Ransomware Redefined: RedEnergy Stealer-as-a-Ransomware

zscaler.com/blogs/security-research/ransomware-redefined-redenergy-stealer-ransomware-attacks

Summary

Zscaler ThreatLabz has discovered a new malware variant, **RedEnergy stealer** (not to be confused with the australian company Red Energy)that fits into the hybrid **Stealer-as-a-Ransomware** threat category.

RedEnergy stealer uses a fake update campaign to target multiple industry verticals and possesses the ability to steal information from various browsers, enabling the exfiltration of sensitive data, while also incorporating different modules for carrying out ransomware activities.The name of the malware was kept due to the common method names observed during the analysis.

This blog provides detailed insights into the different campaigns associated with this newly identified malware, along with a technical analysis of its stealer and ransomware characteristics.

Introduction

During the cybersecurity event Botconf 2023, ThreatLabz unveiled a novel threat category called **RAT-as-a-Ransomware** in April this year. However, more recently, researchers have identified another hybrid category following a similar approach, now known as **Stealer-as-a-Ransomware**. This latest discovery of RedEnergy stealer combines silent data theft with encryption to inflict maximum harm and gain control over its victims. It targets multiple industries, including energy utilities, oil, gas, telecom, and machinery. These advancements in malware represent a notable shift and key advancements beyond traditional ransomware attacks.

The sample Stealer-as-a-Ransomware variant analyzed in this case study employs a deceptive FAKEUPDATES campaign to lure in its targets, tricking them into promptly updating their browsers. Once inside the system, this malicious variant stealthily extracts sensitive information and proceeds to encrypt the compromised files. This leaves victims vulnerable to potential data loss, exposure, or even the sale of their valuable data.

This blog offers a comprehensive analysis of various campaigns associated with this emerging threat, shedding light on its operational aspects. Additionally, ThreatLabz provides a detailed technical overview of the malware, aiding in a better understanding of its

behavior and potential countermeasures.

Key takeaways

The key takeaways from this research article are:

- **Discovery of RedEnergy Stealer**: ThreatLabz latest research uncovers a highly sophisticated malware campaign using industries with reputable LinkedIn pages to target victims, including the Philippines Industrial Machinery Manufacturing Company and several organizations in Brazil. The attackers launch the attack on users that click to visit the website from LinkedIn for a compromised company, using multi-stage techniques and disguise the malware as browser updates to deceive users.
- **Stealer-as-a-Ransomware**: the malware analyzed has dual capabilities as both a stealer and ransomware, representing an alarming evolution in ransomware attacks. It employs obfuscation techniques and utilizes HTTPS for command and control communication, making detection and analysis challenging.
- **Multi-Stage Execution**: The malware operates through multiple stages, starting with the execution of disguised malicious executables. It establishes persistence, communicates with DNS servers, and downloads additional payloads from remote locations. Suspicious FTP interactions suggest potential data exfiltration and unauthorized file uploads.
- **Ransomware Functionality**: The malware includes ransomware modules that encrypt user data with the ".FACKOFF!" extension, rendering it inaccessible until a ransom is paid. It also modifies the desktop.ini file to evade detection and modify file system folder display settings.
- **Deletion of Shadow Drive Data**: In its final stage, the malware deletes shadow drive data and Windows backup plans, reinforcing its ransomware characteristics. It drops a batch file and a ransom note, demanding payment in exchange for file decryption.

By understanding these key takeaways, organizations can enhance their security posture and better protect themselves from RedEnergy stealer and similar types of malware campaigns.

Campaign:

Zscaler recently made a significant discovery involving a new and sophisticated threat campaign named RedEnergy stealer targeting the Philippines Industrial Machinery Manufacturing Company, as well as other industries with notable LinkedIn pages. These pages typically contain essential company information and website links, making them attractive targets for cybercriminals.

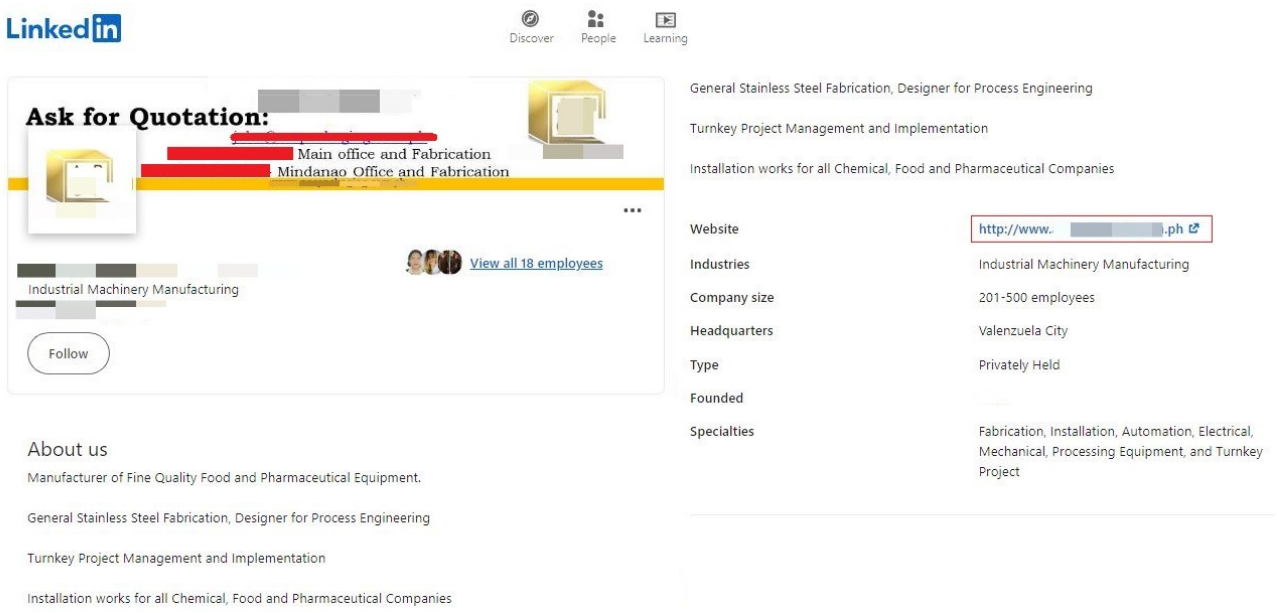

Fig 1. - LinkedIn page for Philippines Industrial Machinery Manufacturing

The operating mode for this threat campaign involves a deceptive redirection technique. When a user attempts to visit the targeted company's website through their LinkedIn profile, they are unsuspectingly redirected to a malicious website. Once there, they are prompted to install a seemingly legitimate browser update, which is presented as a set of four different browser icons. However, instead of a genuine update, the unsuspecting user unwittingly downloads an executable file known as RedStealer.

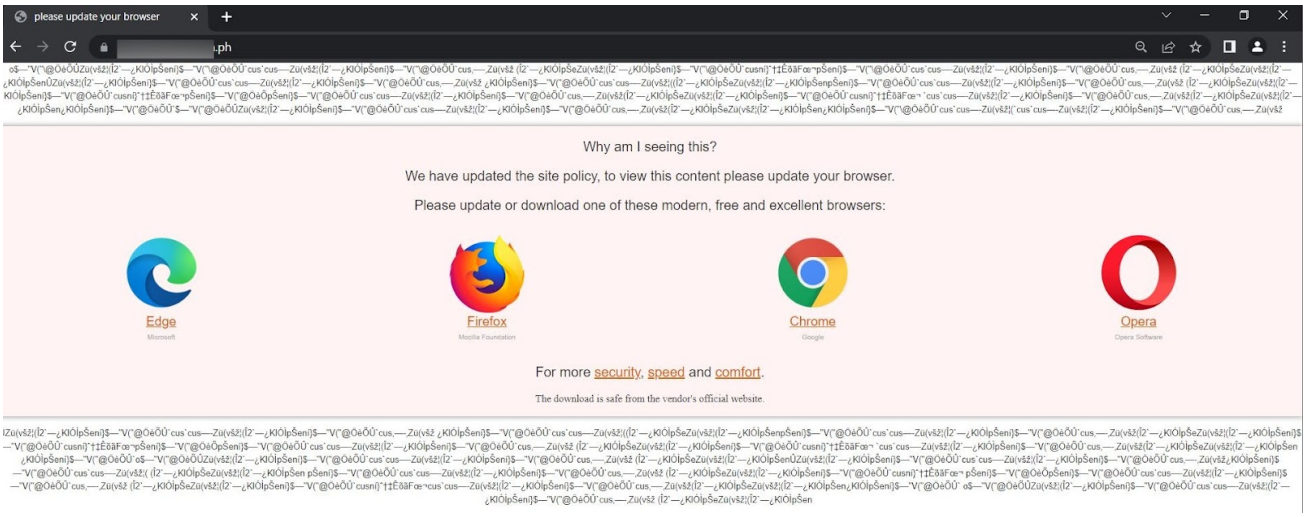

Fig 2. - Malicious download site

Interestingly, regardless of which browser icon the user clicks on, they are redirected to the same URL: **www[.]igrejaatos2[.]org/assets/programs/setupbrowser.exe**. This URL initiates the download of a file called setupbrowser.exe, which is part of the malicious payload.

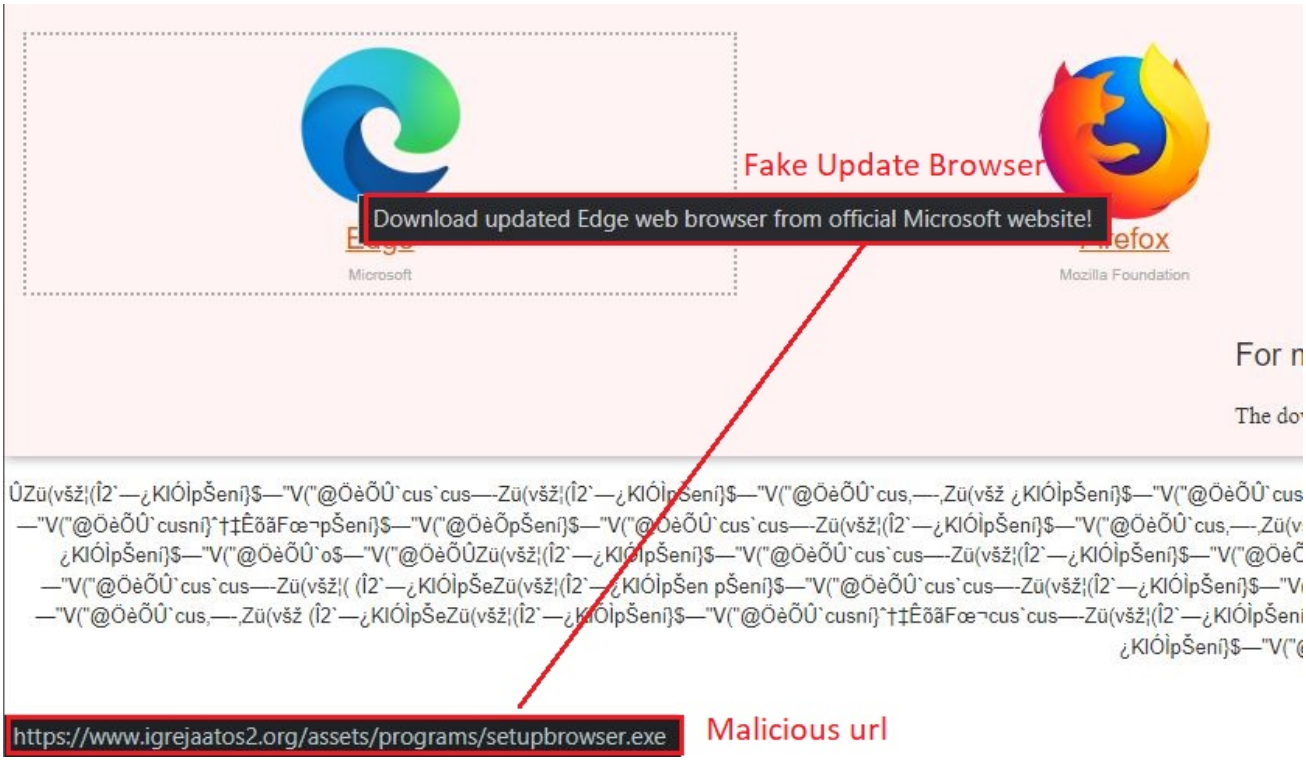

Fig 3. - Website downloading malicious payload

What makes this threat campaign even more insidious is the use of a deceptive download domain called **www[.]igrejaatos2[.]org**. This domain serves as a disguise, presenting itself as a ChatGpt site to lure victims into downloading a fake offline version of ChatGpt. However, upon downloading the purported ChatGpt zip file, the victim unknowingly obtains the same malicious executable mentioned earlier.

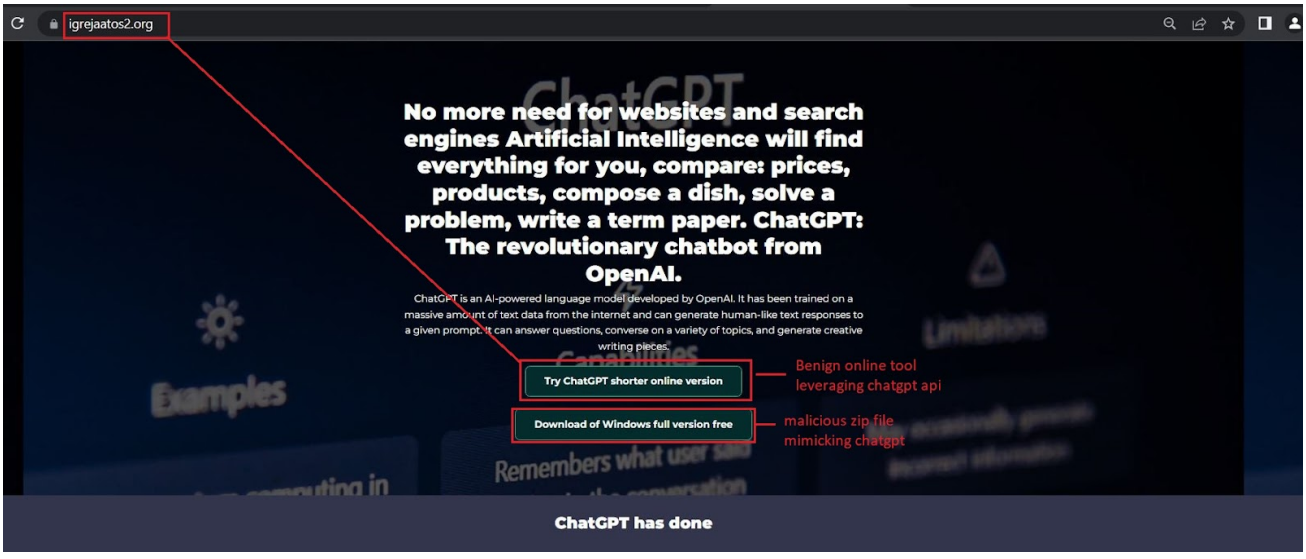

Fig 4. - Downloading domain luring users to download fake chatgpt tool

It is crucial for individuals and organizations to exercise utmost caution when accessing websites, especially those linked from LinkedIn profiles. Vigilance in verifying the authenticity of browser updates and being wary of unexpected file downloads is paramount to protect against such malicious campaigns.

Additional Campaigns:

In addition to the discovery of the threat campaign targeting the Philippines Industrial Machinery Manufacturing Company, Zscaler's thorough campaign search has uncovered several other related campaigns that exploit the FAKEUPDATES tactic. These campaigns exhibit similar characteristics and techniques, indicating a broader coordinated effort by the cybercriminals behind these attacks.

One such campaign involves impersonating a prominent Brazilian telecom company. Like the previously mentioned campaign, this variant directs victims to the same webpage and initiates the download of the identical executable file, **www[.]igrejaatos2[.]org/assets/programs/setupbrowser.exe**. This indicates that the attackers behind this campaign are reusing their infrastructure and tactics to maximize impact and profits.

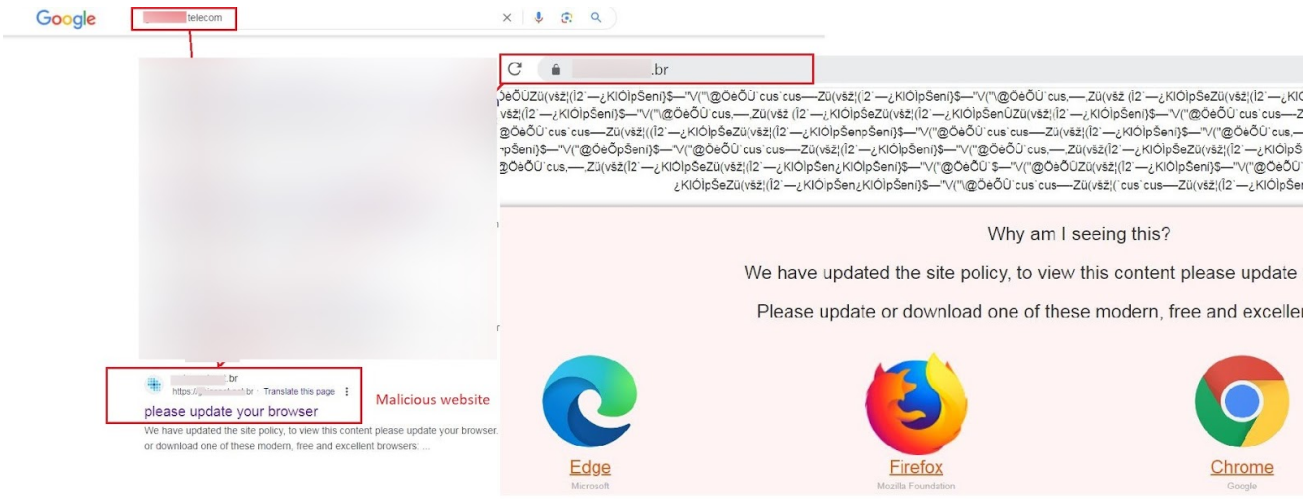

Fig 5. - Similar campaign leveraging google search

Furthermore, a well-known Brazilian cosmetics company has also fallen victim to this malicious campaign, experiencing the same type of attack which downloads the same payload. It is evident that the cybercriminals behind these campaigns are targeting organizations across various industries, leveraging their already established reputations and online presence to deceive unsuspecting users.

To gain a deeper understanding of the technical aspects of this malware, let us delve further into its analysis in the sections that follow. By examining the intricacies of the malicious code, security researchers can uncover crucial details about its behavior, functionality, and

potential impact on the compromised systems. This information is essential for developing effective countermeasures and mitigating the risks associated with this ongoing threat.

Technical Analysis:

The RedEnergy malware under investigation exhibits a dual functionality, acting both as a stealer and a ransomware. This .NET file, intentionally obfuscated by its author, possesses advanced capabilities to evade detection and hinder analysis. To establish communication with its command and control servers, the malware utilizes HTTPS, adding an additional layer of encryption and obfuscation.

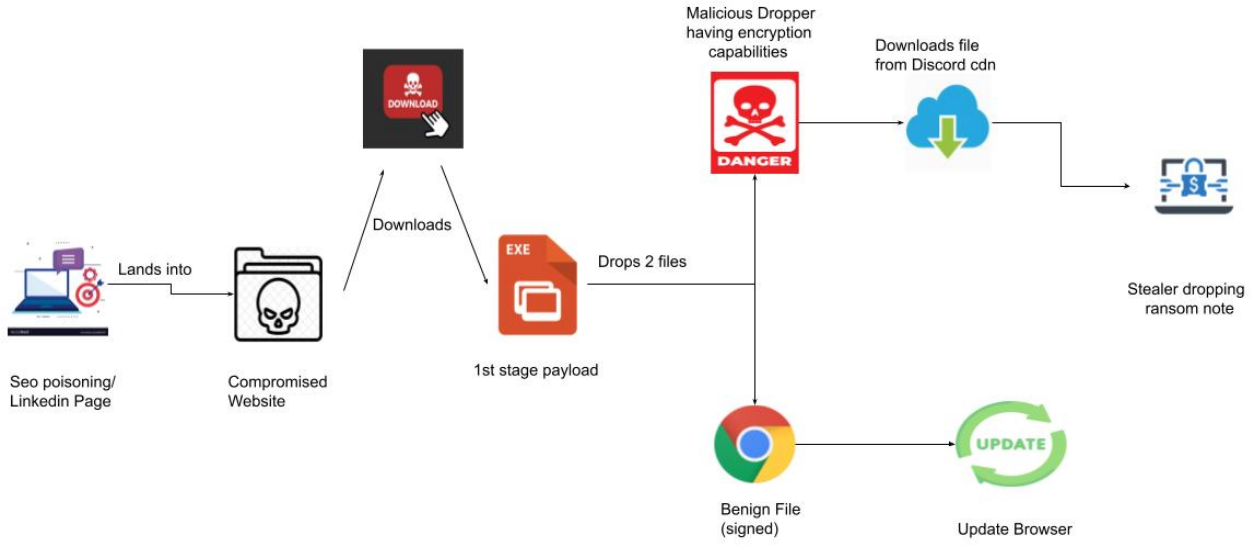

Fig 6. - Infection chain

The execution of this malware unfolds in three distinct stages, each serving a specific purpose. Each stage is outlined in the sections below.

Stage 1: Initial Startup

Upon execution, the malicious RedEnergy executable masquerades as part of a legitimate browser update, depicted in Fig. 7 below. It cleverly disguises itself with a legitimate update from one of the various popular browsers, including Google Chrome, Microsoft Edge, Firefox, and Opera, to deceive the user. Notably, looking at the properties of the malicious executable reveals the presence of an invalid certificate, however at surface level this attack hides behind a genuine signed certificate from the user's browser as shown by the Google example examined in Fig. 8 below. This deceptive tactic aims to instill trust and convince the victim of the authenticity of the update.

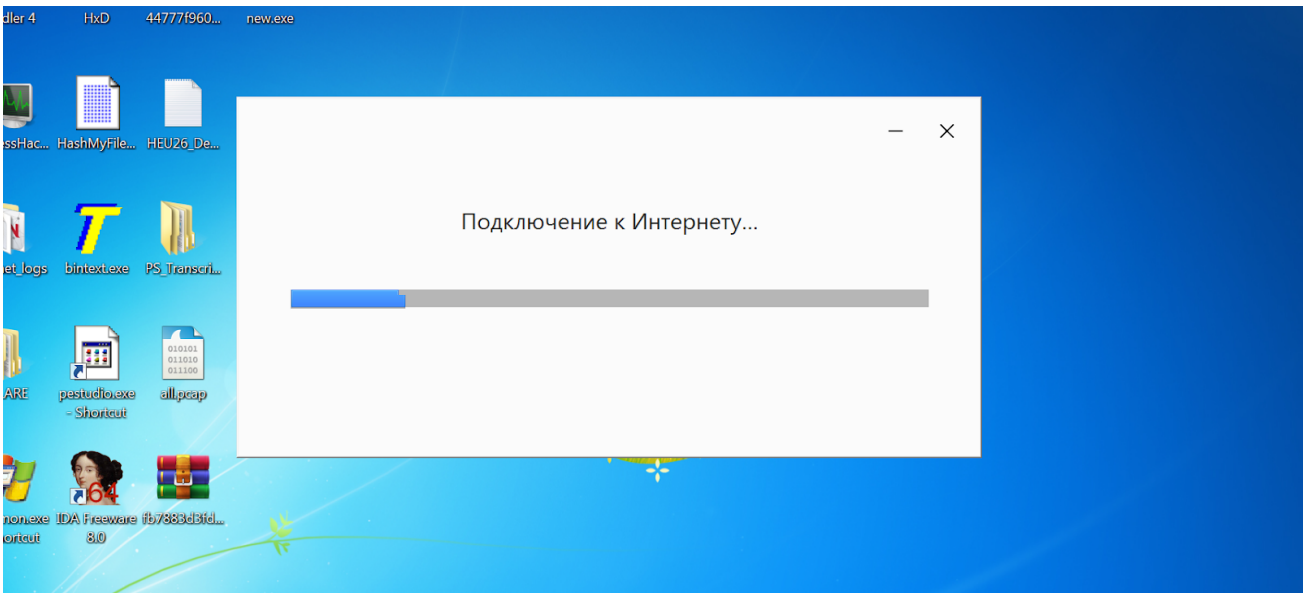

Fig 7. - Google updater executing the malicious RedEnergy binary

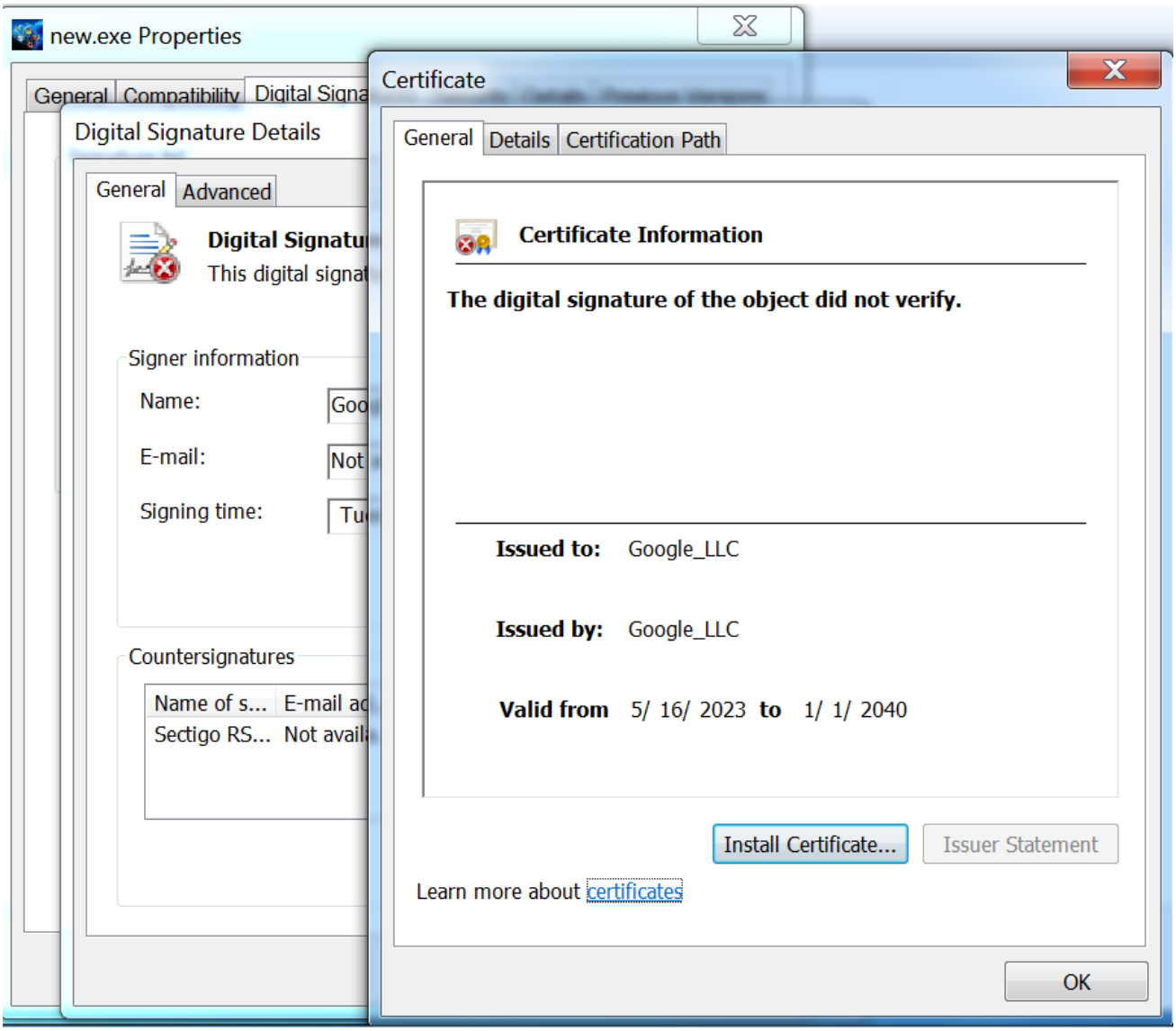

Fig 8. - Fake certificate

Stage 2: Dropping Files, Persistence, Outgoing Requests, Encrypted Files

Dropping Files:

In this stage, the malware drops four files onto the victim's system, shown in Fig. 9 below, precisely within the path **%USERPROFILE%\AppData\Local\Temp**. These dropped files consist of two temporary files and two executables, all following a similar pattern with filenames beginning with "**tmp**" and four randomly generated hexadecimal characters, followed by the "**.exe**" extension: **tmp[4 random hex characters].exe**. Among the executable files, one serves as the malicious payload, while the other disguises itself as the legitimate, digitally signed Google Update. The benign executable possesses the hash value **8911b376a5cd494b1ac5b84545ed2eb2** and is responsible for performing the actual update of Google Chrome, thereby further deceiving the victim. Simultaneously, the malware executes another background process, identified by the MD5 hash **cb533957f70b4a7ebb4e8b896b7b656c**, which represents the true malicious payload. During execution, this payload displays an inappropriate message on the victim's screen, displayed in Fig. 10 below, most likely as part of the threat actor's intent to cause distress or confusion.

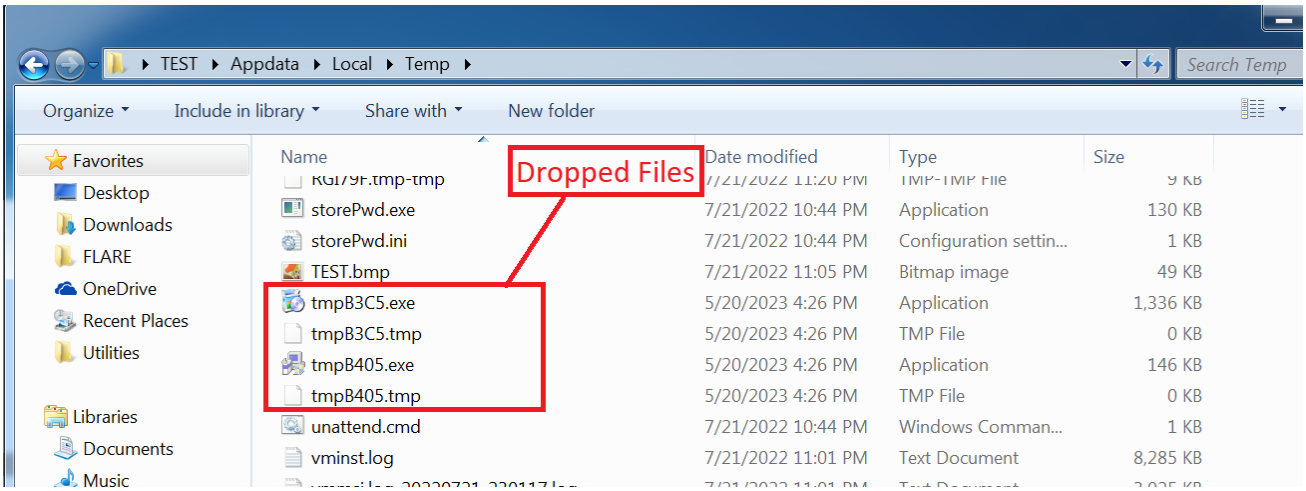

Fig 9. - Dropping malicious file in temp directory

Fig 10. - Display message after executing the binary

Persistence:

Persistence is a critical aspect of malware, enabling it to maintain its presence on an infected system even after rebooting or shutting down. To achieve persistence, the malicious executable stores files in the Windows startup directory. It creates an entry within the start menu (**Start Menu\Programs\Startup**) and initiates an immediate reboot, ensuring that the malware is executed once the system is up and running again. This persistence mechanism guarantees that the malware remains active and continues its malicious operations even after system restarts.

Outgoing Requests:

During the analysis of the malware, researchers utilized Fakenet, a Windows malware analysis tool that simulates network activity, to gain insights into its behavior. Through Fakenet, they discovered that the malicious tmp.exe file established communication with the DNS server **2no.co**, depicted in Fig. 11 below. To delve deeper into the network interactions, the widely used packet analysis tool, Wireshark, was employed. This allowed researchers to identify the specific DNS query made by the malicious tmp.exe file, providing crucial information for further investigation, as shown in Fig. 12 below. It was observed that upon establishing a connection with the DNS server, tmp.exe was expected to initiate the download of an executable file from cdn.discord. Unfortunately, during this particular analysis, the Command and Control (CnC) server was unavailable, making it impossible to obtain a sample. However, another sample resembling the final payload was discovered, which had been hosted on the same domain just two days prior to the current analysis.

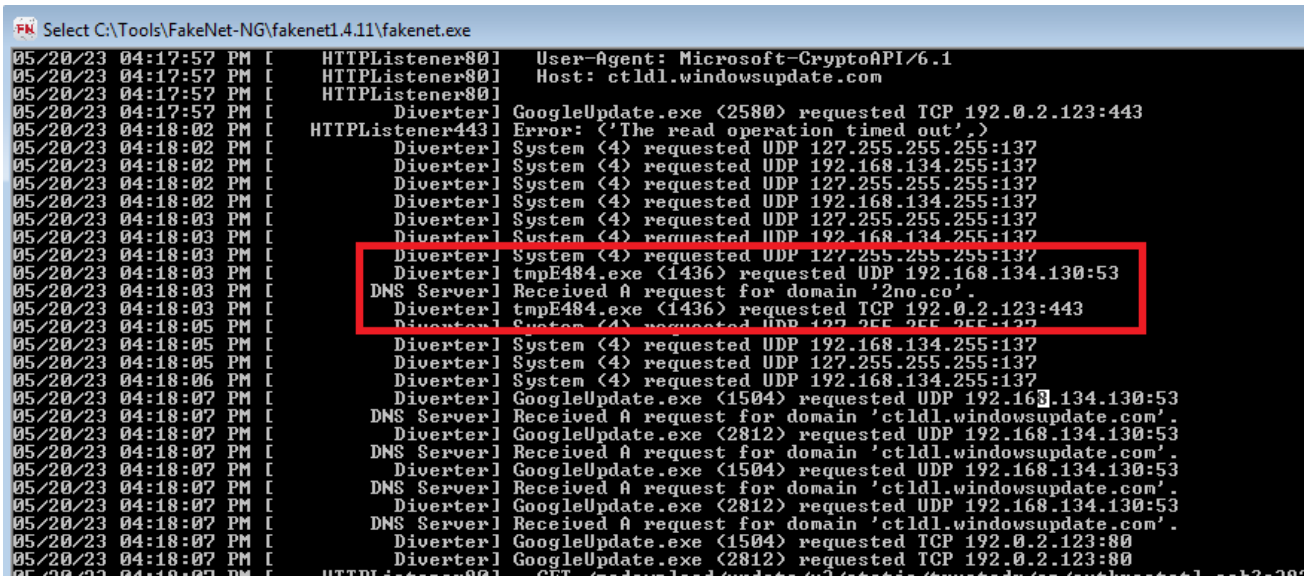

Fig 11. - Malicious binary communication with CnC server

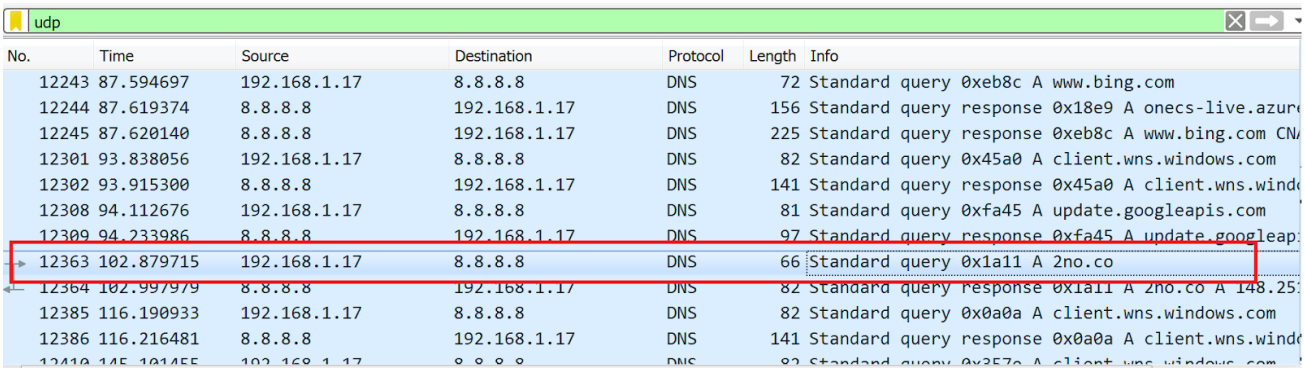

Fig 12. - Network communication seen via Wireshark

Additionally, suspicious activity involving File Transfer Protocol (FTP) was uncovered during the investigation. A user with the username "**alulogrofp**" successfully accessed a private system hosted by OVH, a renowned cloud computing company and one of the largest hosting providers globally. The user's credentials were authenticated, granting them access to a restricted directory, which was identified as the root directory ("/"). Notably, UTF-8 encoding was enabled for file transfers, indicating support for international character sets.

```
220-  ~~~ Welcome to OVH ~~~
220 This is a private system - No anonymous login
USER alulogrofp
331 User alulogrofp OK. Password required
PASS Aluniz[redacted]
230 OK. Current restricted directory is /
OPTS utf8 on
200 OK, UTF-8 enabled
PWD
257 "/" is your current location
CWD assets/bootstrap/css
250 OK. Current directory is /assets/bootstrap/css
TYPE I
200 TYPE is now 8-bit binary
PASV
227 Entering Passive Mode (51,68,11,192,115,132)
NLST
150 Accepted data connection
226-Options: -a
226 6 matches total
QUIT
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
```

```
220-  ~~~ Welcome to OVH ~~~
220 This is a private system - No anonymous login
USER alulogrofp
331 User alulogrofp OK. Password required
PASS Aluniz[redacted]
230 OK. Current restricted directory is /
OPTS utf8 on
200 OK, UTF-8 enabled
PWD
257 "/" is your current location
TYPE I
200 TYPE is now 8-bit binary
PASV
227 Entering Passive Mode (51,68,11,192,82,103)
RETR assets/bootstrap/css/SPP
150-Accepted data connection
150 1650.0 kbytes to download
226-File successfully transferred
226 0.597 seconds (measured here), 2.70 Mbytes per second
```

Fig 13. - FTP interaction on OVH private system

Within the FTP session, the user navigated to the "/assets/bootstrap/css" directory, following standard directory traversal practices. To ensure efficient and accurate file transfers, the transfer mode was set to binary (8-bit). Subsequently, the server entered passive mode and provided an IP address and port number, indicated by the message "Entering Passive Mode (51,68,11,192,115,132)". By combining the extracted data, the IP address 51.68.11[.]192 was obtained. Further interactions revealed that the user requested a file list using the "NLST" command, resulting in the retrieval of six matching files.

In another session, the client initiated a file retrieval operation using the "RETR" command, specifying the file path as "assets/bootstrap/css/SPP". The server acknowledged the data connection and confirmed the acceptance of the file transfer.

These FTP interactions raised concerns regarding potential data exfiltration, as well as the possibility of uploading files using the same method.

Encrypted Files:

With ransomware modules integrated into the payload, the malware proceeded to encrypt the user's data, appending the ".FACKOFF!" extension to each encrypted file, as shown in Fig. 14 below. This malicious software is specifically designed to lock the user's files, rendering them inaccessible until a ransom is paid. After the encryption process is completed, the user receives a ransom message, demanding payment in exchange for restoring access to their files. Failure to comply with the ransom demands results in the permanent loss of access to the compromised data.

Furthermore, the malicious executable alters the desktop.ini file, which contains configuration settings for the file system folders. By modifying this file, the malware can manipulate how the file system folders are displayed, potentially further concealing its presence and activities on the infected system. This alteration serves as an attempt to mislead the user and impede the detection of the malware's impact on the file system.

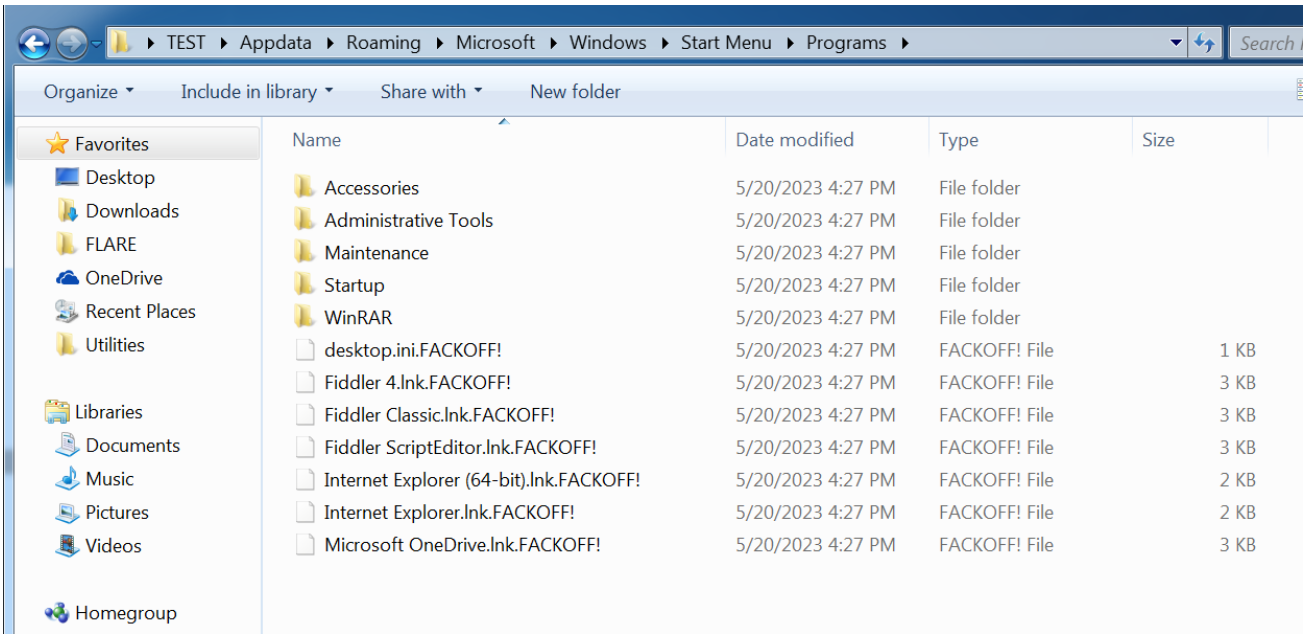

Fig 14. - Encrypted files with .FACKOFF! extension

Stage 3: Decryption Routine

The final stage payload is responsible for various actions, including dropping the ransom note and executing multiple commands and stealer functionalities, and for encryption it uses the **RijndaelManaged** algorithm. Within the payload, numerous functions are named RedEnergy, giving rise to its namesake.

In the second stage, the malware downloads the executable **SystemPropertiesProtection.exe** via the discord cdn. This leads to the third stage, where the malware executes a series of actions typically associated with ransomware. It begins by deleting data from the shadow drive, effectively removing any potential backups. The malware also targets Windows backup plans, further hindering the user's ability to recover their data. Additionally, a batch file is executed, and a ransom note is dropped, indicating the user's files have been encrypted. Furthermore, the malware possesses stealer capabilities, allowing it to exfiltrate the user's data.

Notably, the Config method, shown in Fig. 15 below, plays a crucial role in decrypting key information. It stores important strings related to the stealer functionality in a dictionary, depicted in Fig. 16, which is used to construct command lines for further operations.

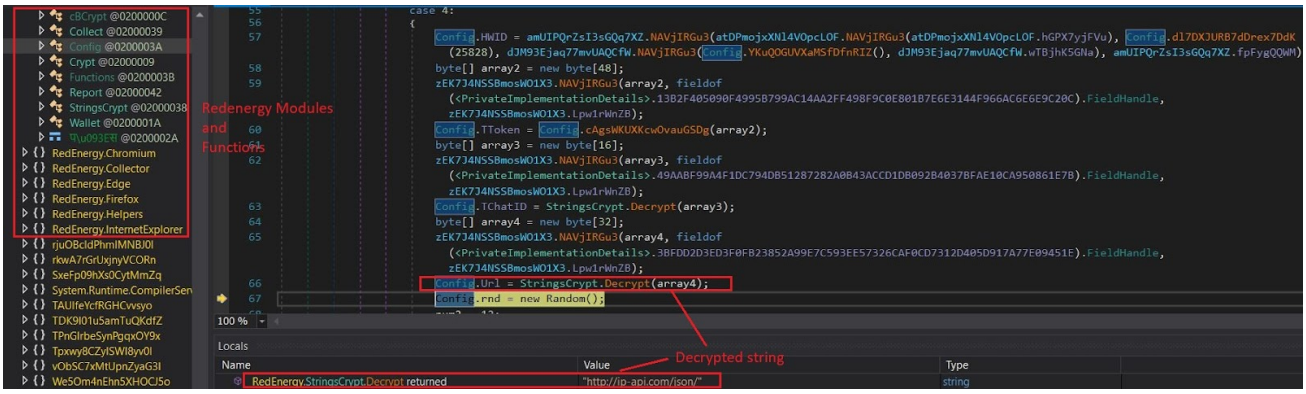

Fig 15. - Config decryption function

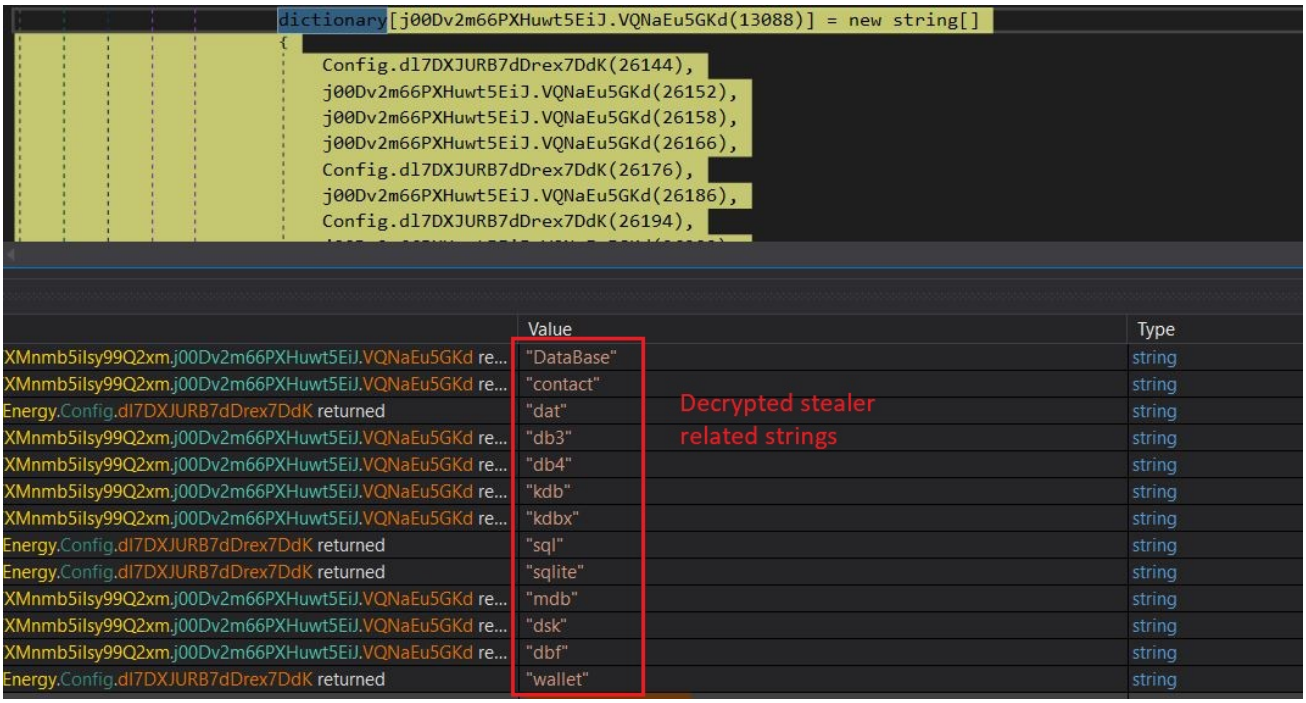

Fig 16. - Malware showcasing stealer capabilities

One such decrypted command line, shown in Figure 17, modifies the boot configuration to ignore failures and disables the automatic recovery options in Windows. The payload also drops specific files in the Temp directory, as seen in Figure 18, using it as a camouflage to conceal its malicious intent. Among the files dropped, C.bin serves as a payload, while a batch file contains commands to terminate processes and perform cleanup tasks associated with the payload. Figure 19 illustrates the instructions executed by the batch file.

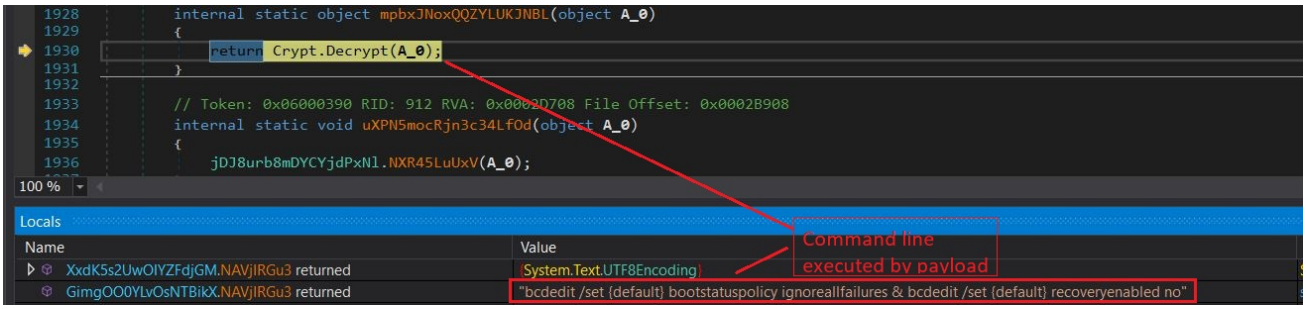

Fig 17. - Command line executed post decryption

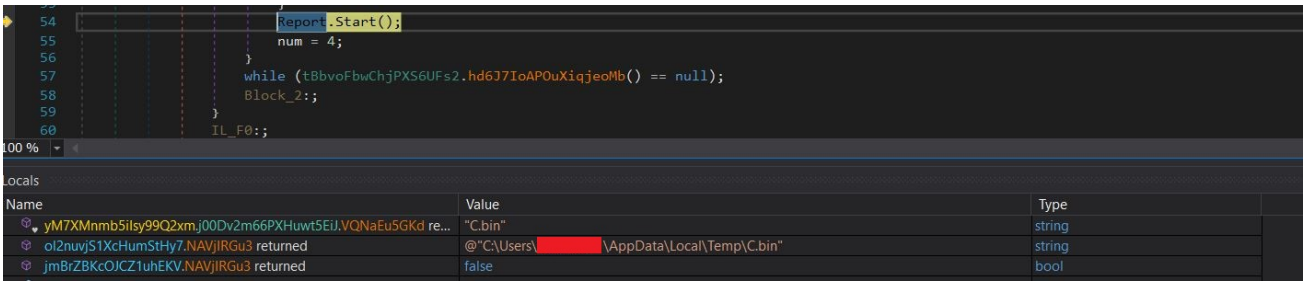

Fig 18. - Dropping supporting files in temp directory

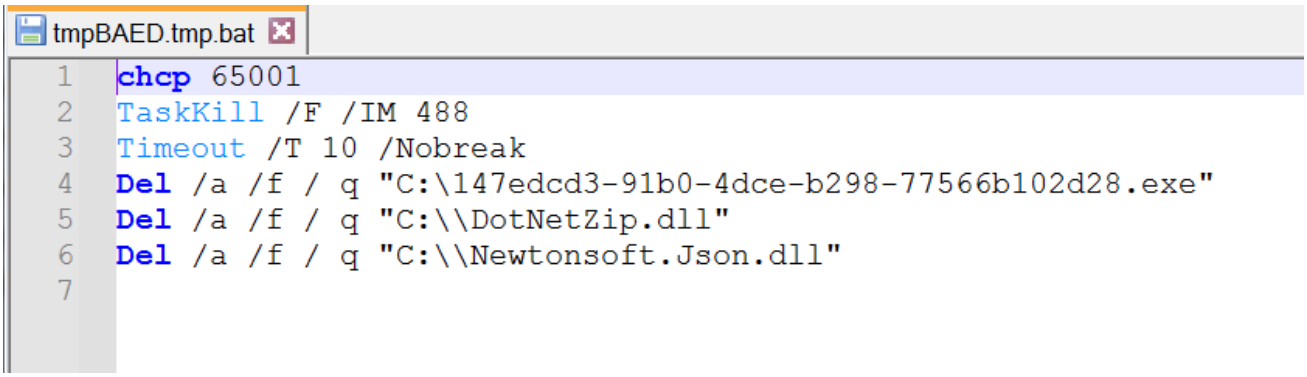

Fig 19. - Content inside batch file

Furthermore, the payload is programmed to delete all volume shadow copies (VSS), the backup catalog, and shadow copies using the Windows Management Instrumentation Command-line (WMIC). The following command lines exemplify this process:

- C:\Windows\System32\cmd.exe /C vssadmin delete shadows /all /quiet & wmic shadowcopy delete
- C:\Windows\System32\cmd.exe /C wbadmin delete catalog -quiet

Additionally, the payload undergoes a three-stage process to gather antivirus (AV) information. Based on this information, it generates a string that it sends to the Command and Control (CnC) server as a User Agent, as depicted in Figure 20 below. During the analysis, it was observed that the AV detected is Windows Defender. STM, RSM, and RZ likely provide additional information related to Windows Defender.

Lastly, the payload is responsible for dropping the final ransom note, **read_it.txt**, shown in Figure 21. This note is placed in all the folders where file encryption occurs, serving as a notification to the user that their files have been encrypted and demanding a ransom for their release.

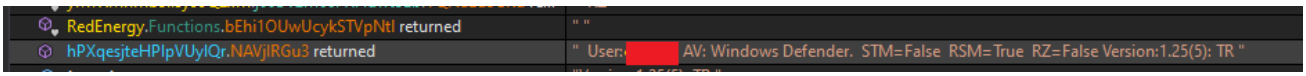

Fig 20. - User Agent built from malicious code storing AV information

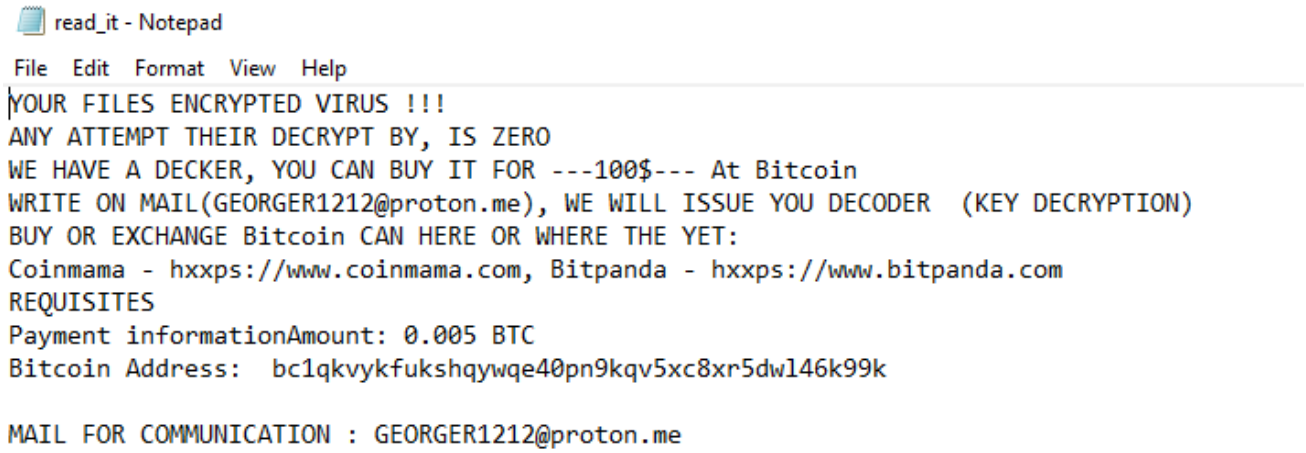

Fig 21. - Screenshot of the ransom note

Zscaler Sandbox Coverage:

Zscaler's security sandbox actively detects indicators for this threat, helping Zscaler customers defend against such attacks automatically, as shown in Fig. 22 below.

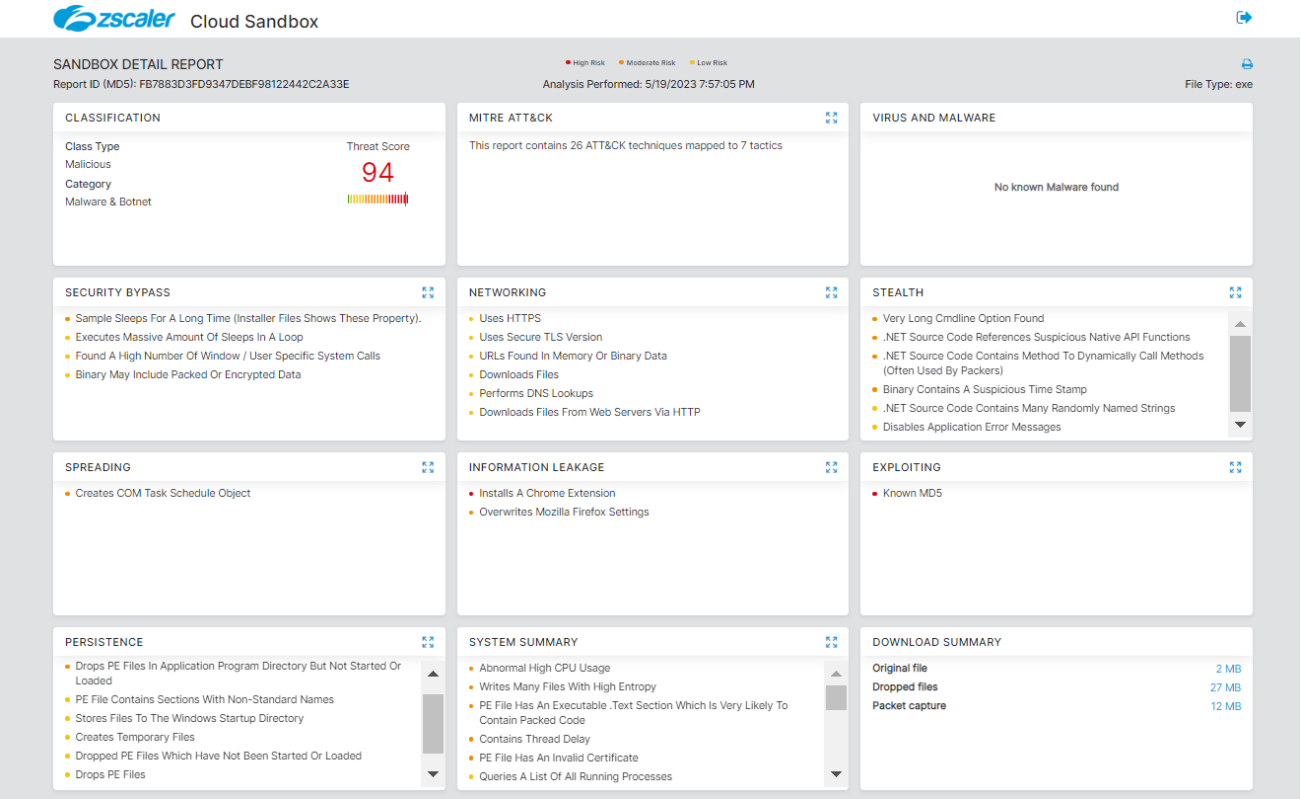

Fig 22. - Zscaler sandbox report

The following threat names are detected by Zscaler's multilayered cloud security platform for identifying malicious payloads: **Win32.Downloader.RedEnergyStealer**

Conclusion

In conclusion, the analysis of the malware campaign targeting the Philippines Industrial Machinery Manufacturing Company, along with other industries through reputable LinkedIn pages, has revealed a highly sophisticated and multi-stage attack. This campaign involves the distribution of malware disguised as browser updates, leading unsuspecting users to malicious websites where they unknowingly download the RedStealer executable. Notably, similar campaigns have been observed targeting companies in Brazil, highlighting the broad reach of this threat.

The technical analysis of the malware has exposed its dual functionality as both a stealer and ransomware, representing a concerning evolution in the development of ransomware-like attacks. The malware employs obfuscation techniques and leverages HTTPS for command and control communication, making it challenging to detect and analyze. It operates through multiple stages, starting with the execution of the malicious executable masquerading as a browser update. Subsequently, it drops files, establishes persistence, and initiates outgoing requests to communicate with DNS servers and download additional payloads from remote locations.

The discovery of suspicious FTP interactions raises further concerns about potential data exfiltration and unauthorized file uploads. The malware's ransomware modules are responsible for encrypting user data using the ".FACKOFF!" extension, rendering it inaccessible until a ransom is paid. Additionally, the alteration of the desktop.ini file enhances the malware's ability to evade detection and manipulate file system folder display settings.

The final stage of the malware execution involves the deletion of shadow drive data and Windows backup plans, solidifying its ransomware characteristics. A batch file is executed, and a ransom note is dropped, demanding payment in exchange for decrypting the files. Furthermore, the malware exhibits stealer functionalities, enabling the theft of user data.

Overall, this analysis highlights the evolving and highly sophisticated nature of cyber threats targeting various industries and organizations. It emphasizes the critical importance of implementing robust security measures, fostering user awareness, and ensuring prompt incident response to effectively mitigate the impact of such attacks. By remaining vigilant and implementing comprehensive cybersecurity strategies, businesses can better protect themselves against these malicious campaigns and safeguard their valuable data.

Zscaler's ThreatLabz team remains dedicated to monitoring these threats and sharing their findings with the wider community. It is crucial for individuals and organizations to stay informed and take necessary precautions to defend against malware attacks. This includes regularly updating software, using strong passwords, and exercising caution when encountering suspicious emails or messages. By collectively addressing these challenges, we can enhance the security of our digital landscape and mitigate the risks associated with evolving cyber threats.

MITRE ATT&CK TTP Mapping

ID	Tactic	Technique
T1036	Defense Evasion	Masquerading
T1185	Collection	Browser Session Hijacking
T1070.006	Defense Evasion	Timestomp
T1560	Collection	Archive Collected Data
T1027	Defense Evasion	Obfuscated Files or Information

T1562.001	Defense Evasion	Disable or Modify Tools

Indicators of Compromise (IOCs)

Main Payload	fb7883d3fd9347debf98122442c2a33e
Downloading Domain	www[.]igrejaatos2[.]org/assets/programs/setupbrowser[.]exe
Dropper Payload	cb533957f70b4a7ebb4e8b896b7b656c
Connecting Domain	2no[.]co
Final Payload	642dbe8b752b0dc735e9422d903e0e97