TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Cyber Security Engineering

Fothul Karim Forhan 194489IVSB

Analysis of Infostealer Malware Samples and Proposed Defensive Measures

Bachelor's thesis

Supervisor: Shaymaa Mamdouh Khalil
MSc

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Küberturbe tehnoloogiad

Fothul Karim Forhan 194489IVSB

Infostealer'i pahavara näidiste analüüs ja soovitatavad ennetusmeetmed

Bakalaureusetöö

Juhendaja: Shaymaa Mamdouh Khalil
MSc

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Fothul Karim Forhan

13.05.2023

Abstract

Infostealer is a type of malicious software that steals several types of sensitive data from the victim's device. The stolen data consists of passwords, screenshots, network activities, browsing history, and other private information. These types of malwares are becoming increasingly sophisticated and difficult to detect, posing significant threats to individuals and organizations alike.

In this research, Automated dynamic analysis of multiple samples for the Redline variant of Infostealer Malware is performed. The analysis aimed in finding the common traits and behaviours of these samples based on MITRE ATT&CK detection. Additional research and analysis are performed on the Initial Access phrase of this malware variant. According to the findings, the thesis also proposes defensive measures to be taken in preventing such attacks.

The results of the research can be used by organization or individuals in getting insight on Infostealer malware and utilizing the proposed defensive measures to increase their defence capabilities. Some key findings from this research have been made available in our GitHub repository to ensure that the information reaches the targeted audiences.

This thesis is written in English and is 48 pages long, including 5 chapters, 19 figures and no table.

List of abbreviations and terms

API	Application Programming Interface
CLSID	Class Identifier
COM	Component Object Model
CTI	Cyber Threat Intelligence
CVE	Common Vulnerability and Exposures
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Massage Authentication, Reporting & Conformance
EDR	Endpoint Detection and Response
FTP	File Transfer Protocol
HWID	Hardware ID
IM	Instant Messaging
IOC	Indicator of Compromise
IP	Internet Protocol
JSON	JavaScript Object Notation
MaaS	Malware as a Service
MFA	Multi-Factor Authentication
OODA	Observe, Orient, Decide, Act
OS	Operating System
PE	Portable Executable
RC4	Rivest Cipher 4
SIEM	Security Information and Event Management
SPF	Sender Policy Framework
TLS	Transport Layer Security
YARA	Yet Another Recursive Acronym

Table of contents

List of figures

1 Introduction

In this section, we establish the context for the research topic by highlighting the increasing importance of cybersecurity, specifically focusing on the challenges and risks associated with Infostealer malware and its potential impact on organizations.

1.1 Motivation

In the last few years, cyberattacks have become more advanced and sophisticated, thus the importance of cybersecurity has become a critical concern for both individuals and organizations. Malware attacks are a widespread and serious type of cyber threat that involves executing unauthorized actions on a victim's system The term malware refers to malicious software, and various specific types of malwares exist. One such type is Infostealer, which is designed to steal sensitive information by performing unauthorized actions within a system. The primary objective of Infostealer is to collect information without the victim's knowledge or consent, potentially resulting in significant harm to individuals or organizations.

Undoubtedly stolen sensitive information is a serious risk to multiple pillars of Cybersecurity. There have been several incidents of data breaches on the impact of Infostealer. A recent case of such an incident of the data breach was at CircleCl, where Infostealer were deployed on an employee’s laptop and unauthorized third party were able to steal authentication single sign-on session, enabling them to impersonate the targeted employee thus resulting in exfiltrating data [1]. Additionally, the stolen information is often sold on the dark web, where threat actors can purchase it and use it to carry out other types of cyberattacks. This makes Infostealers a significant risk for individuals and organizations, as the stolen data can be used for identity theft, financial fraud, and other malicious activities.

These combined factors make the research topic particularly attractive. Additionally, the process of conducting the research will allow the researcher to apply the knowledge obtained to their daily work activities.

1.2 Research Problem

Infostealer malware is a significant contributor to Credential Compromise and Account Hijacking attacks, often going undetected due to its Trojan-based nature and lack of disruption to daily activities [2]. The impact of Infostealer malware may cause loss of data privacy and financial or reputational damage to a person or corporate entity. While ransomware attacks receive the most attention, Infostealer malware helps in the initial step of a ransomware attack. Infostealer malware attacks are often perpetrated by organized groups and the stolen information is sold on the dark web.

According to the Accenture, the recent rise in Multi Factor Authentication (MFA) Fatigue Attacks[1] has led to an increase in the sale of stolen credentials on the Darkweb. Accenture also anticipated that in 2023 the Infostealer landscape will continue to evolve and pose significant risks to organizations [3].

1.3 Research Goal and Objective

The primary goal of this research is to conduct a comprehensive analysis of Infostealer malware samples, with a specific focus on the Redline variant. The study aims to identify common MITRE ATT&CK-based patterns in multiple samples of the malware, and to conduct an in-depth reports review on the delivery phase of the malware. Based on the findings, an attack flow is developed, illustrating the key steps and techniques utilized by the malware. Upon examining the outcomes of this analysis and web-based reports review, the research proposes a list of defensive measures that organizations can implement to mitigate against the threat of Infostealer malware.

1.4 Limitation

Infostealer malware comprises numerous variants, such as Racoon, Vidar, AZOrult, Trickbot, Redline, Taurus, and others [3]. These variants are designed to compromise the security of targeted systems, and to steal sensitive information from infected devices.

[1] https://www.beyondtrust.com/resources/glossary/mfa-fatigue-attack

Each variant of Infostealer malware may have unique characteristics, tactics, and techniques. Given the wide range of Infostealer malware variants available, the research focuses specifically on the Redline Stealer variant. Additionally, it is important to acknowledge that the research is limited by the number of Redline Stealer samples collected. Therefore, the findings and results presented in this study are based solely on the collected samples, and there is a possibility that other samples of the Redline Stealer may produce different outcomes or indicators.

Furthermore, it should be noted that the proposed defensive measures were not tested in this study due to time limitations. A separate study could be conducted in the future to evaluate the effectiveness of these techniques in protecting against Infostealer malware.

1.5 Structure of the Thesis

Chapter 1 introduces the motivation behind the study, the research problem being addressed, and the specific goals and objectives of the thesis. It also outlines the limitations of the research. Chapter 2 provides the background information required to understand the research, discussing the Redline Stealer malware, the MITRE ATT&CK Framework, and the tools used in the study. In Chapter 3, the methodology is presented, detailing the research design employed in the thesis. Chapter 4 emphasis on presenting the findings of the research, which include the process of conducting automated dynamic and static analyses, identification of common MITRE techniques, analysis of these techniques and their indicators, initial access trends analysis, attack flow, and proposed defensive measures. Finally, Chapter 5 concludes the thesis and suggests potential approach for future work and improvements to the study.

2 Background Information

The following sections provide an overview of Redline Stealer, a powerful Infostealer malware, and discuss the rise of Malware as a Service (MaaS). Additionally, this section also introduces various tools and the MITRE ATT&CK framework used in the research to analyse and better understand the tactics, techniques, and procedures employed by Redline Stealer.

2.1 Redline Stealer

Redline Stealer is an Infostealer malware that was first detected in the wild in early 2020 [4]. It is written in the C# programming language and has been continuously updated to evade detection [5]. Redline Stealer is an information-stealing tool that can steal a wide variety of sensitive data from a victim's computer. The malware targets login credentials, cryptocurrency wallets, credit card information, and browser data [4] [5]. Additionally, it can take screenshots of the victim's desktop and steal information from the clipboard. Once it has stolen the information, Redline Stealer sends it to a remote command and control (C&C) server operated by the attacker [5].

The impacts of Redline Stealer can be significant. The malware has been linked to several high-profile cyber-attacks; a mentionable case is for Microsoft. In the Microsoft attack, the attacker used Redline Stealer to steal sensitive information and perform malicious activities on the victim's system [6]. Redline Stealer uses several techniques to evade detection and infect the victim's computer. Redline Stealer has also been found to self-propagate on YouTube via malicious advertisements [7]. The malware is hidden in a bundle file that advertises itself on YouTube, and when a user downloads the file, Redline Stealer is installed on the victim's computer.

In summary, Redline Stealer is a highly sophisticated and dangerous information-stealing malware that has been used in several cyber-attacks. Its ability to steal a wide range of sensitive data and self-propagation capabilities make it a significant threat to businesses and individuals, emphasizing the need for strong defensive measures.

2.1.1 Redline as a Service

The rise of Malware as a Service (MaaS) has had a significant impact on the global cybersecurity landscape, making it easier for individuals with malicious intent to gain access to sophisticated hacking tools and carry out cyber-attacks. MaaS is an underground economy model that allows users to purchase subscriptions to malware and hacking tools, often at low cost and with little technical knowledge required. According to [8], MaaS has contributed to the growth of the global cybercrime industry, which is estimated to cost businesses and individuals billions of dollars each year.

Like many other types of Infostealer, the primary motivator for the creation of Redline Stealer was the increasing popularity of the Malware-as-a-Service (MaaS) business model. The Stealer is likely to have spread worldwide since it is available to anyone who would like to pay the price for the software [9]. Redline Stealer has been advertised in multiple Telegram channels and different underground forums, where users can pay a price to access the entire infrastructure and launch their own campaigns. For research purposes, one of these public Telegram channels was viewed and following screenshots were captured. Figure 1 displays an advertisement for a new version of Redline Stealer, featuring log management capabilities that can collect various types of information from different domains.

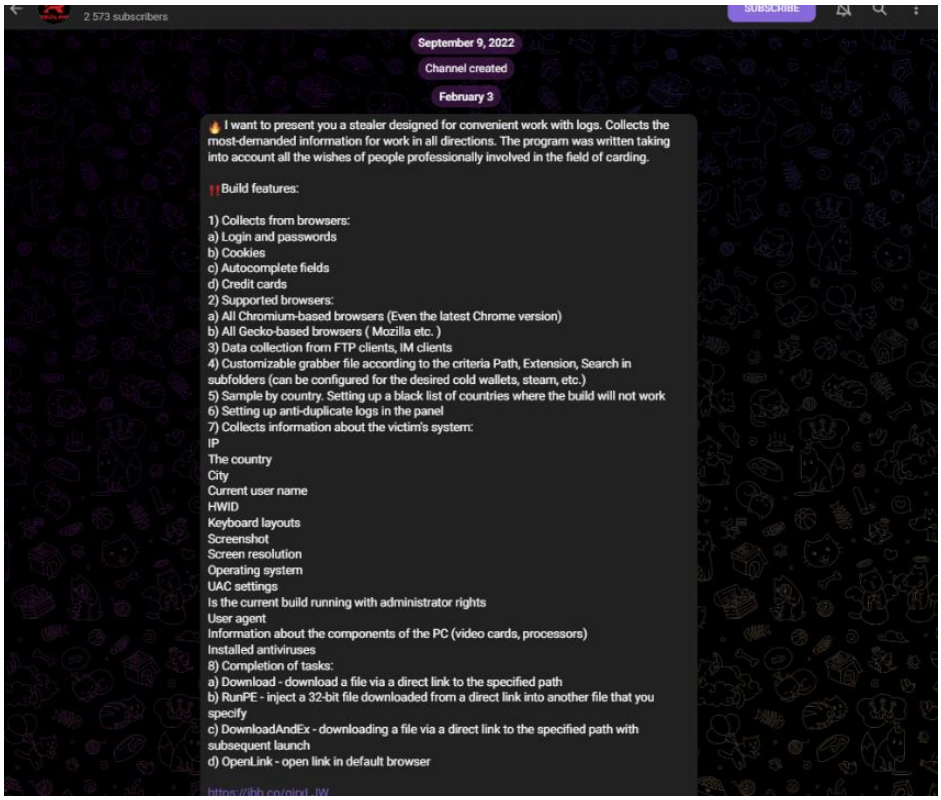

Figure 1. Build feature from Redline's Telegram Channel.

The Stealer captures login credentials, cookies, autocomplete fields, credit card details from browsers like Chromium and Gecko, sensitive data from FTP and IM clients, and system information such as IP, location, and operating system. Redline Stealer has a customizable grabber file and can perform tasks like downloading, injecting, launching files, and opening links. Additionally, the program includes anti-duplicate logs in the panel and can blacklist countries where it will not work. The development of the Redline stealer was based on feedback from professionals involved in carding. Carding is an illicit activity that involves the use of stolen credit or debit card information to make unauthorized transactions or purchases [10]. It is considered a type of fraud and is often associated with organized crime groups.

According to Figure 2, the Redline Stealer's panel is a web-based interface that allows attackers to manage and view stolen data. The panel, hosted on a server controlled by the attacker, efficiently organizes the data collected from infected systems. It includes features such as displaying a list of logs, saving them to a specified folder or uploading them to a specified location.

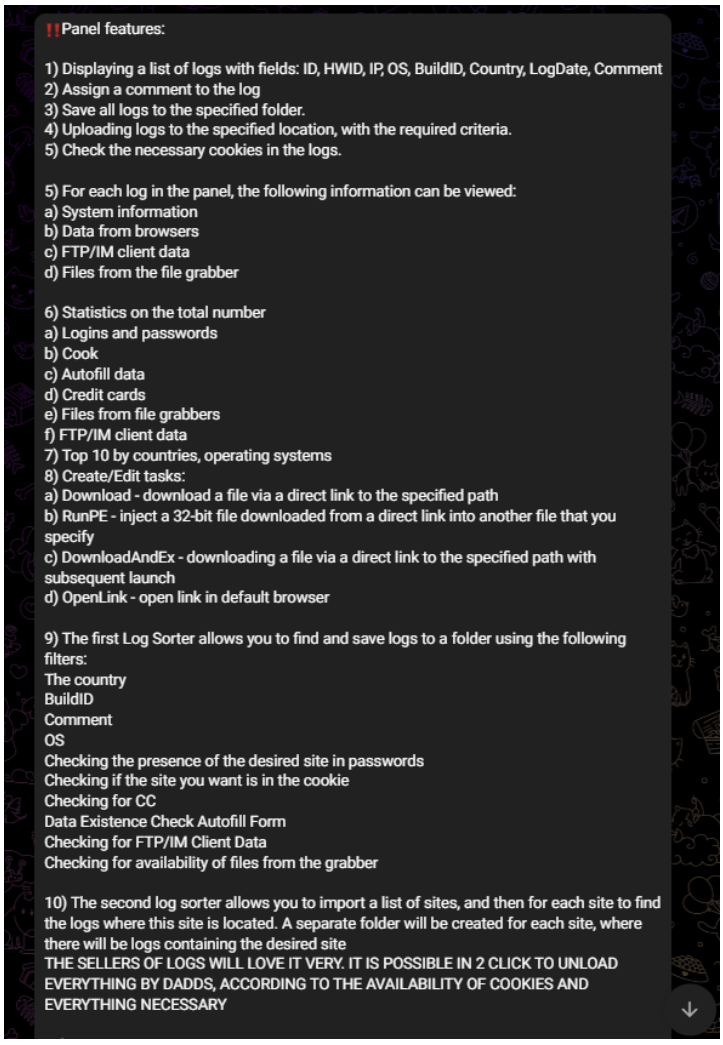

Figure 2. Panel feature from Redline's Telegram Channel.

As seen from Figure 2, the attacker can also check for necessary cookies, view system and browser data, FTP/IM client data, and files from the file grabber, as well as create and edit tasks such as downloading and launching files. The panel includes two log sorters to help the attacker find and save logs using various filters or import a list of sites and locate the logs where each site is located. Overall, the Redline Stealer's panel provides attackers with a comprehensive and efficient way to carry out their malicious activities.

The Redline Stealer has two versions: Lite and Pro, as shown in Figure 3. The Lite version costs $150/month and includes a one-month subscription to the stealer and a complimentary one-month subscription to the cryptor. The Pro version costs $900 and includes a three-month subscription to the scanner and cryptor. A cryptor is a tool designed to obfuscate the code in a malware sample so that it cannot easily be detected

using a signature-based scanner [11]. Both versions offer free updates, but the Pro version provides access to the bot for three months, which has several functions such as unlimited crypto capabilities and loader with unlimited links.

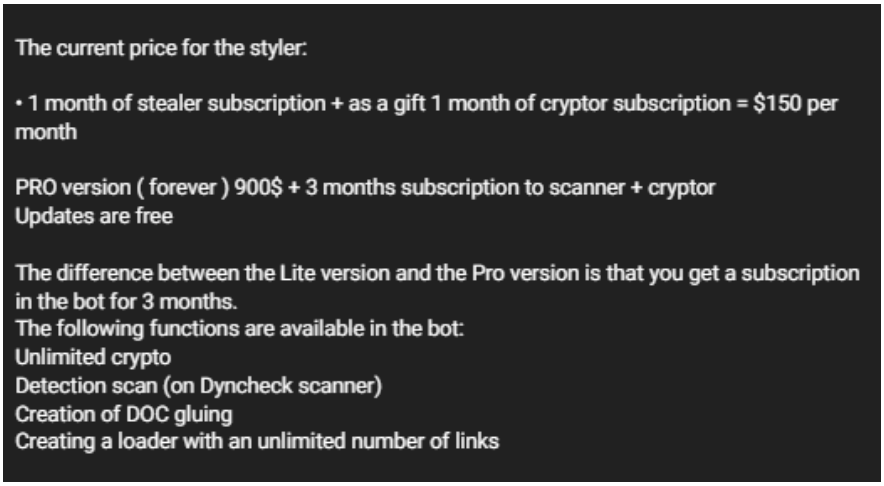

Figure 3. Pricing from Redline's Telegram Channel.

2.1.2 Redline Stolen Information in the Dark Market

Redline Malware often packages and sells the data it has stolen from a targeted machine to interested customers on the dark web [12]. The dark web is a network of unindexed websites that can only be accessed with specialist software, and it is a haven for criminal activities such as the sale of stolen information. Dark web marketplaces, such as the Russian Market, provide a platform for cybercriminals to trade in stolen data, including credit card details, login credentials, and personal identifying information [13]. These marketplaces provide a sense of anonymity and security for the buyers and sellers, with various tools and features such as Escrow[1] services and encryption to protect against fraud and detection. They also use various means to hide their identities and their transactions, including the use of cryptocurrency such as Bitcoin.

According to the cybersecurity research arm of Recorded Future, Insikt Group, the Redline Stealer malware is responsible for the vast majority of stolen credentials currently

[1] https://socradar.io/dark-web-stories-escrow/

sold on two dark web underground markets. Insikt Group's report shows that both Amigos Market and Russian Market have been identified as offering stolen credentials that originate from systems infected with Redline Stealer [12].

Despite the increasing adoption of multi-factor authentication (MFA), cyber threat actors continue to successfully combine stolen credentials and social engineering to carry out high-profile breaches, leading to increased demand for Infostealer on the dark web. Figure 4 displays the author's observations from February 2023, which reveal that there are 1,415,580 Redline Stealer logs available for purchase on the Russian market.

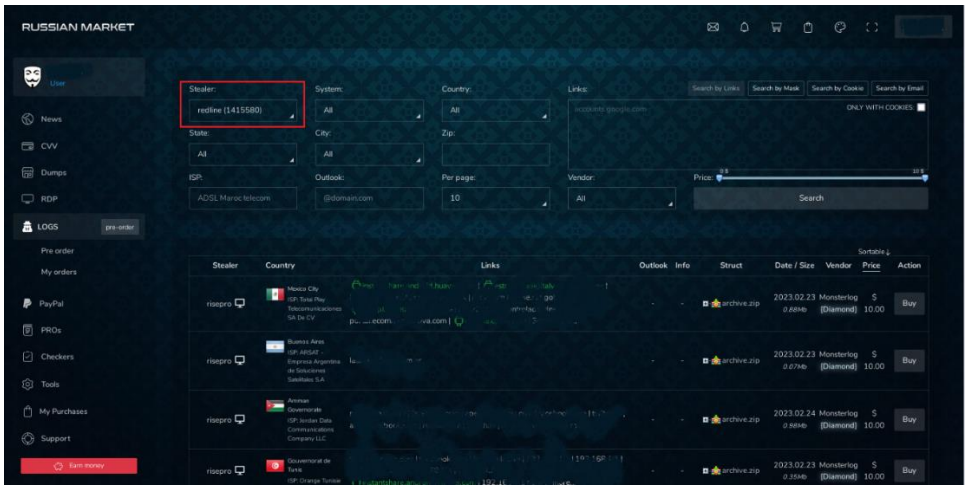

Figure 4. Russian Market filtering Redline as Stealer.

The Russian Market website enables users to search for inventory based on the type of malware used, the operating system of the victim, and the location of the victim. In terms of the volume of logs available for sale, this site was one of the most frequented markets in 2022, with victim data being sold for an average price of $10 per log. From July to October 2022, the total number of logs for sale on this market increased by almost 40%, from approximately 3.3 million to 4.5 million [3].

2.1.3 Redline Trends

According to the Malware Trends Tracker provided by ANY.RUN, as shown in Figure 5, Redline has been identified as the top malware threat in the previous 365 days and is currently ranked second in the global ranking, with a cumulative count of 51,125 indicators of compromise (IOC) as of the present day [14]. Furthermore, there have been

5,548 documented instances of URLs featuring the Redline Stealer label in the URLhaus database, and 22,378 occurrences of malware samples attributed to the Redline Stealer signature in the malwarebazaar database [15] [16].

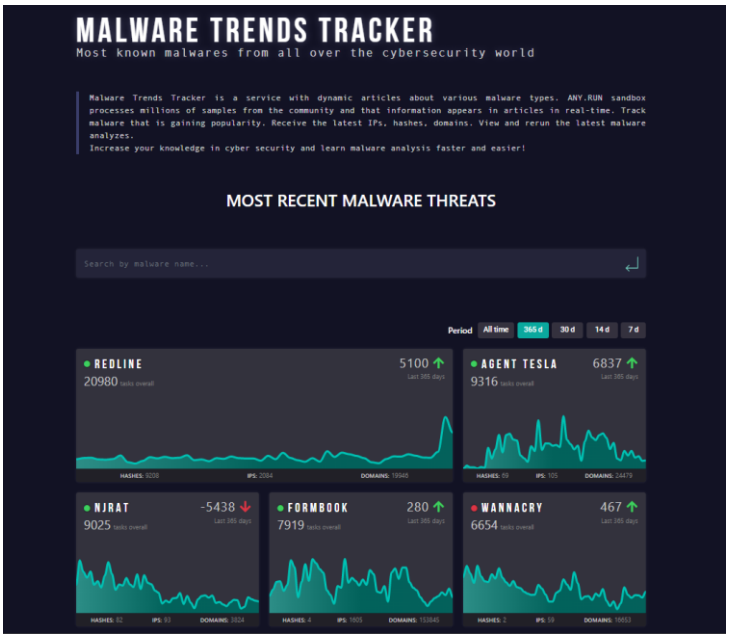

Figure 5. ANY.RUN malware trends tracker.

2.2 MITRE ATT&CK Framework

MITRE ATT&CK was created in 2013 as part of MITRE's Fort Meade Experiment to improve the detection of threats by categorizing adversary behavior. Today, it has evolved into three iterations for Enterprise, Mobile, and ICS, and is used worldwide across various fields to enhance threat detection through behavioral analysis. MITRE ATT&CK is a cybersecurity framework for understanding cyber adversary behavior that provides a common language for describing adversary actions and ways to counter them. It comprises tactics and techniques that reflect the various stages of an attacker's attack cycle and the platforms they typically target. It is an open-source framework that is accessible to all organizations and is continually updated with the latest threat intelligence and best practices. The framework is community-driven and has become a standard for security vendors to integrate their products [17].

Several cybersecurity intelligence frameworks and models exist, such as the Cyber Kill Chain, Diamond Model, OODA Loop, and the MITRE ATT&CK framework. However, the security community tends to prefer the MITRE ATT&CK framework over other

frameworks due to its detailed matrices containing attack tactics and sub-techniques. These matrices provide a comprehensive and structured view of the attack surface and help security practitioners to identify potential threats and vulnerabilities [18].

The study utilizes the ATT&CK Enterprise matrix, which comprises 14 tactics and numerous techniques and sub-techniques that encompass various stages of cyberattacks. This matrix is widely utilized in large enterprises for developing alert use cases, conducting threat hunting, and other blue team tasks.

2.3 Tools

This section discusses the main tools employed during the research, providing a brief overview of each tool.

2.3.1 MITRE ATT&CK Navigator Tool

The ATT&CK Navigator, developed by MITRE, is a web-based tool that enables users to navigate and annotate ATT&CK matrices in a simple and generic way [19]. Its main purpose is to make it easier for users to visualize the matrix and highlight cells (such as adding comments or assigning scoring values). One of its key features is the ability to define layers and combine multiple layers into one. Furthermore, the tool also includes a legend to help users associate meanings with customized colours used in the matrix. Users can open and close the legend, add, or remove items, change item colours and labels, and save the legend to the layer file.

2.3.2 MITRE Engenuity Attack Flow Builder

The Attack Flow language project has been developed and is continuously maintained by the MITRE Engenuity Centre for Threat-Informed Defense. The primary objective of this initiative is to contribute to the comprehension of adversary tactics by providing comprehensive information on the sequence and combination of offensive techniques leveraged by cybercriminals. Its purpose is to enhance threat intelligence, improve the defensive posture of blue teams, facilitate effective executive communication, promote lessons learned, and support adversary emulation and threat hunting, thereby strengthening an organization's overall security [20]. The Attack Flow Builder is a web-based tool that is both free and open-source. Its primary function is to allow users to create, view, and edit Attack Flows.

2.3.3 Hybrid Analysis Tool

Hybrid-Analysis is a cloud-based sandboxing technology that perform malware analysis to examine suspicious files and URLs, enabling organizations with quick and accurate identification and response to cyber threats. The platform provides several features, including file and URL analysis, threat intelligence feeds, dynamic behaviour analysis, static analysis, MITRE indicators and more [21]. Hybrid-analysis utilizes CrowdStrike's Falcon Sandbox, since it became part of CrowdStrike in 2017, when the company acquired Payload Security, the original developer of Hybrid-analysis [22].

2.3.4 PEStudio

PEStudio is an effective open-source malware analysis and reverse engineering tool. It provides detailed information about Portable Executable (PE) files and can assist in identifying hidden malware. PEStudio provides an in-depth analysis of PE files, differentiating whether an executable file is legitimate or potentially hazardous. It also provides information on the file's imports and exports and can identify suspicious code behaviour. In addition, it can detect the presence of anti-debugging techniques and packers that malware authors commonly employ to avoid detections.

3 Methodology

This chapter explains the research method and design used in the study to reach its goals. It outlines the steps followed to gather and analyse data, ultimately leading to the desired results.

3.1 Research Method

In the study, a mixed-methods research approach was adopted, which combined qualitative and quantitative methods to examine malware samples behaviour and associated trends on delivery phase. The qualitative aspect focused on understanding the techniques and behaviours of the malware, while the quantitative aspect involved measuring the commonness of specific techniques. This combination of methods allowed for a more detailed understanding of the research, leading to the identification of indicators and the development of well-informed defensive measures to counter the threats posed by the analysed malware samples.

3.2 Research Design

Figure 6 displays the research design for this study. The design comprises several distinct steps aimed at identifying common MITRE techniques, proposing defensive measures, and providing valuable insights into the topic under investigation.

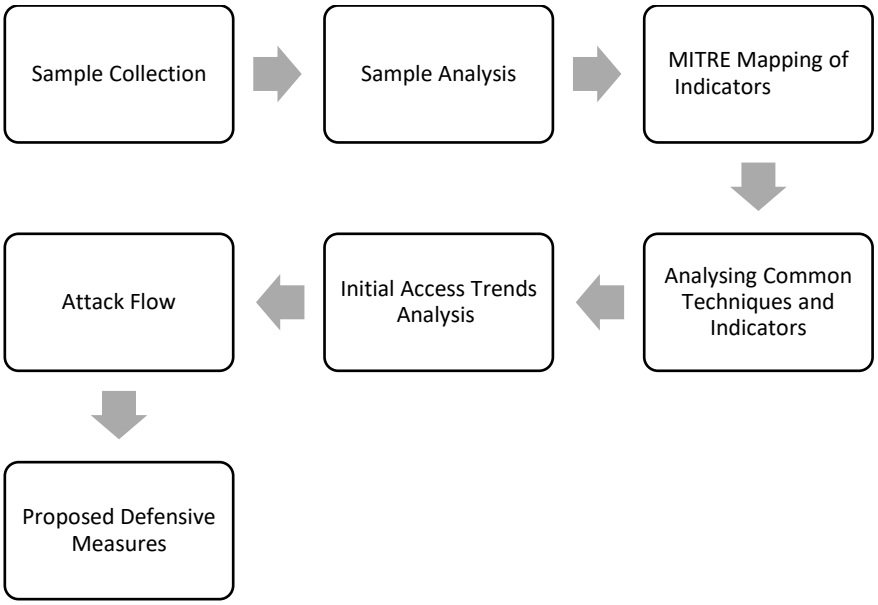

Figure 6. Research Design.

Malware samples were gathered in the first step of the research process. Due to time limitation, automated dynamic analysis was performed using an open-source sandboxing tool called "Hybrid-Analysis" to gather MITRE indicators. Additionally, Static analysis of one sample was conducted to validate the accuracy of the dynamic analysis results. MITRE mapping of indicators was then performed to correlate the collected indicators with known techniques and procedures in the MITRE ATT&CK framework. The data obtained from these steps were then analysed to identify the most frequently used techniques and procedures by the malware. In addition, since the samples were manually submitted for dynamic analysis, the analysis have not covered the initial attack tactics, as there was no information available on how the initial infection occurred. Therefore, a web-based reports review was conducted to identify the initial access techniques used by the malware in real-world cases for delivering the malware. An attack flow was created to provide a visual representation of the malware's techniques and procedures. Finally, based on the findings of the analysis, defensive countermeasures were proposed to strengthen the overall security posture of the systems against such malware attacks.

Overall, this research design intends to provide a structured approach to identify the common MITRE Techniques and proposing effective defensive measures. By utilizing these steps, the methodology employed in this study aims to ensure accuracy and provide valuable insights into the investigated topic.

4 Results

4.1 Sample Collection

For the purpose of this research, the collection of malware samples was an essential step in analysing the behaviour and characteristics of the Redline variant. Various open-source malware-sharing platforms similar to MalShare, Malware DB, MalwareBaazar, URLhaus, and other sandboxing websites were explored to obtain a collection of the most current and relevant samples. Ultimately, samples were collected from URLhaus because it links to live sites hosting malware, which is ideal for acquiring newly emerged samples. During the sample collection process, a total of 8 Redline malware samples were acquired from 8 unique and live malicious sites. In order to obtain a wide range of Redline samples, samples with different tags and characteristics, including samples in .zip, .rar, and exe formats, samples with 32-bit and 64-bit architectures, and samples with various other attributes, were collected. Specifically, 2 samples were in .rar format, 1 sample was in .net and exe format, and the rest of them were in exe format. Six of the samples had a 32-bit architecture, while the other two had a 64-bit architecture.

The sample collection was conducted in a sandboxed environment to ensure the safety of the system and prevent any potential damage caused by the malware. A Windows 10 virtual machine was employed as the sandbox environment. While attempting to download the malware samples, multiple alerts were encountered from the browser and system warning of potentially malicious content. This could have been due to the files and sites already being flagged as malicious by multiple threat intelligence platforms.

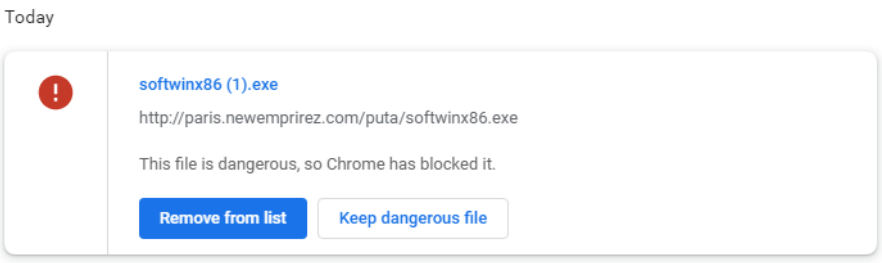

Figure 7. Browser alert while attempting to download a sample.

As displayed in Figure 8, to circumvent the alerts, the "curl" command from the terminal was used successfully to download the files. Additionally, compressed samples in .rar

format were attempted to be downloaded via Browser, and no alerts were triggered before decompressing the files.

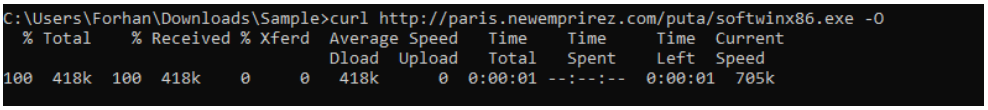

Figure 8. Successful download using "curl".

4.2 Automated Dynamic Analysis

After the collection of Redline malware samples, the next step is to conduct automated dynamic analysis in a safe and controlled environment. To achieve this, open-source sandboxing tools were used to analyse the samples. There are several options available, such as Cuckoo, Hybrid-analysis, Polyswarm, Any.Run, Triage, and Joe Sandbox. For this research, Hybrid-analysis was selected due to its capabilities with the MITRE ATT&CK Matrix and the fact that it does not require registration for sample submission.

The samples were uploaded to Hybrid-analysis with the purpose of collecting MITRE ATT&CK indicators. The submission of the file was carried out in a sandbox environment, where the operating system selected was Windows 10 64-bit Professional version 10.0 (build 16299). Outbound network traffic simulation was enabled during the analysis, and the resulting reports were generated using Falcon Sandbox v9.5.7©Hybrid-analysis. The URLs for the reports on the malware samples can be found in Appendix 2.

The purpose of automated dynamic analysis is to observe the behaviour of the malware in a controlled environment and extract useful indicators to identify the common pattern among different samples. The MITRE ATT&CK indicators were acquired from the dynamic analysis and analysed for the common pattern.

4.3 Static Analysis

Static analysis was conducted to better understand the behaviour of the malware and how indicators were discovered in the dynamic analysis process. Due to time limitations, the analysis was performed on a single sample named "Kiddions ModMenu.exe."

The static analysis of "Kiddions ModMenu.exe" involved examining the file's information, embedded imports, strings, and functions. This process allowed identifying indicators of compromise and better understand the malware's potential capabilities. The results of the static analysis were compared with the findings from the Hybrid-Analysis to ensure consistency and accuracy.

The information obtained during the malware analysis was discovered through the utilization of the PEStudio Tool. Figure 9 shows the information found on the File-Header section; File was compiled on Thu Feb 16 15:25:39 2023 UTC. The malware's signature was identified as 0x00004550 (PE00).

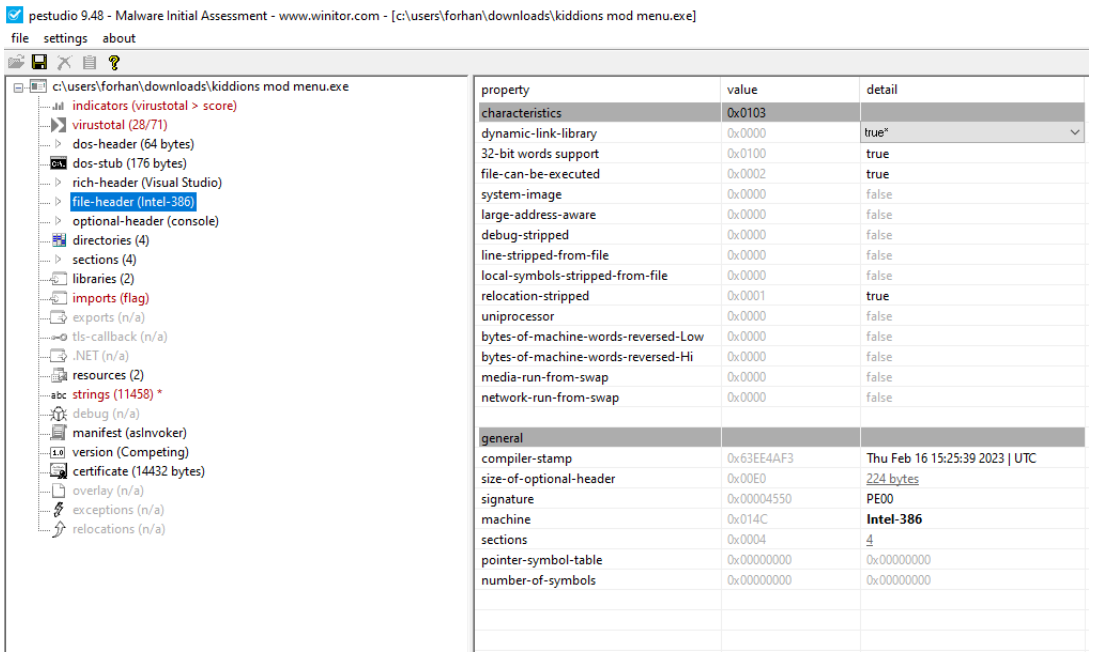

Figure 9. PEStudio File-Header section.

As shown in Figure 10, The Version section of this sample revealed significant information about the malware, including its executable file-type and its MD5 and SHA1 hashes. The malware was found to have an internal name of "Punctuate", and an original name of "Competing". Its file description was noted as "Paradoxical outsiders soldering talons candles ontogeny". Moreover, the malware had comments attached to it, stating "Revival wilful perchlorate exudate spill iridescent". While the significance of these descriptions and comments remains unknown, it is possible that they were added to the file to obfuscate the code or serve as a marker for the malware's creators.

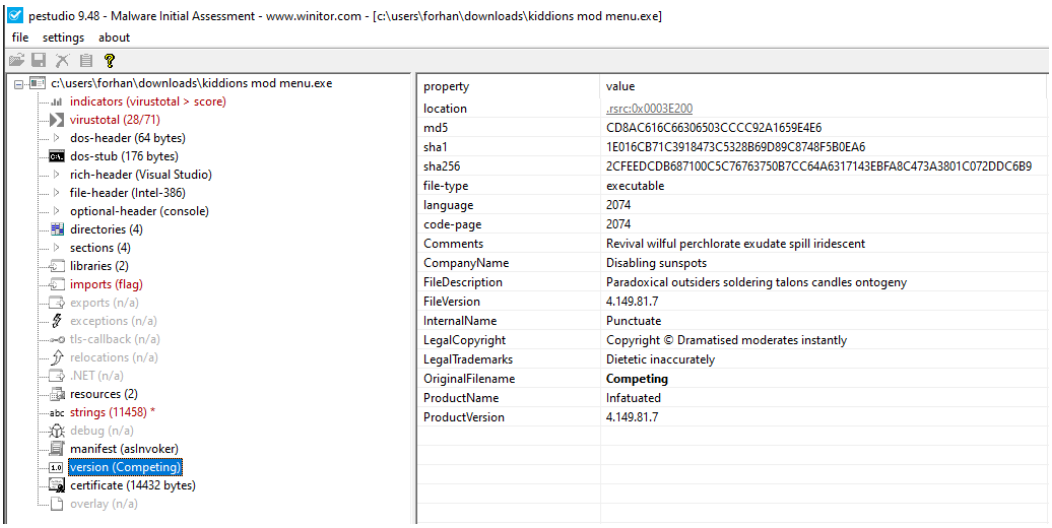

Figure 10. PEStudio Version section.

Figure 11 shows the malicious file contains 4 sections named .rdata, .rsrc, .data and .text. and the malware entry point was identified as 0x00006D42.

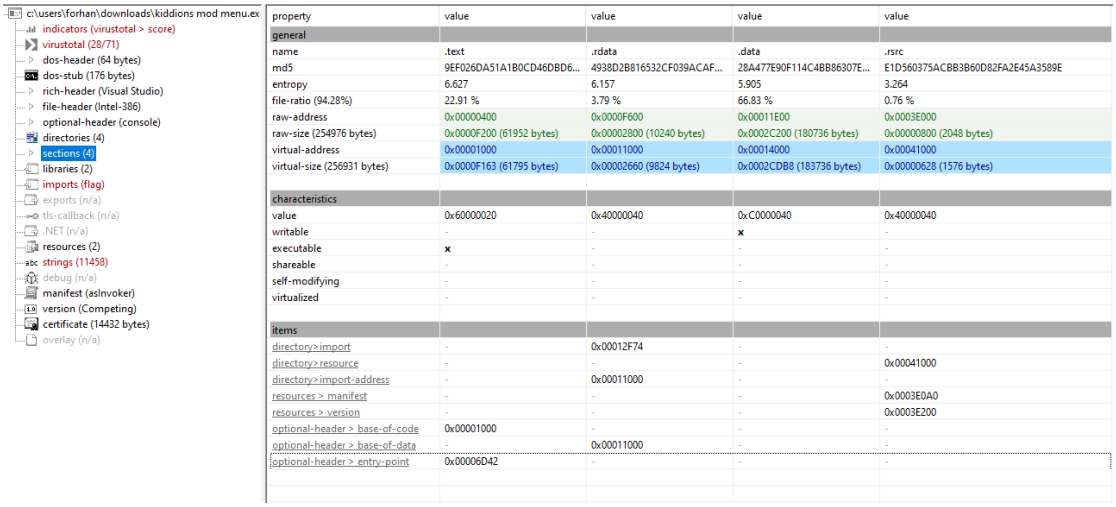

Figure 11. PEStudio Sections section.

Figure 12 shows that, the malware imports 2 libraries kernel32.dll and user32.dll, These libraries are commonly used by Windows-based applications, and their use by malware may indicate an attempt to blend in with legitimate software or to evade detection. Additionally, multiple flagged imports have been discovered that correlate with the indicators found in the Hybrid-Analysis. These flagged imports are indicative of various MITRE techniques employed by the malware to evade detection and modify its behaviour.

It uses the T1106: Native API Technique to retrieve the command line string and obtain the full path of the executable file using "GetCommandLineA@KERNEL32.DLL" and "GetModuleFileNameA@KERNEL32.DLL," respectively. The T1543: Create or Modify System Process Technique is used to retrieve startup information with "GetStartupInfoA@KERNEL32.DLL" and GetCurrentProcess@KERNEL32.Dll" imports. The malware also employs the T1622: Debugger Evasion Technique to evade analysis by checking if the current process is being debugged with the "IsDebuggerPresent" import. The T1497: Virtualization/Sandbox Evasion Technique involves imports like "GetTickCount@KERNEL32.DLL" and "Sleep@KERNEL32.DLL," which can detect sandbox environments and delay the malware's execution. Additionally, the T1082: System Information Discovery Technique uses the "GetModuleHandleA@KERNEL32.dll" import to locate and manipulate other modules in the system.

In the following section of this study, the techniques observed during the static analysis are explained in more detail.

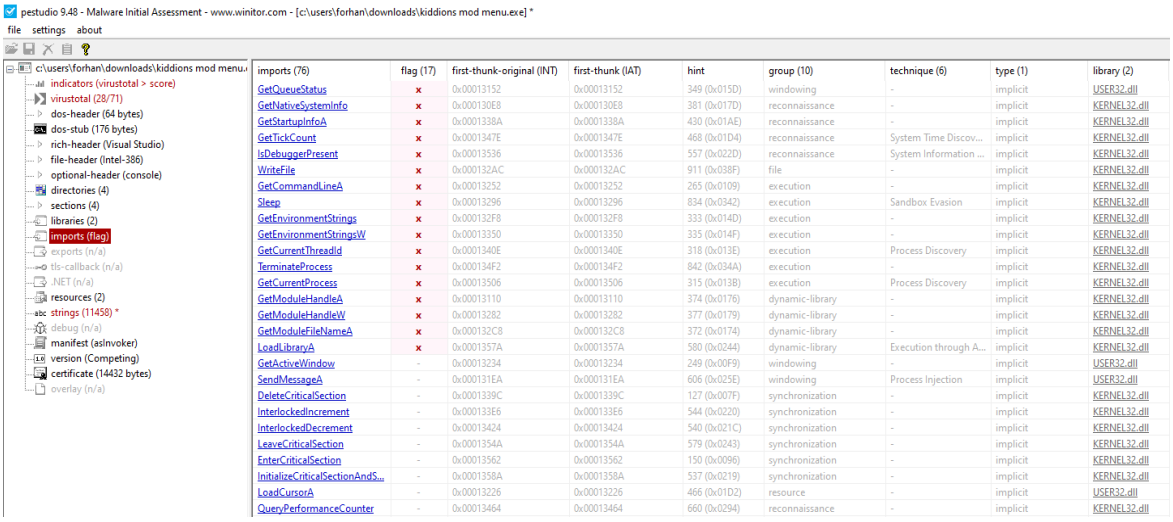

Figure 12. PEStudio Imports section.

The manifest section shown in Figure 13 is used in defining the security and execution level requirements for a Windows executable file. According to the manifest found in the malware the following segment of the code-snippet

```
"<requestedExecutionLevel level="asInvoker"
uiAccess="false"></requestedExecutionLevel>"
```

specifies the execution level required by the assembly. The assembly is requesting to run with the "asInvoker" level, which means that it will run with the same permissions as the user who launched it. The "uiAccess" attribute is set to "false", which means that the assembly does not require UI access, Hence, it was found that the sample did not exhibit indicators of attempting to gain elevated privileges.

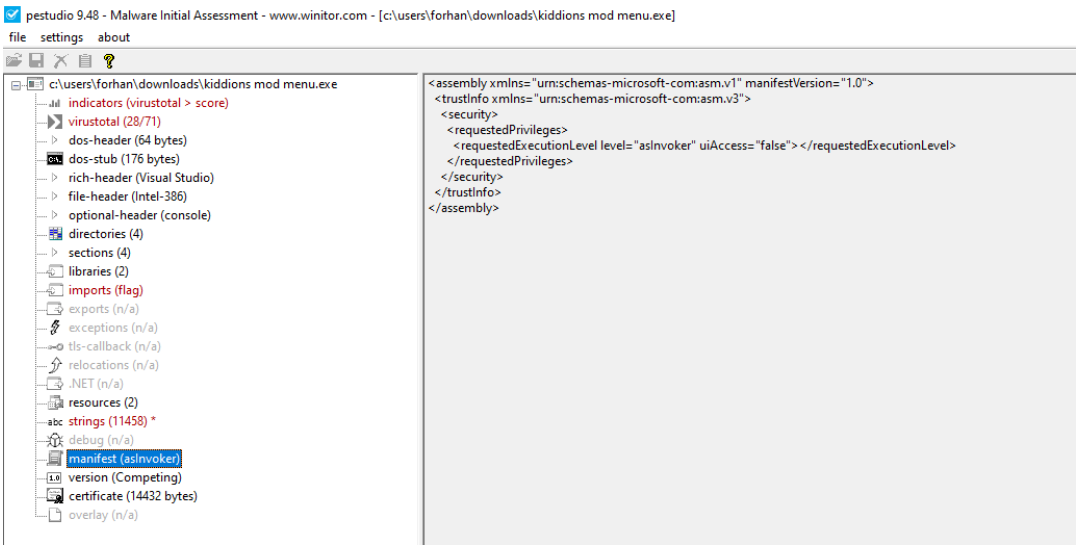

Figure 13. PEStudio Manifest section.

In conclusion, the indicators obtained from the static analysis of the malware sample were found to match those of the dynamic analysis, which also helped in understanding how the dynamic analysis results were achieved. This process improved the accuracy of the findings and the overall research quality.

4.4 Identifying common MITRE Technique

In this section, the MITRE Attack Navigator tool was utilized to analyse and compare collected samples across various layers. The study utilized the Enterprise ATT&CK v12 domain and filter of Windows platform in the Navigator tool. MITRE Techniques identified from the Hybrid-Analysis were mapped into separate layers for each sample. Another layer was created by combining all the samples layers into one to compare and identify the common MITRE Indicators among them. These layers were saved as JSON files, which can be utilized in other applications or combined with other layers for future

analyses. The JSON files for all the layers were exported and made available on a GitHub repository [23].

Figure 14 displays an additional layer which was created by mapping only the common techniques that appear in at least 5 out of 8 samples. In this context, the term 'common' refers to a characteristic that is seen in the majority, and in this case, a technique observed in 5 or more samples is considered common. Each sample exhibits its own set of indicators. However, this study focused on finding the common MITRE techniques to better understand the malware's behaviour and narrow down the attack flow to the most observed techniques. This approach also helps in proposing defensive measures in a more concise manner. The legend in the figure indicates score expression based on the colour, which reflects the number of samples that match a particular technique.

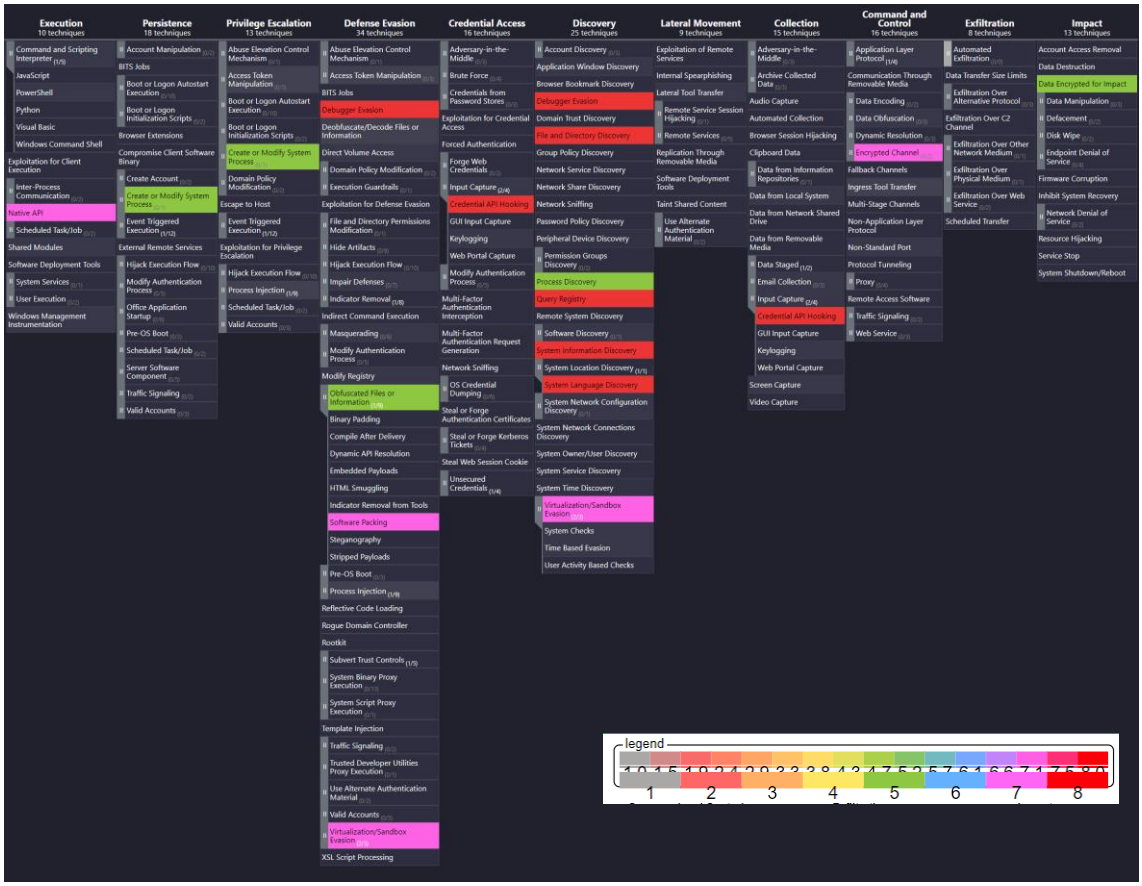

Figure 14. ATT&CK Navigator Common Techniques Layer[1].

[1] The full resolution figure can be found at https://raw.githubusercontent.com/FothulForhan/Thesis_Infostealer/main/MITRE%20Attack%20Navigator/Common_Techniques_Mapping.svg

4.5 Analysing Common Techniques and Indicators

This section aims to explain the common techniques discovered in the previous step. For better understanding, each technique is explained along with its respective tactic. Additionally, the section includes brief description of the identified techniques and the indicators observed in the sample analysis results. The obtained indicators were subjected to meta-analysis to achieve detailed understanding of their meaning and to confirm their correlations with respective techniques.

4.5.1 TA0002: Execution

Execution tactic consists of techniques that can be used by attackers to run malicious payloads on the victim's system. Execution tactic is helpful in understanding how attackers are able to effectively deploy their malicious code onto victim's systems, bypassing defenses and gaining unauthorized access. There are a total of 13 techniques within this tactic. The technique T1106: Native API was observed in 7 out of 8 analysed samples.

T1106: Native API technique involves adversaries exploitation the native operation system's (OS) application programming interface (API) in executing the malicious behaviour.These APIs are leveraged by the OS during system boot and routine operations, and are also exposed to user-mode applications via interfaces and libraries. Abuse of such API is often attempted to bypass the defensive tools [24]. Based on the results of automated dynamic analysis conducted using Hybrid Analysis, common indicators seen for this technique were :

- Ability to retrive the command-line string from the current process.

  "GetCommandLineA@KERNEL32.DLL" was detected

- Ability to retrieve the fully qualified path of module.

  "GetModuleFileNameA@KERNEL32.DLL" was detected

- Ability to dynamically determine API calls

  "GetProcAddress()" and "LoadLibraryA()" were found in a import section.

- Calls an API typically used to create a process.

  "*Sample.exe"* called "CreateProcessW" with parameter "%WINDIR%\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe"

4.5.2 TA0003: Persistence

Persistence tactic comprise techniques utilized by attackers to maintain a foothold in a compromised system. This tactic clarifies how attackers can establish long-term access to a targeted system. There are a total of 19 techniques within this tactic. Among the analysed samples, the common technique found in this tactic was T1543: Create or Modify System Process, with 5 out of 8 samples matching this technique.

This technique is what adversary uses in establishing persistence by installing or modifying services, daemons or agents that execute at bootup of an OS or a regular interval [25]. Common indicators for this technique were:

- Ability to retrieve the contents of the STARTUPINFO structure.

  "GetStartupInfoW@KERNEL32.dll" was detected.

  "GetStartupInfoA@KERNEL32.DLL" was detected.

4.5.3 TA0004: Privilege Escalation

Privilege Escalation tactic consists of techniques that can be used by adversary to gain higher-level permissions on a system or network. There are a total of 13 techniques within this tactic. Within the MITRE ATT&CK framework, it has been observed that some techniques can appear in multiple tactics. An example of this is the common technique T1543: Create or Modify System Process, which is present in both Persistence and Privilege Escalation tactics. A brief explanation of this technique has been provided earlier in Persistence tactic.

4.5.4 TA0005: Defense Evasion

Defense Evasion involves techniques that help adversaries avoid detection during a compromise. This tactic is useful in understanding how attackers remain undetected within a targeted system. Some other tactics also overlaps with Defense Evasion when they provide the added benefit of bypassing defenses. There is a total of 42 techniques within this tactic. The common techniques found in the analysed samples were T1622: Debugger Evasion, detected in all the analysed samples (8 out of 8 samples matched); T1497: Virtualization/Sandbox Evasion, with 7 out of 8 samples matching; and T1027: Obfuscated Files or Information, seen in 5 samples. Additionally, sub-technique

T1027.002: Obfuscated Files or Information: Software Packing was discovered in 7 of the 8 samples.

T1622: Debugger Evasion technique involves adversaries detecting and evading debuggers used by defenders to trace and analyse potential malware payloads. They do this by altering their behaviour based on checks for the presence of debugging artifacts. The checks may involve Native API function calls or manually checking the Process Environment Block, and if a debugger is detected, adversaries may modify their malware to disengage from the victim or conceal the core functions of the implant [26]. This technique has been detected in all the analysed samples. The indicators observed for this technique include:

- Ability to Create guarded memory regions (anti-debugging trick to avoid memory dumping)

  "sample.exe" is allocating memory with PAGE_GUARD access rights.

- Found debugger evasion API strings.

  The string: "IsDebuggerPresent" was detected.

- Containing ability to register a top-level exception handler (API string)

  API string: "SetUnhandledExceptionFilter" was detected.

  API string: "UnhandledExceptionFilter" was detected.

- Containing ability to register a top-level exception handler (often used as anti-debugging trick)

  SetUnhandledExceptionFilter@KERNEL32.dll was detected.

T1497: Virtualization/Sandbox Evasion involves adversaries detecting and avoiding virtualization and analysis environments by altering their behaviours based on checks for the presence of artifacts indicative of a virtual machine environment or sandbox. If a virtualization or analysis environment is detected, adversaries may modify their malware to disengage from the victim or conceal the implant's core functions [27]. Common indicators detected in this technique are:

- Containing ability to delay the execution of current thread.

  Sleep@KERNEL32.DLL was detected.

- Containing ability to detect virtual environment (API)

GetTickCount@KERNEL32.DLL was detected.

T1027: Obfuscated Files or Information is a technique in which attackers use encryption, encoding, or obfuscation to hide executable signatures, allowing them to evade signature-based detection methods. Indicators for this technique have been discovered in 5 of the collected samples.

- Cryptographic related strings were found.

  “md5cryptoserviceprovider, System.Security.Cryptography,

  tripledescryptoserviceprovider, createdecryptor”

T1027.002: Software Packing is a sub-technique of T1027: Obfuscated Files or Information. Software Packing involves compressing or encrypting an executable, altering its file signature to bypass signature-dependent detection. Most unpacking approaches decompress the code within the memory [28]. The indicators of this sub-technique were:

- PE files detected having higher entropy sections.

4.5.5 TA0006: Credential Access

Credential Access tactic consist of techniques aimed at stealing credentials such as usernames and passwords. There is a total of 17 techniques within this tactic. The sub-technique T1056.004: Credential API Hooking has been discovered in all 8 of the analysed samples.

T1056.004: Credential API Hooking is a Sub-Technique of the technique Input Capture. It involves adversaries utilizing hooking mechanism in intercepting windows API functions and gathering user’s credentials. This sub technique has been discovered in all 8 of the samples. Common indicators detected for the sub-techniques are:

- Hooking API calls.

  "Wow64Transition@NTDLL.DLL were seen in *"sample.exe"*.

- Installs hooks along the running process.

4.5.6 TA0007: Discovery

The Discovery tactic comprises techniques that are used by attackers to gather information about systems and networks. This tactic explains adversary’s techniques for

exploring the environment to identify potential targets and gather information to plan their next steps. Discovery is essential for the success of stealing malware, and attackers often employ a range of techniques to identify vulnerable systems and data sources. There are a total of 30 techniques within this tactic. Several common techniques were found in the sample analysis process, including T1083: File and Directory Discovery, T1012: Query Registry, T1082: System Information Discovery, and sub-technique T1614.001: System Language Discovery, which were detected in all the samples. Additionally, Process Discovery was observed in 5 out of 8 samples. The techniques T1622: Debugger Evasion and T1497: Virtualization/Sandbox Evasion overlap in both Discovery and Defense Evasion tactics; both techniques have been briefly explained earlier. The high number of techniques related to Discovery tactic detected in the Redline Stealer samples suggests that the malware is designed to perform reconnaissance on the victim system and identify potential targets for data theft.

T1083: File and Directory Discovery technique includes adversaries using command shell utilities or custom tools in discovering specific information within a file system [29]. Common indicators noted for these techniques are:

- Calling an APIs typically used for searching a directory for a file.

  "sample.exe" called "FindFirstFileW".

- Attempting to access non-existent files.

  "sample.exe" trying to access non-existent file "%WINDIR%\System32\WOW64LOG.DLL".

  "sample.exe" trying to access non-existent file "C:\FLTLIB.DLL".

Registry contains vital information about the OS, configuration software and security. The technique T1012: Query Registry involves interacting with Windows Registry to gather such information [30]. Common indicators detected in this technique are:

- Monitoring specific registry key for changes.

  "sample.exe" monitors "\REGISTRY\MACHINE\SOFTWARE\Microsoft\Ole"

  "sample.exe" monitors "\REGISTRY\USER\S-1-5-21-735145574-3570218355-1207367261-1001_Classes\Local Settings\Software\Microsoft"

- Reading the active computer name.

"sample.exe" queried the registry key (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME"; Key: "COMPUTERNAME")

- Reading information about supported languages.

  "sample.exe" queried the registry key (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE"; Key: "EMPTY")

  "sample.exe" queried the registry key (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\EXTENDEDLOCALE"; Key: "EN-US")

  "sample.exe" queried the registry *key* (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE"; Key: "EN-US")

T1082: System Information Discovery technique is collecting system information, including OS, hardware, and architecture information to tailor attacks. Windows utility "systeminfo" is often used in conducting such technique in Windows OS [31]. The indicators observed for this technique include:

- Calling an API typically used to retrieve information about the current system.

  "sample.exe" called "GetNativeSystemInfo".

- Containing ability to retrieve a module handle for the specified module.

  GetModuleHandleA@KERNEL32.dll

- Containing ability to query CPU information.

  cupid[1] from *"sample.exe"*

T1614.001: System Language Discovery sub-technique involves adversaries gathering system language information to determine a victim's geographical location, influencing their attack strategy. Various data sources, like system defaults and keyboard layouts, can be used to infer system language. Techniques may involve in Query Registry or using Native API functions [32]. The indicators observed in the T1012: Query Registry technique is consistent with those found in the System Language Discovery sub technique.

[1] https://iq.opengenus.org/cpuid/

T1057: Process Discovery technique is gathering information on running processes to understand common software and applications, shaping their attack strategy. In Windows, they can use command like “Tasklist” or “Get-Process” to obtain information about running processes on their system. Additionally, adversaries can also enumerate processes via Native API calls [33]. Common indicators seen in the samples for this technique were :

- Containing ability to enumerate processes/modules/threads.

  Module32Next@KERNEL32.DLL from *sample.exe.*

- Calling an API typically used for taking snapshot of the specified processes.

  "sample.exe" called "CreateToolhelp32Snapshot”.

4.5.7 TA0009: Collection

The Collection tactic comprises techniques that are employed by attackers to gather data of interest, such as sensitive information or system configurations. There are a total of 17 techniques within this tactic. Upon analysis, the common sub-technique T1056.004: Input Capture: Credential API Hooking was identified. This sub-technique was also previously discovered in the tactic Credential Access and has been explained earlier.

4.5.8 TA0011: Command and Control

The Command-and-Control tactic includes techniques that adversaries employ to communicate with compromised systems from a victim's network. This tactic is crucial for understanding how attackers maintain and control their presence on the infiltrated systems. There are a total of 16 techniques within this tactic. In the analysed samples, the common technique T1573: Encrypted Channel was identified as matching in 7 of the samples.

T1573: Encrypted Channel technique is using known encryption algorithm to hide command and control traffic, instead of relying on protocol-based protections. Indicators discovered in this technique is:

- Sample making suspicious HTTPS connections using insecure TLS/SSL version.

  Connection was made using TLSv1.1

4.5.9 TA0040: Impact

The Impact tactic comprises techniques that adversaries use to disrupt, destroy, or manipulate systems, data, or networks. This tactic explains how attackers inflict damage or achieve their end goals after infiltrating systems. There are a total of 13 techniques within this tactic. The technique T1486: Data Encrypted for Impact was seen as the common technique for this tactic.

In this technique adversaries uses encryption to disrupt access to system resources and data, often targeting common user files. Encryption malware may spread across networks, targeting local and remote drives, as well as cloud storage [34]. The indicators associated with this technique are related to YARA signature matches for possible RC4 encryption. However, upon careful examination, it becomes apparent that this indicator may not be accurate, as there is no supporting indicators or additional information about this technique's match with the collected samples.

4.6 Initial Access Trends Analysis

The techniques utilized by cybercriminals to gain initial entry into a targeted computer are collectively known as Initial Access. The Redline Malware family, which has been evolving over time, employs various delivery strategies to ensure successful penetration of target computers. As previously mentioned, the indicators from the initial access tactic are not covered by the results obtained from dynamic analysis due to the samples being submitted manually. Therefore, a web-based reports review was conducted to analyse the initial access trends observed by this malware in real-life cases. This section discusses the techniques identified from the Initial Access Trends analysis.

4.6.1 T1566: Phishing

Cybercriminals utilize this social engineering technique to trick consumers into disclosing sensitive information, such as login credentials. Attackers construct convincing and legitimate-looking phishing emails. Emails could include links or attachments that, when opened, download malware onto the target system.

According to Viettel Security's report [35], phishing campaigns containing Redline Stealer taking advantage of COVID-19 vaccine issues were seen in early 2020. The technique of spreading the malware through phishing continued, and it was once again

seen in very high volume around April 2022 [36]. The emails sent out contained malicious attachments, and opening the attachment would start the process of installing the malware. The study conducted by Cyble Research & Intelligence Labs (CRIL) revealed that Redline Stealer was being circulated through fake VPN sites, with phishing as the preferred method of targeting users [37]. Specifically, the threat actors behind this campaign created fraudulent websites and sent phishing links to direct users to download them. While collecting the samples for this study from URLhaus, it was observed multiple malicious Dropbox links ended with *"?dl=1"*. In a URL, the query parameter *"dl=1"* typically indicates that the resource being accessed should be downloaded. *"dl"* stands for "download," and the value *"1"* indicates that the download should be triggered. This process forces the browser to download the contents of a link instead of displaying it [38]. Such links could be embedded into phishing emails, and thus clicking them would result in downloading the malware without the user noticing.

In September 2022, The Redline malware was released via hacking 2K Games' customer care website [39]. Attackers sent phishing emails with a malware attachment posing as a video game patch from the support website. More recently, in early 2023, researchers from Rapid7 discovered that Microsoft OneNote has been used to spread the malware [40]. Cybercriminals have been creating fake OneNote pages and sharing them with victims via phishing emails, with the pages containing malicious code that downloads and executes the Redline malware. These attacks highlight the continued threat posed by phishing technique in distributing Redline malware.

4.6.2 T1189: Drive-by Compromise

T1189: Drive-by Compromise is a technique which can be used by adversaries to gain access to a system by exploiting a user's normal course of browsing [41]. Various methods of this technique have been observed and reported in the delivery of Redline Stealer.

Malvertising is a method used by attackers to spread the Redline stealer by inserting malicious code into internet advertisements that are shown on trustworthy websites [42]. When a person hits the advertisement, the code runs on their computer, downloading and installing the Redline stealer. For example, the attacker could pay for advertising space on a popular website and then put malicious code in the ad. The code may be meant to trick the user into downloading and installing the Redline malware on their system or to take advantage of flaws in the user's web browser or other software. According to

Spamhaus, Malvertising increased at the start of 2023 [43], with different variants of Infostealer malware being sent to user's devices through Google Ads. The bad actors behind these attacks are impersonating reputable brands like Adobe Reader, Gimp, Microsoft Teams, OBS, Slack, and Thunderbird to distribute various Infostealer malware, including Redline malware. Like this campaign, Redline was seen associated with the advertisement of fake MSI Afterburner download portals [44], mimicking a website associated with well-known software like Notepad++ and Blender 3D [45] and multiple other Malvertising campaigns.

Exploit kits, also known as exploit packs, are software toolkits used by cybercriminals to exploit system vulnerabilities and perform malicious activities, such as malware distribution [46]. When a user visits a hacked website, the exploit kit attempts to use a browser or other software flaw to infect their machine with malware. Exploit kits may not be as prevalent as they once were, but they still pose a significant threat to users whose web browsers have not been updated. Bitdefender discovered early in 2022 a RIG Exploit Kit campaign that exploited the CVE-2021-26411 Internet Explorer vulnerability to distribute Redline Stealer [47]. CVE-2021-26411 is a vulnerability in Internet Explorer that causes memory corruption when a specially crafted website is visited [48].

The adversaries responsible for the Redline malware have been improvising and developing new techniques to spread the malware across the internet. It has been reported on multiple occasions that these techniques are spread via social media platforms. According to a recent report [49], there has been an approximate 200–300% month - to - month growth in YouTube videos containing links to stealer malware since November 2022. Most of these videos are generated by artificial intelligence posing as tutorials on how to download cracked versions of licensed software thus luring victims into downloading malicious software. Additionally, Kaspersky reported on a campaign targeting YouTube users [50], which utilizes Redline Stealer to propagate itself to users YouTube channels, spreading through videos that advertise game cheats and cracks, ultimately leading users to the malware itself. Kaspersky has noted that the campaign is an example of how stealth-type malware is distributed under the guise of game hacks. Like YouTube, Redline Stealer has been observed spreading through compromised Facebook business pages [51].

4.7 Attack Flow

As mentioned earlier, the MITRE Engenuity Attack Flow tool was used to construct the attack flow presented in this thesis. The attack flow has been presented with the aim of providing a clear understanding of the various stages involved in Redline Malware. The flow was developed based on the common pattern of MITRE techniques observed in the previous sections of this thesis. The built attack flow has been saved as *.json format and uploaded to the GitHub repository, making it accessible to other security professionals who wish to study, collaborate, or build upon the work. Due to space limitation in this document the attack flow has been divided into multiple figures. Full figure[1] can be accessed in the GitHub repository [23].

Figure 15 shows the primary initial access tactic used by malware involve phishing or drive-by compromise techniques, which deliver the malware to the victim's device.

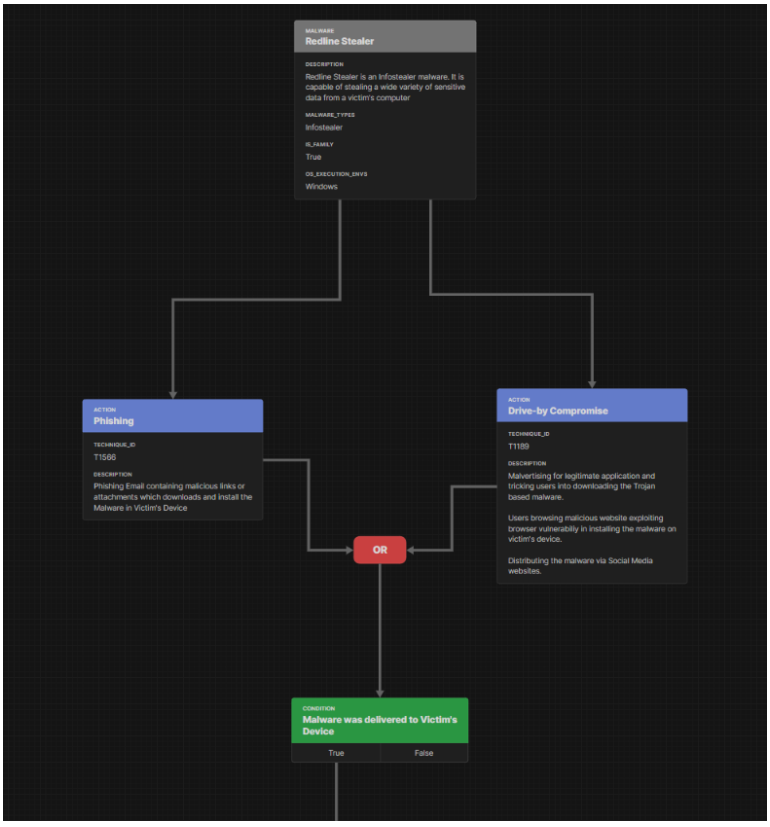

Figure 15. Attack Flow Initial Access.

[1] The full resolution figure can be found at https://raw.githubusercontent.com/FothulForhan/Thesis_Infostealer/main/MITRE%20Attack%20Flow/Redline_Malware_Attackflow.png

Figure 16 displays that once the malware is delivered to a victim's device, it employs Native API technique which takes advantage of the native operating system's (OS) application programming interface (API) to carry out the execution of the malware.

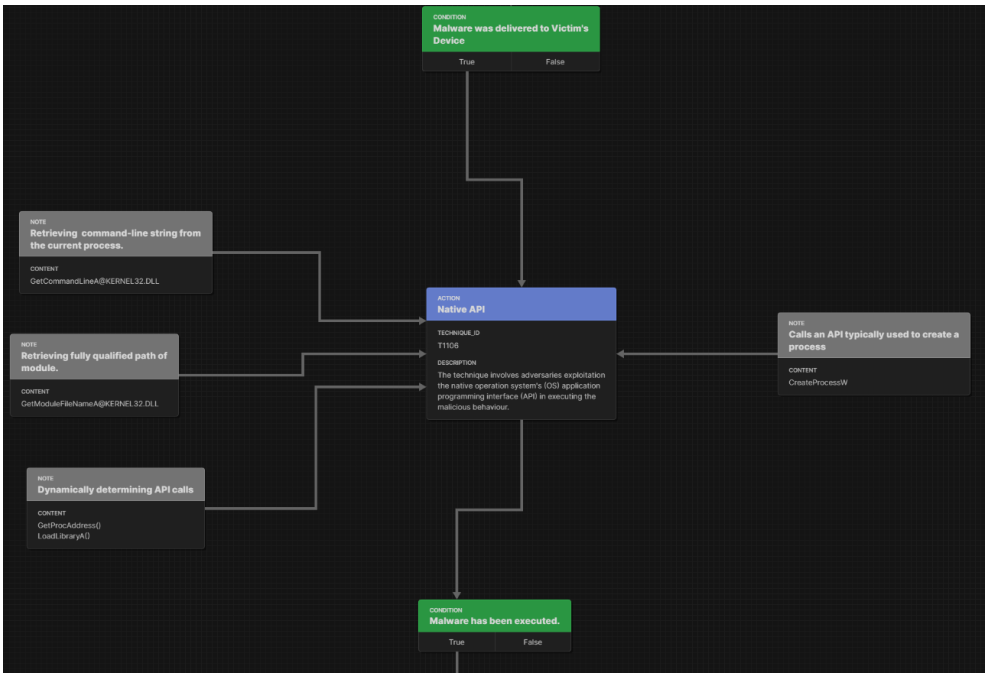

Figure 16. Attack Flow Execution.

Figure 17 shows a segment of the attack flow, demonstrating that upon execution of the malware on the victim's device, it tends to utilize the Create or Modify System Process technique. This technique is employed to establish and maintain a foothold within the victim's device, ensuring the persistence of malware and furthering into the next steps.

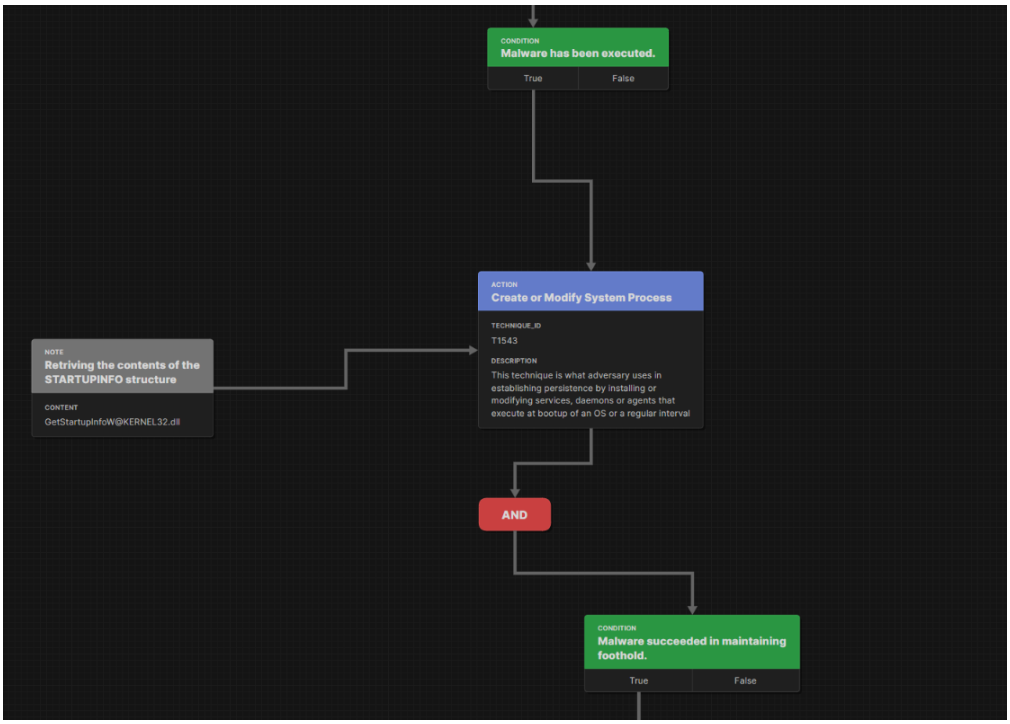

Figure 17. Attack Flow Persistence.

Figure 18 shows the part attack flow containing techniques which are employed to avoid detection within the victim's device.

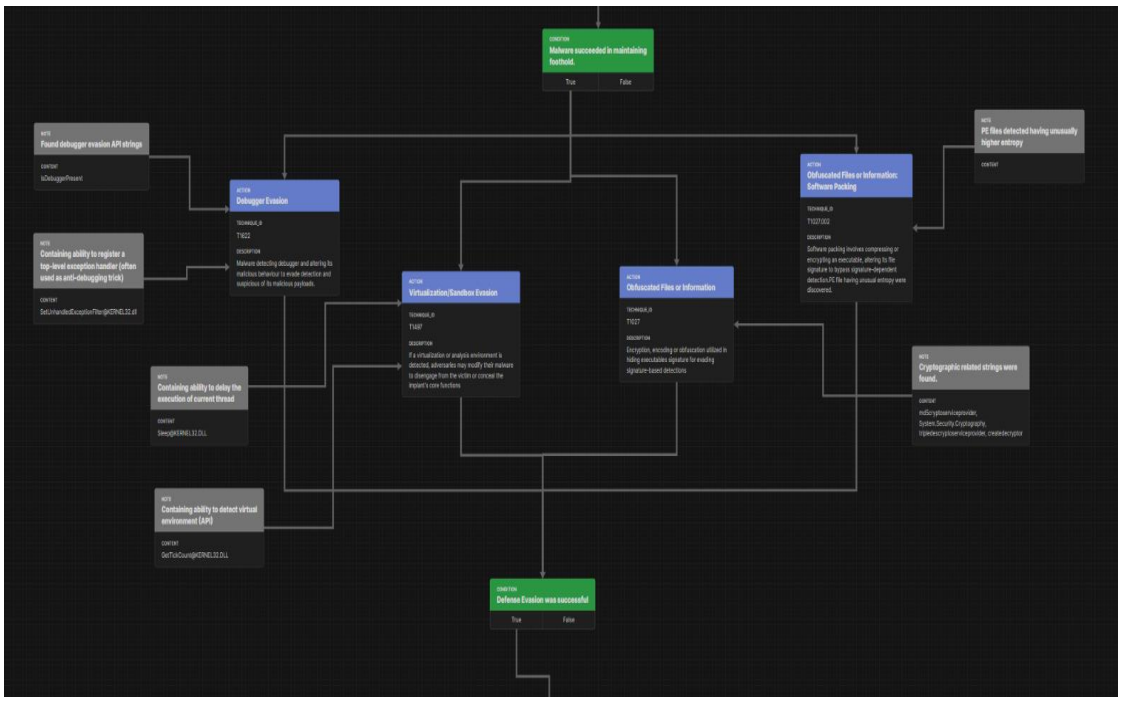

Figure 18. Attack Flow Defense Evasion.

Figure 19 illustrates the attacker's techniques for collecting sensitive data from the compromised systems and exfiltrating the collected information.

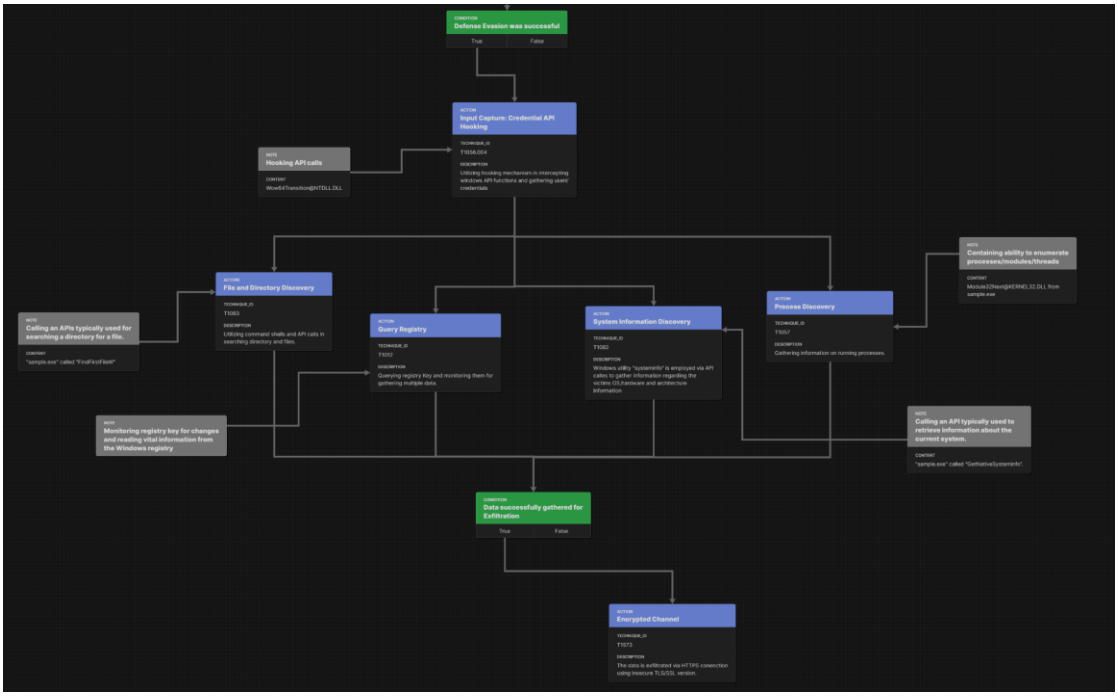

Figure 19. Attack Flow data gathering and exfiltration.

4.8 Proposed Defensive Measures

Redline Stealer malware has emerged as a significant threat to organizations, as it is a highly sophisticated and stealthy Trojan that is designed to steal sensitive data. To counter this threat, implementing effective defensive measures is essential, as it can help to prevent, detect, and respond to Redline Stealer attacks. This section talks about some of the proposed defensive measures that can be employed to mitigate the risk of Redline Stealer malware infections.

4.8.1 Employee education

In any organization's cybersecurity strategy, educating employees is a crucial component as the human factor remains a significant vulnerability in combatting malware attacks. As identified in the Initial Trends Analysis section, Redline Stealer gains its initial foothold in a victim's device through social engineering attacks and/or manipulating users into downloading malicious executables through drive-by compromise without their knowledge of the harm or impact. Educating employees on best practices for email and

web browsing, as well as the risks of phishing and social engineering, can decrease the chances of a malware infection. Regular training on identifying and avoiding social engineering techniques, such as phishing emails and other deceptive tactics, is critical since employees are the primary targets of such attacks.

According to the Ponemon Institute's research [52], employee training can lower the likelihood of a successful phishing attack by up to 70%. Furthermore, the National Institute of Standards and Technology (NIST) recommends that organizations implement a comprehensive security awareness and training program that includes regular training on common threats, such as phishing and malware [53]. By investing in employee education and training, organizations can establish a security-conscious culture and mitigate the risk of a successful Redline Stealer attack.

4.8.2 Email Security

Email security is an essential countermeasure against Redline Malware. As observed in numerous reported cases, phishing is a crucial initial access technique that Redline employs to deliver malware to victim’s devices. Implementing email security solutions can effectively scan all inbound emails and attachments for potential malware. It is quite common for organizations to receive emails from unknown senders. Implementing authentication protocols such as SPF, DKIM, and DMARC can be essential in addressing this issue as such protocols verifies the sender's identity and ensures that emails originated from legitimate source. Additionally, email filters can be configured to detect messages from unknown senders, as well as emails containing unfamiliar attachments or links. These suspicious emails will get quarantined, allowing for validation of their legitimacy before they are delivered to the recipient's mailbox. Email filters can also block specific emails based on pre-determined criteria. For instance, in response to a reported case of Redline malware utilizing OneNote files for propagation, attachments with the .one extension could be blocked at the email security gateway, provided there is no specific need for such files within the organization. By implementing email security, enterprises can significantly reduce the risk of phishing attempts and, as a result, decrease the likelihood of falling victim to Redline Stealer.

4.8.3 Web filters

As discovered in earlier analysis, malicious links are often used to distribute malware, and web filters can be implemented as a countermeasure to this technique. Web filters can be used to block access to websites that are known to distribute malware or engage in malicious activities. The solution can be implemented by configuring it on the organization's network to filter web traffic and block access to malicious websites.

4.8.4 Endpoint Detection and Response

Endpoint Detection and Response (EDR) is an advanced security solution designed to provide in-depth protection against malware. Unlike traditional antivirus software that relies primarily on signature-based detection, EDR technology employs a combination of signature and behaviour-based detection methods to identify and respond to a wide range of threats [54]. Implementing EDR solutions is a crucial measure to defend against Redline Stealer as it can detect and remove malware from the endpoints. Additionally, as EDR focuses on monitoring and analysing endpoint logs, this approach allows EDR to identify and analyse the behaviour of malware, enabling it to detect most of the common MITRE techniques observed in analysis earlier.

4.8.5 Application Whitelisting

Application whitelisting means that only approved programs can run on the system, and all other programs are blocked. This defensive solution is crucial due to the Trojan-based nature of Redline Stealer. Application whitelisting would prevent the user from installing malware disguised as legitimate software. There are multiple software and tools available for the application whitelisting process. Windows has a built-in application whitelisting feature called Windows AppLocker, which can be used to allow only authorized applications to run on Windows systems.

4.8.6 Vulnerability and Patch Management

Redline Stealer frequently takes advantage of vulnerabilities present in widely used software. As discussed earlier, a Redline campaign exploited CVE-2021-26411, a vulnerability in Internet Explorer, to deliver the malware [47]. Vulnerability and patch management can be introduced in organizations. Vulnerability management involves identifying and prioritizing vulnerabilities in the system and taking steps to remediate

them. Patch management involves keeping the system up to date with the latest security patches and updates.

4.8.7 Password Security

Redline Stealer primarily targets sensitive data, with credentials and passwords being the most valuable assets for cybercriminals. To defend against the potential impacts of Redline malware, organizations should prioritize password security. Redline Stealer predominantly targets sensitive data, with credentials and passwords being cybercriminals' most valuable assets. To protect against the potential consequences of the Redline malware, organizations must prioritize password security. This can be accomplished by enforcing strong password policies for employees, requiring complex and unique passwords with regular updates; implementing policies to restrict saving credentials in browsers; utilizing password managers to securely store and manage passwords within the corporate environment; and adopting multi-factor authentication (MFA) to add an additional layer of security, reducing the effectiveness of stolen credentials. Organizations can effectively protect sensitive data and reduce the risk of credential theft by implementing these measures.

4.8.8 Proper Visibility & Threat Detection

There is famous saying in Information Security by Dr. Eric Cole: "Prevention is Ideal but Detection is a must" [55]. While prevention serves as the initial and crucial step in safeguarding against Redline Stealer, it is equally important to have detection mechanisms in place. This is because threat actors are continuously evolving, and their tactics are becoming more sophisticated. As a result, organizations must be proactive in detecting potential threats and intrusions.

To effectively detect threats, proper visibility into the organization's infrastructure is essential. Security Information and Event Management (SIEM) systems play a pivotal role in gathering and analysing security-related information from a variety of sources, such as logs, network traffic, and endpoints [54]. SIEM solutions can be implemented to collect and analyse security-related data triggering alerts for further investigation.

YARA is a powerful and flexible pattern-matching tool specifically designed for identifying and classifying malware samples. YARA utilizes customizable rulesets to detect malicious code [56]. On the other hand, SIGMA is a generic, open-source signature

format that allows creation and sharing of SIEM detection rules, allowing seamless integration with various SIEM systems, and enabling efficient threat detection [57]. In the context of this study, YARA and SIGMA detection rules were developed based on common MITRE techniques and indicators identified during the analysis. By implementing these rules within a SIEM, organizations can receive alerts when a match is detected thus enhancing their threat detection capabilities. The rules created can be found in Appendix 3 and 4, and they have also been made available in the GitHub repository for easy access and testing purposes [23]. By providing a comprehensive view of the security landscape, SIEM solutions enable organizations to identify, assess, and respond to potential threats in real-time.

As a next step, the rules can be tested and validated for their accuracy and efficacy in real-world scenarios. This would include deploying these detection rules with the SIEM in various network environments to assess their performance in detecting Redline stealer attacks.

5 Conclusion

In conclusion, this thesis has thoroughly explored the analysis of Infostealer malware, specifically focusing on the Redline stealer. Through automated dynamic analysis, the research identified key indicators which were subsequently mapped to the MITRE ATT&CK framework to reveal the most common techniques employed by this specific malware. Trends analysis of the initial delivery phase of the Redline stealer contributed valuable insights into how the malware is distributed to victim’s device. Additionally, an ATTACK flow was developed to provide a visualized understanding of the malware's attack process. The study ultimately proposed defensive measures for the Redline stealer, including the creation of YARA and Sigma rules to help in detection and prevention. The findings from this research serve as a strong foundation for future studies in the field of Infostealer malware defense.

References

[1] Mascellino, Alessandro, "CircleCI Confirms Data Breach Was Caused By Infostealer on Employee Laptop," 2023. [Online]. Available: www.infosecurity-magazine.com/news/cir.

[2] Malwarebytes, "Malwarebytes Labs," [Online]. Available: https://www.malwarebytes.com/blog/threats/info-stealers.

[3] Accenture Security, "Popularity spikes for information stealer malware on the dark web," 2022. [Online]. Available: https://www.accenture.com/us-en/blogs/security/information-stealer-malware-on-dark-web.

[4] Cyware, "All about high in-demand information theft tool Redline Stealer," June 2022. [Online]. Available: https://cyware.com/research-and-analysis/all-about-high-in-demand-information-theft-tool-redline-stealer-0df1. [Accessed 23 February 2023].

[5] FLARE, "RedLine Stealer Malware: The Complete Guide," February 2023. [Online]. Available: https://flare.systems/learn/resources/blog/redline-stealer-malware/.

[6] Bleeping Computer, "Microsoft confirms they were hacked by Lapsus extortion group," March 2022. [Online]. Available: https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/. [Accessed 23 February 2023].

[7] Kaspersky, "Redline Stealer self-propagates on YouTube," 15 September 2022. [Online]. Available: https://www.kaspersky.com/blog/redline-stealer-self-propagates-on-youtube/45528/. [Accessed 23 February 2023].

[8] V. H. a. N. Gupta, "Malware-as-a-Service: A Lucrative Business Model for Cyber Criminals," *2018 7th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions)*, pp. 542-547, 2018.

[9] SOCRadar, "What is Redline Stealer and What Can You Do About It?," [Online]. Available: What is Redline Stealer and What Can You Do About It?. [Accessed 24 February 2023].

[10] Investopedia, "Carding," [Online]. Available: https://www.investopedia.com/terms/c. [Accessed 24 February 2023].

[11] Kaspersky Encyclopedia, "Cryptor," Kaspersky Encyclopedia, [Online]. Available: https://encyclopedia.kaspersky.com/glossary/cryptor/. [Accessed 24 February 2023].

[12] The Record by Recorded Future, "RedLine Stealer identified as primary source of stolen credentials on two dark web markets," 21 October 2021. [Online]. Available: https://therecord.media/redline-stealer-identified-as-primary-source-of-stolen-credentials-on-two-dark-web-markets/. [Accessed 23 February 2023].

[13] The Hacker News, "The hidden internet and the Russian Market," [Online]. Available: https://thehackernews.com/2018/07/r. [Accessed 24 February 2023].

[14] ANY.RUN, "ANY.RUN Malware Trends," [Online]. Available: https://any.run/malware-trends/redline. [Accessed 24 February 2023].

[15] URLhaus, "RedLineStealer," URLhaus, [Online]. Available: https://urlhaus.abuse.ch/browse/tag/RedLineStealer. [Accessed 22 February 2023].

[16] MalwareBazaar, "RedLineStealer," MalwareBazaar, [Online]. Available: https://bazaar.abuse.ch/browse/signature/RedLineStealer/. [Accessed 24 February 2023].

[17] Mcafee, "What is the MITRE ATT&CK Framework? | Get the 101 Guide |," [Online]. Available: https://www.mcafee.com/enterprise/ko-kr/security-. [Accessed 11 March 2023].

[18] A. Roberts, Cyber threat intelligence, Berkeley, CA: Apress., 2021.

[19] THE MITRE Coporation, "attack-navigator," [Online]. Available: https://mitre-attack.github.io/attack-navigator/. [Accessed 2023 March 11].

[20] Mitre Engenuity, "Attack Flow," [Online]. Available: https://center-for-threat-informed-defense.github.io/attack-flow/overview/. [Accessed 26 March 2023].

[21] Hybrid-Analysis, "Hybrid-Analysis: Malware Analysis & Threat Intelligence," [Online]. Available: https://www.hybrid-analysis.com/. [Accessed 20 February 2023].

[22] E. Kovacs, "CrowdStrike Adds Malware Search Engine to ‘Hybrid Analysis'," Secruityweek, 21 August 2018. [Online]. Available: https://www.securityweek.com/crowdstrike-adds-malware-search-engine-hybrid-analysis/. [Accessed 11 March 2023].

[23] "GitHub," [Online]. Available: https://github.com/FothulForhan/Thesis_194489IVSB. [Accessed 23 April 2023].

[24] MITRE ATT&CK, "Native API," [Online]. Available: https://attack.mitre.org/techniques/T1106/. [Accessed 20 March 2023].

[25] MITRE ATT&CK, "Create or Modify System Process," [Online]. Available: https://attack.mitre.org/techniques/T1543/. [Accessed 20 March 2023].

[26] MITRE ATT&CK, [Online]. Available: https://attack.mitre.org/techniques/T1622/. [Accessed 20 March 2023].

[27] MITRE ATT&CK, "Virtualization/Sandbox Evasion," [Online]. Available: https://attack.mitre.org/techniques/T1497/. [Accessed 20 March 2023].

[28] MITRE ATT&CK, "Obfuscated Files or Information: Software Packing," [Online]. Available: https://attack.mitre.org/techniques/T1027/002/. [Accessed 21 March 2023].

[29] MITRE ATT&CK, "File and Directory Discovery," [Online]. Available: https://attack.mitre.org/techniques/T1083/. [Accessed 26 March 2023].

[30] MITRE ATT&CK, "Query Registry," [Online]. Available: https://attack.mitre.org/techniques/T1012/. [Accessed 26 March 2023].

[31] MITRE ATT&CK, "System Information Discovery," [Online]. Available: https://attack.mitre.org/techniques/T1082/. [Accessed 26 March 2023].

[32] MITRE ATT&CK, "System Location Discovery: System Language Discovery," [Online]. Available: https://attack.mitre.org/techniques/T1614/001/. [Accessed 26 March 2023].

[33] MITRE ATT&CK, "Process Discovery," [Online]. Available: https://attack.mitre.org/techniques/T1057/. [Accessed 26 March 2023].

[34] MITRE ATT&CK, "Data Encrypted for Impact," [Online]. Available: https://attack.mitre.org/techniques/T1486/. [Accessed 26 March 2023].

[35] Viettel Security, "Report-Redline-Stealer," [Online]. Available: https://viettelcybersecurity.com/wp-content/uploads/2022/02/Report-Redline-Stealer.pdf. [Accessed 13 March 2023].

[36] zdnet, "this-phishing-campaign-delivers-malware-that-steals-your-passwords-and-chat-logs," [Online]. Available: https://www.zdnet.com/article/this-phishing-campaign-delivers-malware-that-steals-your-passwords-and-chat-logs/. [Accessed 13 March 2023].

[37] The Cyber Express, "Redline-stealer-spread-fake-express-vpn-sites," [Online]. Available: https://thecyberexpress.com/redline-stealer-spread-fake-express-vpn-sites/. [Accessed 13 March 2023].

[38] Dropbox, "Force-Download," [Online]. Available: https://help.dropbox.com/share/force-download. [Accessed 13 March 2023].

[39] Rapid7 Blog, "Rapid7 observes use of Microsoft OneNote to spread Redline Infostealer," Rapid7, [Online]. Available: https://www.rapid7.com/blog/post/2023/01/31/rapid7-observes-use-of-microsoft-onenote-to-spread-redline-infostealer-malware/ . [Accessed 13 March 2023].

[40] BleepingComputer, "2K game support hacked to email RedLine info-stealing malware," [Online]. Available: https://www.bleepingcomputer.com/news/security/2k-game-support-hacked-to-email-redline-info-stealing-malware/ . [Accessed 13 March 2023].

[41] MITRE ATT&CK, "Drive-by Compromise," [Online]. Available: https://attack.mitre.org/techniques/T1189/. [Accessed 26 March 2023].

[42] K. Williams, "Malvertising-makes-a-comeback," SmarterMSP, [Online]. Available: https://smartermsp.com/malvertising-makes-a-comeback/. [Accessed 13 March 2023].

[43] S. Miller, "A surge of malvertising across Google Ads is distributing dangerous malware," SPAMHAUS, [Online]. Available: https://www.spamhaus.com/resource-center/a-surge-of-malvertising-across-google-ads-is-distributing-dangerous-malware/. [Accessed 13 March 2023].

[44] B. Toulas, "Fake MSI Afterburner targets Windows gamers with miners, info-stealers," BleepingComputer, [Online]. Available: https://www.bleepingcomputer.com/news/security/fake-msi-afterburner-targets-windows-gamers-with-miners-info-stealers/. [Accessed 13 March 2023].

[45] V. Vlasova, "Malvertising through search engines," Kaspersky, [Online]. Available: https://securelist.com/malvertising-through-search-engines/108996. [Accessed 13 March 2023].

[46] Trendmicro, "Exploit Kit," [Online]. Available: https://www.trendmicro.com/vinfo/us/security/definition/exploit-kit. [Accessed 13 March 2023].

[47] M. NEAGU, "Redline-stealer-resurfaces-in-fresh-rig-exploit-kit-campaign," Bitdefender, [Online]. Available: https://www.bitdefender.com/blog/labs/redline-stealer-resurfaces-in-fresh-rig-exploit-kit-campaign/. [Accessed 13 March 2023].

[48] cve.mitre.org, "CVE-2021-26411," [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26411. [Accessed 13 March 2023].

[49] P. K. M, "Threat Actors Abuse AI-Generated Youtube Videos to Spread Stealer Malware," CloudSek, [Online]. Available: https://cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-stealer-malware. [Accessed 14 March 2023].

[50] A. Mascellino, "YouTube Users Targeted By RedLine Self-Spreading Stealer," Infosecurity, [Online]. Available: https://www.infosecurity-magazine.com/news/youtube-users-targeted-by-redline/. [Accessed 14 March 2023].

[51] V. BOCEK, "Businesses' Facebook accounts hacked to spread Redline Password Stealer malware," Avast, [Online]. Available: https://blog.avast.com/redline-stealer-malware. [Accessed 14 March 2023].

[52] Ponemon Institute, "2019 State of Phishing Study," 2019. [Online]. Available: https://info.knowbe4.com/hubfs/Ponemon Institute State of Phishing Report 2019.pdf. [Accessed 26 March 2023].

[53] National Institute of Standards and Technology, "(NIST SP 800-50) Building an Information Technology Security Awareness and Training Program," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf. [Accessed 26 March 2023].

[54] A. B. Anton Chuvakin, "Endpoint Detection and Response: What You Need to Know," Gartner, 18 July 2018. [Online]. Available: https://blogs.gartner.com/anton-chuvakin/2018/07/18/endpoint-detection-and-response-what-you-need-to-know/. [Accessed 30 March 2023].

[55] Orange Cyberdefense, "How to find the right balance between prevention, detection, and response," 31 March 2021. [Online]. Available: https://www.orangecyberdefense.com/global/blog/managed-detection-response/how-to-find-the-right-balance-between-prevention-detection-and-response. [Accessed 04 April 2023].

[56] YARA, "YARA: The pattern matching swiss knife for malware researchers," [Online]. Available: https://yara.readthedocs.io/en/stable/index.html.

[57] Sigma, "Sigma: Generic Signature Format for SIEM Systems," [Online]. Available: https://github.com/SigmaHQ/sigma. [Accessed 09 April 2023].

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Fothul Karim Forhan

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Analysis of Infostealer Malware Samples and Proposed Defensive Measures”, supervised by Shaymaa Mamdouh Khalil
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

13.05.2022

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Automated Dynamic Analysis Malware Samples

The Appendix provides a list of the malware samples analysed in this study, along with their corresponding links to the Hybrid-Analysis reports. This information is included to aid in further research and provide supporting evidence for the indicators mentioned in this study.

Sample 1
Submission Name: sefile.exe
Original Sample Extension: .exe/32-bit
Report URL: https://www.hybrid-analysis.com/sample/0e8849fae3014fbbf9e1c4e72d1022b8887665eadc0bc019860e2e90d7c7b146

Sample 2
Submission Name: JalopiesCries.exe
Original Sample Extension: .exe/64bit
Report URL: https://www.hybrid-analysis.com/sample/b25276475053e1d4abdb00ae75ac931bd554cd508d17d54733f39643c4c697cb

Sample 3
Submission Name: softwinx86.exe
Original Sample Extension: .exe/32-bit
Report URL: https://www.hybrid-analysis.com/sample/c2e6b08bce56c265b9e651a28bbe01d81092465beebf853fbf6cb0094deb5bfc

Sample 4
Submission Name: muza.exe
Original Sample Extension: .exe/32-bit
Report URL: https://www.hybrid-analysis.com/sample/65202f4c7dba4ca26af8a2ecdcbccd2dd9fc0ae1c91940dbf61df26e89663ce1

Sample 5
Submission Name: Kiddions Mod Menu.exe
Original Name: Kiddions_Mod_Menu.rar
Original Sample Extension: .rar/32-bit
Report URL: https://www.hybrid-analysis.com/sample/b3abe4a6ab3a1f7f7c8daf4db51a202edb2f8edf1ace6ac00f7afced3387949a

Sample 6
Submission Name: Setup.exe
Original Name: Install.rar
Original Sample Extension: .rar/32-bit
Report URL: https://www.hybrid-analysis.com/sample/0c53a042d0d38393f870fc0bc79f5a88baec0f79ddd32fc23d523c536e9265d0

Sample 7
Submission Name: l.exe
Original Sample Extension: .exe/64-bit
Report URL: https://www.hybrid-analysis.com/sample/d093cc2e257699ebf02497e30b6c5590ef100f44a7d692d2cac83f0a813985b5

Sample 8
Submission Name: Rrobknnz-FREEAPPS.exe
Original Sample Extension: .exe/64-bit
Report URL: https://www.hybrid-analysis.com/sample/653388cbb84b4a94bcc4370bffca1672fe96f2fe5e3506001e65c3697c7c4191

Appendix 3 – Yara Rule

Based on the indicators observed during static analysis of an individual sample, a YARA rule has been created that focuses on the imports and strings associated with described MITRE techniques. The strings section contains regular expressions that match the names of specific functions imported by the Windows executable being analysed. The condition of the YARA rule checks for two conditions: the file is a Windows executable, and at least three of the specified imports are present, including “IsDebuggerPresent”. These conditions are designed to avoid false positives by requiring the presence of multiple imports, including a known anti-debugging function.

```
rule Redline_Malware_Indicators {

    meta:

        Author = "Fothul Karim Forhan"
        Description = "Rule for Malware Detection"
        Reference = "Indicators observed during Static Analysis"
        Date = "15th April 2023"
        Version = "1.0"

    strings:

        // Imports founds in the Sample(case-insensitive)
        $GetCommandLineA = /GetCommandLineA/i
        $GetModuleFileNameA = /GetModuleFileNameA/i
        $GetStartupInfoA = /GetStartupInfoA/i
        $GetCurrentProcess = /GetCurrentProcess/i
        $IsDebuggerPresent = /IsDebuggerPresent/i
        $GetTickCount = /GetTickCount/i
        $Sleep = /Sleep/i
        $GetModuleHandleA = /GetModuleHandleA/i

    condition:

        // Checks if the file is a Windows executable
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and
        // Checks for the presence of at least 3 of the specified imports,
including IsDebuggerPresent
        (3 of them) and $IsDebuggerPresent
}
```

Appendix 4 – Sigma Rules

```
title: Detection of Redline Malware using Native API Technique
description: Detects the use of Native API technique by Redline malware
references:
    - https://attack.mitre.org/techniques/T1106/
author: Fothul Karim Forhan
date: 15/04/2023
status: experimental
tags:
    - attack.t1106
    - malware
    - redlinestealer
logsource:
    category: process_creation
    product: windows
detection:
    selection1:
        CommandLine|contains: "GetCommandLineA"
        TargetImageFileName|contains: "\\KERNEL32.DLL"
    selection2:
        CommandLine|contains: "GetModuleFileNameA"
        TargetImageFileName|contains: "\\KERNEL32.DLL"
    selection3:
        CommandLine|contains: "GetProcAddress()"
        TargetImageFileName|contains: "\\KERNEL32.DLL"
    condition: selection1 or selection2 or selection3
falsepositives:
    - Some legitimate software might generate this alert
level: high
```

```
title: Detection of Redline Malware using Create or Modify Process technique
description: Detects the use of Create or Modify Process technique by Redline
malware
references:
    - https://attack.mitre.org/techniques/T1543/
author: Fothul Karim Forhan
date: 15/04/2023
status: experimental
tags:
    - attack.t1543
    - malware
    - redlinestealer
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains: '*GetStartupInfoW*'
```

```
        TargetImageFileName|contains: "\\KERNEL32.DLL"
    condition: selection
falsepositives:
    - Some legitimate software may use the GetStartupInfoW function.
level: high


title: Detection of Redline Malware using Debugger Evasion technique
description: Detects the presence of debugger evasion API strings in Redline
Malware
references:
    - https://attack.mitre.org/techniques/T1622/
author: Fothul Karim Forhan
date: 15/04/2023
status: experimental
tags:
    - attack.t1622
    - malware
    - redlinestealer
logsource:
    category: process_creation
    product: windows
    event_id: 1
detection:
    selection:
        EventData.Image: '*'
    condition: >-
        EventData.Image
        Contains "IsDebuggerPresent" AND
        (
            EventData.Image
            Contains "SetUnhandledExceptionFilter" OR
            EventData.Image
            Contains "UnhandledExceptionFilter"
        )
falsepositives:
    - None at the moment.
level: high


title: Detection of Redline Malware using Virtualization/Sandbox Evasion
Technique
description: Detects the presence of Virtualization/Sandbox evasion
techniques in Redline Malware
references:
    - https://attack.mitre.org/techniques/T1497/
author: Fothul Karim Forhan
date: 15/04/2023
status: experimental
tags:
    - attack.t1497
```

```
    - malware
    - redlinestealer
logsource:
    product: windows
    service: sysmon
    source: EventID: 1
detection:
    selection:
        EventID: 1
        Image: '*\\KERNEL32.dll'
        CommandLine: '*Sleep*'
        CommandLine: '*GetTickCount*'
    condition: selection
falsepositives:
    - Legitimate software may use the Sleep and GetTickCount functions.
level: high


title: Detection of Redline Malware using File and Directory Discovery
Technique
description: Detects the presence of File and Directory Discovery technique
in Redline Malware
references:
    - https://attack.mitre.org/techniques/T1083/
author: Fothul Karim Forhan
date: 15/04/2023
status: experimental
tags:
    - attack.t1083
    - malware
    - redlinestealer
logsource:
  product: windows
  service: sysmon
detection:
  selection1:
    EventID: 2
    TargetFilename: '*\WOW64LOG.DLL'
  selection2:
    EventID: 2
    TargetFilename: 'C:\FLTLIB.DLL'
  condition: selection1 or selection2
fields:
  - Image
  - TargetFilename
  - EventType
falsepositives:
  - Legitimate applications trying to access the files
level: high
```

```
title: Detection of Redline Malware using Input Capture sub-technique
description: Detects the presence of Input Capture Sub-technique in Redline
Malware
references:
  - https://attack.mitre.org/techniques/T1056/004
author: Fothul Karim Forhan
date: 15/04/2023
status: experimental
logsource:
  product: windows
  service: process_creation
detection:
  selection:
    CommandLine: '*Wow64Transition@NTDLL.DLL*'
  condition: selection
fields:
  - CommandLine
  - Image
  - ParentCommandLine
  - User
falsepositives:
  - Legitimate applications using Wow64Transition
level: high
```

```
title: Detection of Redline Malware using Query Registry Technique
description: Detects the presence of Query Registry technique in Redline
Malware
references:
    - https://attack.mitre.org/techniques/T1012/
author: Fothul Karim Forhan
date: 15/04/2023
status: experimental
tags:
    - attack.t1012
    - malware
    - redlinestealer
logsource:
  product: windows
  service: sysmon
detection:
  selection1:
    EventID: 12
    TargetObject: '*\REGISTRY\MACHINE\SOFTWARE\Microsoft\Ole*'
  selection2:
    EventID: 12
    TargetObject: '*\REGISTRY\USER\S-1-5-21-*-1001_Classes\Local
Settings\Software\Microsoft*'
  condition: selection1 or selection2
fields:
  - Image
```

```
  - TargetObject
  - EventType
falsepositives:
  - Legitimate applications monitoring the same registry keys
level: high
```