsCodecs.dll	: yalaxyszi

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.

Process Moni	tor - Sysinternals: www	esysinternals.com					\times
File Edit Event	Filter Tools Option	is Help					
2 🛛 🖓 🖾 🖸	700 *	S P 7 📑 🖬 🗣	° 🗛				
Time of Day	Process Name	PID Operation	Path	Result	Detail		
09 37 5487945	calc exe 1	596 🚔 QueryBasicInfor	C Windows/SysWOW6/twinmm dll	SUCCESS	CreationTime: 6/10/		
09 37 5487989			C:Windows(SysWOW64)version.dll	SUCCESS	CreationTime: 6/10/		
09.37.5487999	calc exe 1	596 🐂 CreateFileMapp.	C Windows WinSxSix86 microsoft windows common-controls 6595b64144ccf1df 6.0	FILE LOCKED WIT	SyncType SyncTyp		
09.37.5488085		596 R CloseFile	C.Windows/SysWOW64/version.dll	SUCCESS			
09 37 5488157	calc.exe 1	596 🐂 CloseFile	C/Windows/SysWOW640winmm dll	SUCCESS			
09.37.5488441			C.Windows/WinSxSix86 microsoft windows.common-controls 6595b64144ccf1df 6.0		SyncType SyncTyp		
1 09 37 5491346	calc exe 1	596 ge Load Image	C Windows/WinSxSix86 microsoft windows common controls 6595b64144ccf1df 6.0	SUCCESS	Image Base: 0x74ff		
09.37.5494017		596 🐂 CloseFile	C:Windows/WinSxSix86 microsoft windows.common-controls 6595b64144ccf1df 6.0				
1 09 37 5497673	calc exe 1	596 📻 CreateFile	C Windows/SysWOW64/version dll	SUCCESS	Dosirod Access: R		
09 37 5499016			C:Windows/SysWOW64/version.dll	FILE LOCKED WIT.	SyncType SyncTyp		
1 09 37 5499193		596 🐂 CreateFile	C Windows/SysWOW64hwinnm dll	SUCCESS	Desired Access: R		
09-37 5499235			C:Windows/SysWOW64/version.dll	SUCCESS	SyncType SyncTyp		
1 09 37 5500089			C.Windows/SysWOW64twinmm dl	FILE LOCKED WIT.			
09 37 5502 153			C:\Windows\SysWOW64\winmm.dll	SUCCESS	SyncType SyncTyp		
09 37 5502372			C Windows/SysWOW6/Ivorsion dll	SUCCESS	Image Base: 0x74f		
09 37 5503269			C:Windows/SysWOW64/winmm dli	SUCCESS	Image Base: 0x747		
1 09 37 5504017		596 📻 CloseFile	C \Windows\SysWOW64\version.dll	SUCCESS	toninge out of and the		
09:37.5505804			C:Windows/SysWOW64/winmm dll	SUCCESS			
09.37.5521938		596 🐂 CreateFilo	C \Windows\SysWOW64\mm32 dl	SUCCESS	Desired Access: R		
09 37 5522255			C Windows/SysWOW64/imm32 dl	SUCCESS	CreationTime: 6/10/		
09 37 5522352		596 🙀 CloseFile	C:Windows/SysWOW6/fimm32.dll	SUCCESS	Green and a second second		
09 37 5523825		596 The CreateFile	C:Windows/SysWOW64/imm32.dll	SUCCESS	Desired Access: R		- 1
09 37 5524353			C \Windows\SysWOW64\imm32 dll	FILE LOCKED WIT.			
09 37 5524554			C:Windows/SysWOW64/imm32.dll	SUCCESS	AllocationSize: 143		
09 37 5524941			C WindowsiSysWOW64/imm32 dl	SUCCESS	SyncType SyncTyp		
09 37 5525772		596 CloseFile	C:Windows/SysWOW64/imm32.dll	SUCCESS	cheering cheering		
09-37 552 7570			C Windows/SysWOW8/Imm32 dl	SUCCESS	Image Base: 0x761		
09 37 5650138			C Users/REM/Deskton/WindowsCodecs dl	NAME NOT FOUND			
09.375656489			C Windows/SysWOW6//WindowsCodecs dll	SUCCESS	Desired Access R		
109:37.5656721			.C:Windows/SysWOW64/Windows/Codecs.dll	SUCCESS	CreationTime: 6/10/		
09 37 5656810		596 CloseFile	C \Windows\SysWOW64\WindowsCodecs dll	SUCCESS			
09 37 5658496		596 🙀 CreateFile	C:WindowsiSysWOW64/WindowsCodecs.dll	SUCCESS	Desired Access: R		
09 37 5658907			C Windows/SysWOW6/I/Windows/Codecs dll		SyncType SyncTyp		
09 37 5659333			C/Windows/SysWOW64/WindowsCodecs.dll	SUCCESS	SyncType SyncTyp		
09.37.5661345		596 o ^o Load Image	C\Windows\SysWOW64\WindowsCodecs.dl	SUCCESS	Image Base: 0x742		
09:37.5664442			C:WindowsiSysWOW54bcrypt.dll	SUCCESS	Image Base 0x75c		
		596 🙀 CloseFile	C:Windows/SysWOW64/WindowsCodecs.dll	SUCCESS	mage case over de		
	Contraction (and the constant and	Contraction of the contraction o				

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 filesize hash sha256 virustotal imagebase entrypoint imphash datetime dll directories sections features	WindowsCodecs.dll PE32 executable (DLL) (GUI) Intel 80386, for MS Windows 4608 6e3661049bde832369781afa1d9034315442b1e4b87aa92d571cbe73186997c5 / 0x100000000 * 0x1080 87a1f1c5766b04416c137412a6152760 2022-07-11 14:15:55 True import, export, tls, resources, relocations .text, .rdata, .data, .rsrc, .reloc antidbg, packer			

6e3661049bde832369781afa1d9034315442b1e4bd	87aa92d871cba73386997c5	Q 🛧 🇱 🌻 😋 Shivang Srivastava 🕥 *
. 52	52 security vendors and 1 sandbox flagged this file as malicious	(^ Reanalyze
	6836610490d6832369781sfa1890034315642b1e4b87ea92d571cbe7318699765 WindowsCodeos.dl	Size Last Analysis Date 4.50 KB 5 months ago
Community Score	pedi spreader	
DETECTION DETA	ALS RELATIONS BEHAVIOR COMMUNITY 25+	
Import function		
KERNEL32.dll		
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.



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
XLMMacroDeobfusc	ator: 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	0×400000
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.

http: http: http: http: https	<pre>//crt.sectigo.com/Se //crl.sectigo.com/Se //crl.usertrust.com/ //crt.usertrust.com/ //ocsp.sectigo.com0 ://sectigo.com/CPS0 //ocsp.usertrust.com</pre>	ectigoRSATimeStampin /USERTrustRSACertif /USERTrustRSAAddTrus	ngCA.crl0t icationAuthori	ty.crl0v	
ptr:91.199.2	212.90 Find Problems				C pt
		Domain Name		m	Øp
Туре	212.90 Find Problems IP Address 91.199.212.90 Usteen (Add447)	Domain Name no-dro-yet ccanet co uk		TTL 24 hrs	Op
ttr:91.199.2 Type PTR	IP Address 91 199 212 90		Result		Qt
Туре	IP Address 91 199 212 99 Unitroam (A548447)		Result DNS Record found		Ø
Type PTR	IP Address 01199212 50 University (Addd47) Test	no-dres-yet ocanet co uk subnet tool			
Type PTR Composition	IP Address 91 192 22 29 Unexer: (AddRer) Test DNS Record Published S3.as46447.net on 10/28/2023 at 11:22:34 AM (UTC -9). <u>Nat Ex</u>	no-dres-yet ocanet co uk subnet tool	DNS Record found		Transc
ype PTR mtp diag eported by ns :sectigo.c	IP Address 91 192 22 29 Unexer: (AddRer) Test DNS Record Published S3.as46447.net on 10/28/2023 at 11:22:34 AM (UTC -9). <u>Nat Ex</u>	no-dres-yet ocanet co uk subnet tool	DNS Record found		Transc
Fype PTR Introduced by ns	IP Address 91 199 212 20 Ummere (ASB447) Test DNS Record Published StartMet On 10/26/2023 at 11:22:34 AM (UTC -8), <u>Not 50</u> com	no-dre-yet ccanet co uk subnet lost	DNS Record found	24 hrs	Transc
Fype PTR Into dag eported by ns :sectigo.c	IP Address 91 199 22 29 Ummer (AddRes) Test DNS Record Published as Jas48447, net on 10/28/2023 at 11:23:34 AM (UTO -8) <u>1001 59</u> com Domain Name	no-dre-yet ccanet.co.uk subnet tost LVSS: IP Address 01.199.212.00	DNS Record found	24 hrs	C I Transc

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.

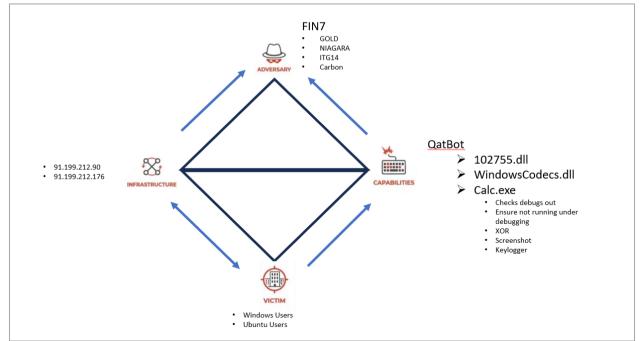


Figure 36: Qakbot Diamond Model



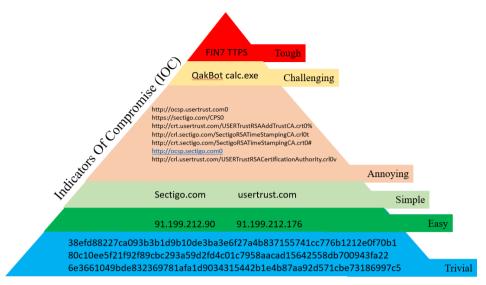


Figure 37: Pyramid Of Pain

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

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"
```

IJFMR

E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com

```
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
```

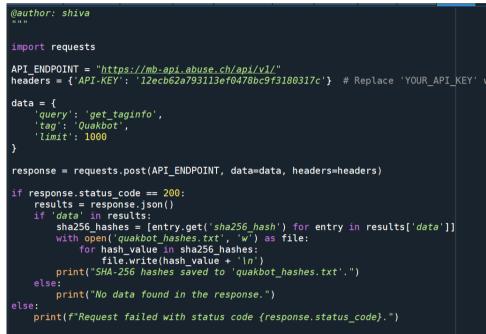
```
}
```



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,



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.

<pre>import requests import pandas as pd API_ENPOINT = "https://wh-api.abuse.ch/api/v1/" API_KEY = "api.abuse.ch/api/v1/" headers = {'AFI-KEY' : '12eCb62a793113ef6478bc9f3180317c'} # Replace with your</pre>	actual API key
<pre>with open('quakbot_hashes.txt', 'r') as file: data = file.read()</pre>	
<pre># Split the data into individual lines (assuming each line contains one hash) hash list = data.strip().split('\n') hashes_hash list #hashes = ["906e3977e1e40cba19d5be5bbc194fd72131e019febae55ba82e91ea3ca28d19",' first_seen_list = [] delivery_method= [] file_type[list = [] delivery_method=[] i=1</pre>	775ca69b395e7d228e5326cfbbd6a47b2455e743c684050317749cff6eec9150°]
"hash": hašh_value, H	
headers = {"API-KEY": API_KEY}	
response = requests.post(API_ENDPOINT, data=data, headers=headers)	
<pre>if response.status_code == 200: response.status_code == 200: # Process the result as needed #print(result) print(i) i=-1 for item in result['data']: for item in result['data']: first_seen_list.append(item['first_seen']) last_seen_list.append(item['last_seen'])</pre>	
<pre>file_type_list.append(item('file_type']) delivery_method.append(item['delivery_method']) sha256_hash.append(item['sha256_hash'])</pre>	
else: print(frRequest 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_
<pre># Save to Excel df.to_excel('output.xlsx', index=False)</pre>	



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							
-	9 15:28:43				e1e40cba	19d5be5b	bc194fd721	31e019feba	ae55ba82e	91ea3ca28	d19
2023-10-1	2023-10-2	zip	_					56e743c684			
2023-09-0	7 18:32:30	Ink		8f5fa78c2	b92c3f4b	0ce7ae1b4	adca6e895	d6bf32e3c1	1a8a604ca	48bbdab1	12
2023-08-2	5 01:11:58	7z		3f004293	165057ac4	40d7d2dc6	63cc62c87	ebe296012	51dcca24b	6aa1062b7	7af
2023-08-1	8 10:40:24	js	email_atta	eec3dce6	ca41b665	70a08433a	5a9b9b2a1	.cffb037b52	55bd589cc	f089c12e8	ac
2023-08-1	8 03:26:20	dll		7ee6095b	a8c4ed9f	e11fbf5e7()3823e1aea	e7f544302	7738f55979	b27ca5717	71
2023-07-1	1 10:43:21	js		66f6ac4a4	1950397df	f2f012b7eb	4d6576d1	dff9629a17	5677786c44	4596715b9 [.]	f9
2023-07-1	0 09:31:25	dll		4c7d5ae6	fefb8f53e	0f557a241	f95a67748	2bc4219c1d	91573425e	bc0cb4483	80
2023-07-1	0 09:31:17	js		cf5295f7c	653e106b	cf8367feb	1daa26144 ⁻	f94e7721f08	840d2c61f0	ec7bd33c4	1
2023-07-1	0 09:31:11	zip	web_dow	749699a9	a6198e91	7dd0b9db	b3769324c	ffe1f7bb570	Da8540c06b	229ec0909	9c6
2023-06-2	5 07:05:26	dll		7619db1c	beef2ec3	8d180fdd9	fecb8dd87	76c90b6c19	41e4f685c0)a9b03b13	43
2023-06-2	3 19:35:13	js		88590eb8	1c23e50c	1a52a49e4	8b37b5bc7	2ead1868c	a45adc4ffe	5c8485a96	526
2023-06-2	3 19:34:52	js		be26c5d7	a70cc3ea	46138c2ef3	3b589a381	d61a9aaabo	150ad9b80	95d80f826	0d9
2023-06-2	3 19:34:31	js		dbc19813	9b9f4ecb	e0170b51c	2e802873a	c2e98db5d	0f8fef6913	c2f01e82e4	41
2023-06-2	3 19:34:05	js		c68f6540	59443159	95c84bc34	5c28a7d73	o797ae8b00)7352ccb48	ddaecf03f	ee
2023-06-2	3 19:33:41	js		2270d9b0	8ecb65e0	1b8a490d	ede9b1480	431bdfaa05	2cecc54a1	231fe56e6	55a
2023-06-2	3 19:32:05	dll		457c622b	a31de68f	44d01c63d	e335b32cc	7ef2cbbf6c4	48a2acdd86	58a28ddba	97
2023-06-2	3 19:31:24	dll		8386c26e	f88062db	37966613a	c32debe4e	c5be1e44ea	a42ae89d8	ad7fbf3f83	le5
2023-06-2	2 10-20-51	All		00480062	50-1051-0	foisbosb	450036365	50af0ba56b	0710225.af	002f18/82	0d

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.

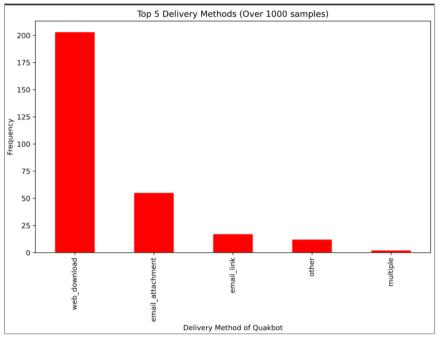
```
# -*- coding: utf-8 -*-
"""
Created on Sun Oct 29 03:15:36 2023
@author: shiva
"""
import pandas as pd
import matplotlib.pyplot as plt
# Reading the CSV
df = pd.read_excel('output.xlsx')
# Extracting the 'Delivery Method' column
delivery_methods = df.iloc[:, 3]
# Counting frequencies
delivery_counts = 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.

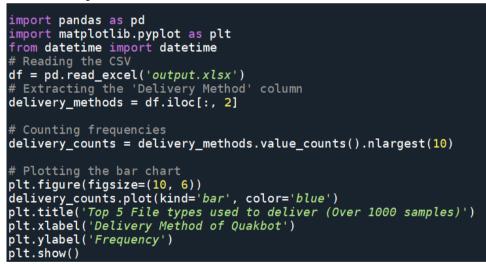
- 1. Web_download
- 2. email_attachment
- 3. email_link
- 4. other
- 5. multiple



Refer the below figure for the generated chart.

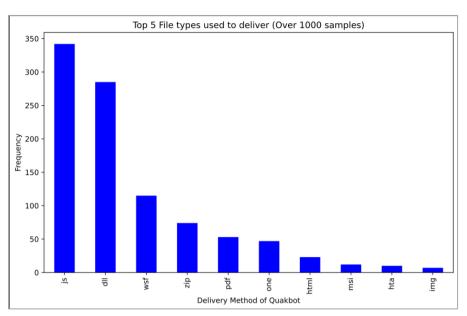


5. With the information gathered in excel, we plotted the delivery method for Qakbot. The below figure shows the code used to plot the chart.



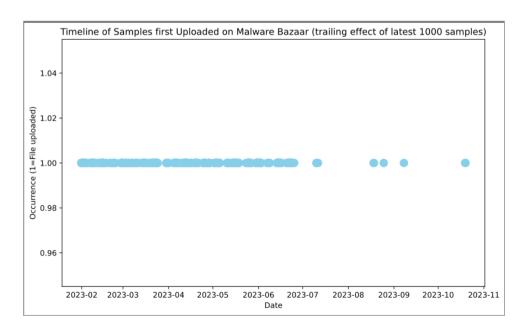
The most common file types used to deliver Qakbot are represented in the below chart.

E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com



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

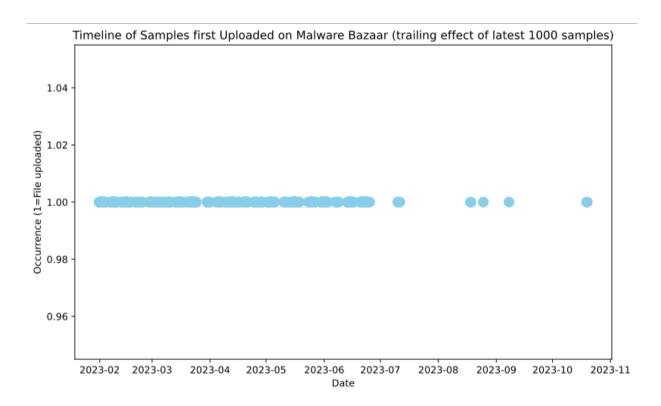
```
df = pd.read_excel('output.xlsx')
# Extracting the dates from the first column
dates = pd.to_datetime(df.iloc[:, 0])
# Creating a list of 1s to represent the presence of an entry on that date
values = [1] * len(dates)
# Creating scatter plot
plt.figure(figsize=(10, 6))
plt.scatter(dates, values, 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.ylabel('Occurrence (1=File uploaded)')
plt.show()
```





E-ISSN: 2582-2160 • Website: www.ijfmr.com

• Email: editor@ijfmr.com

Mitigations for the identified Techniques 8.0

Techniq ue ID	Freque ncy	Technique	Tactic			Mitigations	[2]			1
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 <u>block web</u> 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 <u>Reduction rules</u> 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, Persisten ce, 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)
Techniq	Freque	Technique	Tactic			Mitigations	[2]			
ue ID	ncy	1990 				2	een e	<u>, </u>		
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, q uestionable files can be au tomatically identified and q uarantined. 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 Movemen t	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, Persisten ce, 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.			



E-ISSN: 2582-2160 • Website: www.ijfmr.com

• Email: editor@ijfmr.com

Techniq ue ID	Freque ncy	ncy	ncy Masqueradi	e Technique	Technique	Technique	Technique	Tactic			Mitigations	[2]		
T1036	8			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#S ystem32.					
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)



E-ISSN: 2582-2160 • Website: www.ijfmr.com

• Email: editor@ijfmr.com

8	Entities	Relationships Ingestion	Processing Data sharing	Connectors	Q Search	.	\$ C II Ø 6 4 0
88							
Ê		Workers statistics	701.46K	0/s	7 4/2	200/6	19.96M
Ċ		CONNECTED WORKERS	QUEUED BUNDLES	BUNDLES PROCESSED	7.4/s read operations	200/s WRITE OPERATIONS	TOTAL NUMBER OF DOCUMENTS
85 /1							
۵	ង	Registered connectors					
\$		NAME 🔻		түре	AUTOMATIC TRIGGER	MESSAGES	MODIFIED
*	ង	Abuse.ch SSL Blacklist		Data import		94	Oct 27, 2023, 1:19:31 AME _x
Ŷ	ದ 	Abuse.ch URLhaus		Data import		60.21K	Oct 28, 2023, 9:01:08 AME 🗙 🗍
9	<u>ಬ</u>	AbuseIPDB		Enrichment			Oct 27, 2023, 1:19:31 AME 🗙 📋
鐐	ದ	AlienVault		Data import		223	Oct 27, 2023, 1:19:31 AME,
	ង	CISA Known Exploited Vulne	erabilities	Data import			Oct 27, 2023, 1:19:31 AME _
	ង	Chapsvision		Data import			Oct 26, 2023, 10:55:51 PBx 📋
	ង	Citalid		Data import	NOT APPLI	0	Oct 27, 2023, 1:19:31 AME 🗙 📋
8	Entities	Relationships Ingestion	Processing Data sharing	Connectors	Q Sear	ch	\$ C II 0 6,
88	ង	Common Vulnerabilities and	d Exposures	Data import			Oct 27, 2023, 1:19:31 AME _
Ê	ລ	ExportFileCsv		Files export			Oct 27, 2023, 1:19:31 AME _
٥	ລ	ExportFileStix2		Files export			Oct 27, 2023, 1:19:31 AME,
85 #1	ລ	ExportFileTxt		Files export			Oct 27, 2023, 1:19:31 AME,
۵.	ລ	Hybrid Analysis (Sandbox W	vindows 10 64bit)	Enrichment		106.58K	Oct 27, 2023, 1:19:31 AME _ □
⊉ \$	ມ ເມ	ImportCsv		Files import		0	- =
*	ມີ ເ	ImportDocument		Files import		0	Oct 27, 2023, 1:19:31 AME _
⊡ ₽	ລ	ImportFileStix		Files import		0	Oct 27, 2023, 1:19:31 AM=, □
9	ມ ເມ	MISP		Data import		448.93K	Oct 28, 2023, 9:02:30 AME
鐐	ີ ລ	MISP Feed		Data import		0	Oct 27, 2023, 1:19:31 AME,
	ີ ລ	MITRE Datasets		Data import		0	Oct 27, 2023, 1:19:31 AME,
	ີ ລ	MalwareBazaar Recent Addi	iitions	Data import			Oct 27, 2023, 1:19:31 AME,
	ົລ	OpenCTI Datasets		Data import			Oct 27, 2023, 1:19:31 AME
3							
鐐	ដ	OpenCTI Elastic Connector		Streaming			Oct 28, 2023, 9:03:18 AME _× □
	<u>ل</u> ک	Shodan		Enrichment			Oct 28, 2023, 9:03:22 AME _× ☐
	<u>ධ</u>	VirusTotal		Enrichment		85.41K	Oct 27, 2023, 1:19:31 AME _x
	ង	YARA		Enrichment			Oct 27, 2023, 1:19:31 AME _x
8	Dashboa	rd ŵ			Q Search	h	\$ C III @ E,
	TOTAL E	NTITIES		ATIONSHIPS	TOTAL REPORTS		BSERVABLES
۵ ۲	37	7.05K + 2 (24 hours)	■ 482.	82K 🗠 2 (24 hours)	2.71K → 0 (24 hours)	143	3.03K ↑1 (24 hours)
₿	TOP LABEL	S (3 LAST MONTHS)		INGESTED ENTITIES			
A		13K 31.11I	K 23.31K	450 K			
& ⊗		phishing	blog-post	360 K			
*		13K 15.27	K 15.09K	270 К			/
⊡ ⊋		451A 15.271 qbot	dridex	180 K			
	15.0	02K 14.28					
∰ ₩	qakbol			0 F Oct 2022 Nov 2022 Dec 20	1 I I 022 Jan 2023 Feb 2023 Mar 2023 Apr	1 I I 2023 May 2023 Jun 202:	3 Jul 2023 Aug 2023 Sep 2023



E-ISSN: 2582-2160 • Website: www.ijfmr.com

TOP 10 AC	TIVE ENTITIES (3 LAST MONTHS)				TARGETED COUN	TRIES (3 LAST MONTHS)		
Ransom:W	Axiom trike - 50154 QukBot Dridex Egregor Quakbot Guakbot in32/Egregor Quakbot Emotet 0	эк	18 K		sufi Kores wit COSWER	Const Const	tring language	Conset
LAST ING	STED REPORTS (CREATION DATE IN	I THE PLATFORM)					OBSERVABLES DISTRIBUTION	
	STED REPORTS (CREATION DATE IN PLAYCrypt Extortion Softwar	I THE PLATFORM)	AlienVault	admin	Oct 26, 2023	TLP:CLEAR	80 K 70 K 60 K	• File
			AlienVault AlienVault	admin admin	Oct 26, 2023 Oct 26, 2023	TLP:CLEAR TLP:CLEAR	80 K 70 K	 Domain name Hostname
	PLAYCrypt Extortion Softwar						80 K 70 X 60 X 50 X	Domain name
	PLAYCrypt Extortion Softwar Winter Vivern exploits zero-d		AlienVault	admin	Oct 26, 2023	TLP:CLEAR	80 K 70 X 60 X 50 X	Domain name Hostname URL Text IPv4 address Software Software
	PLAYCrypt Extortion Softwar Winter Vivern exploits zero-d OSINT ShellShock scanning I		AlienVault CthulhuSPRL.be	admin admin	Oct 26, 2023 Oct 26, 2023	TLP:CLEAR	80 K 70 X 60 X 50 X	Domain name Hostname URL Text IPv4 address Email address
	PLAYCrypt Extortion Softwar Winter Vivern exploits zero-d OSINT ShellShock scanning I Trickbot to Ryuk in Two Hours		AlienVault CthulhuSPRL.be wilbursecurity.com	admin admin admin	Oct 26, 2023 Oct 26, 2023 Oct 26, 2023 Oct 26, 2023	TLP:CLEAR TLP:GREEN TLP:GREEN	80 K 70 X 60 X 50 X	Domain name Hostname UrlL Text IPv4 address Email address Software Artifact
	PLAYCrypt Extortion Softwar Winter Vivern exploits zero-d OSINT ShellShock scanning I Trickbot to Ryuk in Two Hours Harma and Odveta Ransomw		AlienVault CthulhuSPRL.be wilbursecurity.com wilbursecurity.com	admin admin admin admin	Oct 26, 2023 Oct 26, 2023 Oct 26, 2023 Oct 26, 2023	TLP:CLEAR TLP:GREEN TLP:GREEN TLP:GREEN	80 K 70 X 60 X 50 X	Domain name Hostname UrlL Text IPv4 address Email address Software Artifact

Figure 38: Snapshots of OpenCTI

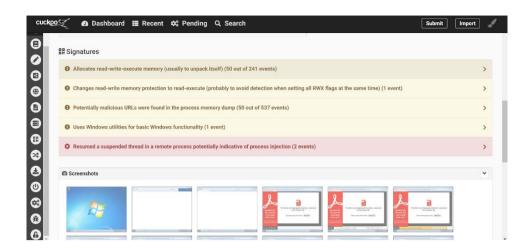
10.2 Cuckoo

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]

cuckoo 🌮 🛛 Da	ashboard	Recent	✿ Pending Q Search		Submit Import
Summary Static Analysis		Sum	mary	f5c16248418a4f1fd8dff	438b26b8da7f587b77db9e180a82493bae140893687.html
Extracted Artifacts Behavioral Analysis	2	File f5c16248	3418a4f1fd8dff438b26b8da7f587b77db9	e180a82493bae140893687.hti	မ်) Score က'
Network Analysis		Summar	y	La Download C Resubmit sample	This file shows numerous signs of malicious behavior.
Dropped Files	4	Size	1.1MB		The score of this file is 2.2 out of 10.
Dropped Buffers		Туре	HTML document, UTF-8 Unicode text, with very lon	g lines, with CRLF line terminators	Place and a The second second sector is a second still in
Process Memory	3	MD5	5cb20a0bfc5e3e2ae8398b1840adf7ae		Please notice: The scoring system is currently still in development and should be considered an <i>alpha</i> feature.
		SHA1	fdae22f8af65bb0af48d3f4413e9ed4d6e815f9c		
Compare Analysis		SHA256	f5c16248418a4f1fd8dff438b26b8da7f587b77db	9e180a82493bae140893687	Feedback
Export Analysis		SHA512	Show SHA512		Expecting different results? Send us this analysis and we will inspect it. Click here
Reboot Analysis		CRC32	DF542F1F		
Options		ssdeep	None		
Feedback		Yara	None matched		



E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com



koo🛫 🛛 Dashboard 🗮 Recent ¢	Pending Q Search		Su	ıbmit	Import
			And ark Construct some	rf (18632)	
Name	Response	Post-Analysis Lookup	IP Address	Status	Action
www.bing.com		2.18.40.153	8.8.8.8	Active	Moloch
dns.msftncsi.com		131.107.255.255			
r20swj13mr.microsoft.com		117.18.232.200			
www.msftncsi.com		96.17.178.209			
go.microsoft.com		23.37.1.150			
iecvlist.microsoft.com		117.18.232.200			
use.typekit.net		104.91.71.78			
ieonline.microsoft.com		204.79.197.200			
ipv6.msftncsi.com					
teredo.ipv6.microsoft.com					

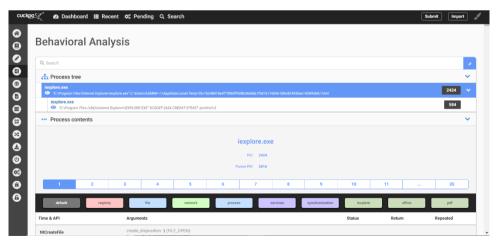


Figure 39: Snapshots of Cuckoo Sandbox

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].



E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com

- "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].Available:
- 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].
- "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/723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd0737 81074224/. [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/3c35f7163318f296b2f63bae7dfdb1037ac0a383b16d2149a455970a8e 139daa/. [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].
- "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]