

# EVASION TECHNIQUES EMPLOYED IN MALWARE: THE RAMSOMWARE CASE STUDY

Danyal Namakshenas  
*School of Computer Science*  
*University of Guelph*  
Guelph, ON, CA  
dnamaksh@uoguelph.ca

Faith C. Obasi  
*School of Computer Science*  
*University of Guelph*  
Guelph, ON, CA  
fobasi@uoguelph.ca

**Abstract**—Malware attacks especially ransomware is a universal pestilence, ravaging industries and causing severe damage. Researchers and security professionals are taking great strides to provide anti-malware systems with feasible methods to detect malicious activities on the network and computer systems. This paper analyzes the various methods used by malware developers to evade detection by traditional security software with a focus on the Blackbyte and Clop ransomware families. The paper also highlights some mitigation techniques that can be used to protect companies against ransomware attacks.

**Keywords**—malware, ransomware, evasion, security

## I. INTRODUCTION

The rise of ransomware has been one of the most significant cyber threats in recent years, affecting both individuals and organizations around the world. A ransomware attack encrypts the victim's files and demands a ransom payment for access to the decryption key [1]. Traditional security measures are often evaded by attackers, making detection and mitigation challenging. Evasion techniques which involve a variety of tactics to conceal malware from being discovered by security systems are employed. These tactics ensure that the ransomware is not detected by antivirus software and can execute its malicious payload without interference [2].

Ransomware differs from other malware types, in that it requires some kind of payment which in most cases is untraceable within a tight deadline, adding another layer of difficulty for security professionals in determining who the culprits are and providing admissible information. The implications are often more severe than simple malware attacks consisting of data loss, financial loss, compromising the victim's network, reputational damage and many more. Even

if the victim refuses to pay the ransom, the threat actors can still profit from the stolen data providing additional leverage for extortion attacks. These factors create an urgency to find methods to prevent and detect ransomware attacks. To accomplish that, we need to know the tactics threat actors employ to avoid detection.

Researchers have created several techniques to identify and stop ransomware attacks, including signature-based, behavioral-based, and machine learning-based techniques. Although behavioral-based detection approaches examine the behaviour of the malware to identify harmful activities, signature-based detection methods focus on finding recognised signatures of the infected code [3]. Algorithms are used in machine learning-based detection techniques to find patterns in data and identify ransomware assaults. However, these methods are not fool-proof and have several drawbacks.

This paper will explore the evasion techniques employed in ransomware, with a focus on the Blackbyte and Clop ransomware families. We will look at the many strategies employed by malware creators to avoid detection, such as code obfuscation, anti-analysis tactics, and polymorphism [4]. We will also consider the potential effects of these approaches on security as well as the difficulties security experts face when trying to detect and mitigate the threat of ransomware [5]. Lastly, We will conclude by offering advice on how people and businesses can defend themselves against ransomware attacks and reduce the risk of data loss and monetary harm.

## II. RELATED WORKS

### A. Ransomware Evolution

Ransomware has been around for a while. The first Windows ransomware appeared in 1989 as in Figure 1 below and has continued to exist today, albeit it has

undergone major changes since then. The PC Cyborg assault, which occurred in December 1989, was the first ransomware incident. It was the first ransomware of the crypto kind since it encrypted the files on the computer drives using a symmetric key and an initialization vector, but it was still relatively rare at this time [6]. Up until this point, we have observed three different varieties of locker ransomware: SMS, MBR, and Fake FBI ransomware types.

The second significant attack during this era occurred in 2004, the GpCode trojan family which was distributed through spam campaigns. The victims were deceived into downloading malicious word document files disguised as a job application form but instead contained a macro that downloaded and installed some trojans on the victim's computer. Once installed the GpCode encrypted over 80 different file types such as .doc, .pdf, .xls, .jpg etc [7]. In 2005, different Fake Antivirus ransomware types including the Spysheerif, Performance Optimizer, and Registry Care followed. Two other families—Archeus and Cryzip—began to proliferate in 2006. After looking for files with specific extensions, Cryzip put the encrypted files in a compressed folder. All the files were put into a password-protected folder by Archiveus [6].

The first MBR (Master Boot Record) ransomware appeared between 2010-2011, introducing the arrival of bootlock.B and boot.Seftad.a. This kind of ransomware locks the user out of its services after replacing the original MBR with its own code. The ransom warning appears when the computer boots up and it never encrypts any files [6].

The next generation of ransomware arrived using the Fake FBI ransomware in 2011 with the ransomlock family. Families like Reveton and ACCDFISA began to proliferate in the wild later in 2012. The fine payment notice from the local law enforcement agencies is shown by these families. Subsequently, in 2013, a variety of Ransomlock and Reveton versions appeared. 2014 saw the arrival of new locker families like Virlock, Kovter, and a few other new Ransomlock iterations [6].

Crypto ransomware made a reappearance in 2013 with Cryptolocker 1 and 2, Ransomcrypt, Crilock, and Dirty Decrypt. It became a major issue because of how rampant and successful these attacks were becoming. An updated version of Ransomcrypt, Cryptolocker, Ransomweb, CryptoFortress, Trolldesh, TelsaCrypt, Vaultcrypt, CryptoTorLocker, Pclock, Cryptoblocker, Cryptowall 3 and 4 appeared later in 2015. Tor anonymity network is utilised by Cryptowall 3 for

C&C communication. Recent crypto ransomware families universally employ quite advanced encryption methods. In 2016, new cryptographic families including PHPRansm.B, Locky, Ransom32, HydraCrypt, Cryptolocker.N, and Cerber have begun to spread. Another notable mention is Wannacry in 2017 which is the biggest ransomware attack in history [9].

The year 2019 saw the network infected by updated versions of ransomware through hacking or other methods. After examining the environment for valuable data, moving laterally to get administrative privileges, they then encrypted the data and demanded a ransom. Conti, Clop, and LockBit are three of the versions with the greatest documentation [8].

Ransomware attacks have evolved in recent years from double-extortion data disclosure threats to multiple extortion threats using additional pressure points, such as the makings threats of distributed denial of service (DDoS) attacks on the networks. They also go ahead to harass victims (clients and suppliers) through social media platforms [10].

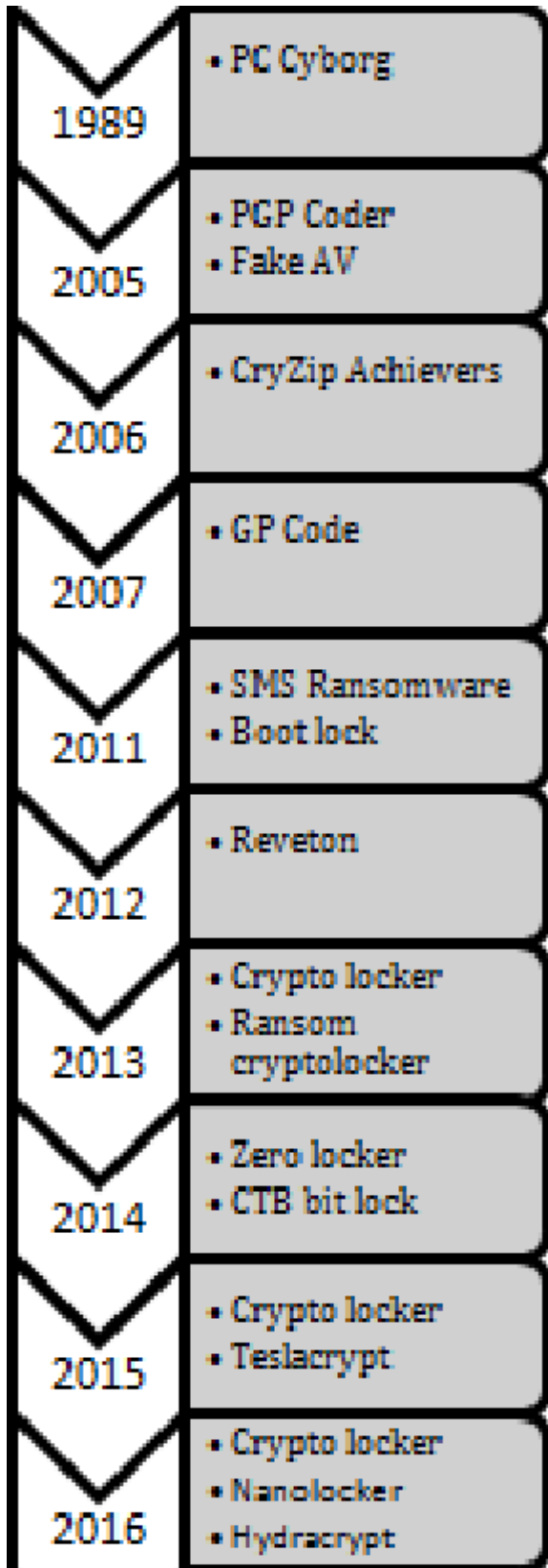


Figure 1. The Evolution and Timeline of Ransomware

### B. Literature Survey

Numerous studies have investigated the evasion techniques used by ransomware to avoid detection by security software and other security measures. There has been a surge in research on ransomware evasion techniques. A research work in [7] by Alsmadi et al., reviewed the current state of research on malware detection techniques. They discussed the main approaches, signature-based and heuristic-based detection, and provide an overview of the advantages and disadvantages of each approach.

In [11] Song et. al proposed a technique for preventing attacks on Andriod devices by monitoring the device's processes. They claim that by continuously monitoring the processes, their technique can detect and prevent the encryption of files by ransomware.

In [12] Aurangzeb et al. compare and assess the efficacy of malware analysis methods for finding ransomware which includes static and dynamic analysis, signature-based analysis, behavior-based analysis, and hybrid analysis, and they provide a thorough analysis of its benefits and drawbacks.

Chen et al. provided a complete survey anti-analysis techniques used in ransomware. They classified the techniques into four categories (packing and obfuscation, detection of virtual environments and sandboxes, anti-debugging and code injection techniques) and evaluated the effectiveness and limitations of each technique with examples of ransomware types that employ each technique [13].

The authors in [14] generated a dataset of benign and ransomware files, extracted features, and assessed how well various machine learning methods performed. Abidin et al. achieved high detection rates with low false positives, demonstrating its effectiveness in detecting ransomware.

In another study [30], the authors proposed a framework for defining malware behavior by using run-time analysis and resource monitoring. It involved using a hybrid approach that combines dynamic and system resource monitoring to capture the behavior of malware in real-time. They claim that the framework can be used to improve the capabilities of malware analysis tools and aid the creation of powerful countermeasures.

In 2022, Alsharif et al. provide insight into some defense mechanisms against ransomware highlighting some deep learning techniques for ransomware detection. They explore the benefits and difficulties of employing deep learning in ransomware detection as

well as identifying some of the shortcomings of current deep learning techniques [15].

### III. LIFECYCLE OF RANSOMWARE

#### A. Initial Access:

This phase refers to the moment when the attacker gains access to the victim's computer system. This is usually accomplished through phishing emails, or a vulnerability exploit that gives the attacker access to the system. The threat actors may use social engineering tactics to deceive the victim into opening a malicious email attachment or click on a link that launches malware installation on the system [27].

#### B. Consolidation and Preparation:

After gaining initial access, the attack then tries to consolidate their presence on the victim's machine and is prepared to launch the attack. This could entail turning off security features, installing and enabling more malicious software, or changing the system's settings to increase the attack's effectiveness. To identify the victim's data and network architecture for the encryption stage, the attacker may perform some reconnaissance during this phase.

#### C. Impact on Target:

At this point, the ransomware attack has had its full impact on the victim. The ransomware has started the process of encrypting the victim's files, making them inaccessible until the ransom is paid, and other demands are met. The victim may get a message requesting money in return for the decryption key that will enable them regain access to their files. The target may not be able to access vital data and systems which may result in loss of productivity, financial loss and reputational damage.

It is essential to note that not all the ransomware attacks adhere to the exact lifecycle depicted in Figure 1 below, attackers may utilize various strategies to execute their attacks. Furthermore, not every victim decides to pay the ransom or meet the demands of the bad actors, and some of them may be able to recover their data using other methods like backups.

Nonetheless, possessing the basic knowledge of the lifecycle of ransomware can help organizations and individuals take measures to protect themselves against ransomware attacks.

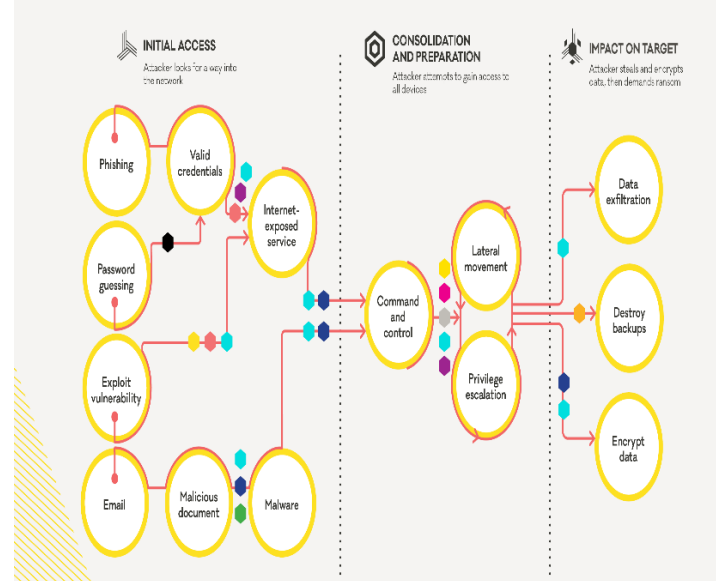


Figure 1- Lifecycle of Ransomware

### IV. RANSOMWARE ANALYSIS

In this study we explore two popular ransomware families: Blackbyte and Clop. These families are well-known for their state-of-the-art evasion techniques. The design of these ransomware types is incredibly sophisticated with functionalities ranging from detecting the operating systems they are being executed on to bypassing and disabling Endpoint Detection and Response systems (EDR) and Event Tracing for Windows (ETW) [16][17]. We will perform analysis using static and behavioral analysis to uncover the evasion techniques used by each group. We will also discuss the evolution of both families and provide possible mitigations.

#### A. Blackbyte Ransomware Family

The second quarter of 2021 witnessed the beginning of the BlackByte ransomware campaign as hackers started breaking into business networks to accomplish their destructive goals. According to an alert from Secret Service and the FBI, the Blackbyte ransomware was responsible for attacking key infrastructure industries like some agricultural industries and government agencies [18]. They have a reputation for exploiting security flaws to break into networks, and they have previously attacked Microsoft Exchange servers using the ProxyShell attack [18]. A sophisticated "Bring Your Own Vulnerable Driver" (BYOVD) approach has been developed in the newer version of BlackByte to bypass most of the drivers that are employed by commercial EDR systems [19]. The MD5 hash value of the sample used for the analysis is

9344afc63753cd5e2ee0ff9aed43dc56. It is an executable file that was gotten from Tria.ge.

### 1) Static analysis:

During the static analysis phase using pestudio, many indicators illustrated the program as a suspicious executable. The red flags were included entry point of the executable, libraries, and the use of UPX0 and UPX1 packers. Some of those suspicious flags are shown in Figure 2 below

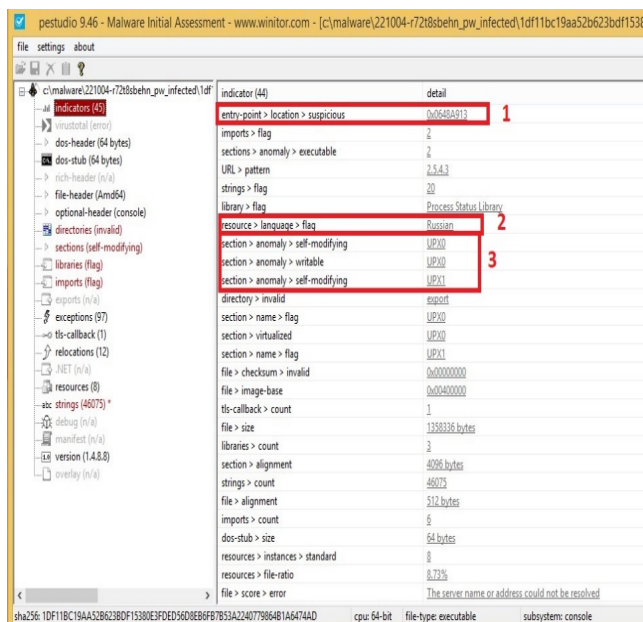


Figure 2 – Screenshot showing Indicators in PeStudio

Only three libraries were detected because the malware was packed. One of the libraries, PSAPI.dll, was used by malware, which is a dynamic link library capable of retrieving windows processes information and monitoring system performance as seen in Figure 3. Also, there is no human-readable information under strings section. We only discovered some characters that seem randomly generated.

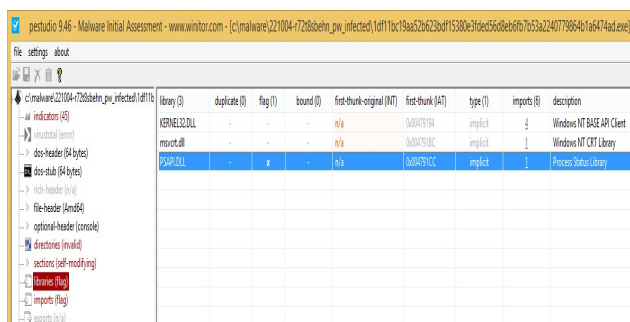


Figure 3 – Screenshot showing Libraries in PeStudio

### 2) Behavioral analysis:

The next stage after static analysis was to study the behavior of the ransomware sample on the host. The file could have a destructive impact on the host so, it is always recommended to execute it in an isolated environment to avoid compromising the host machine. Nonetheless, virtual environment and sandboxes have some processes running on the background, which can be detected by monitoring the machine processes. One thing that makes BlackByte unique is its capability to detect what environment it is being executed in. This makes it impossible to execute the sample in a virtual environment, it can only be executed on the host operating system. Figure 4 shows the result of executing the suspicious file on VMware.

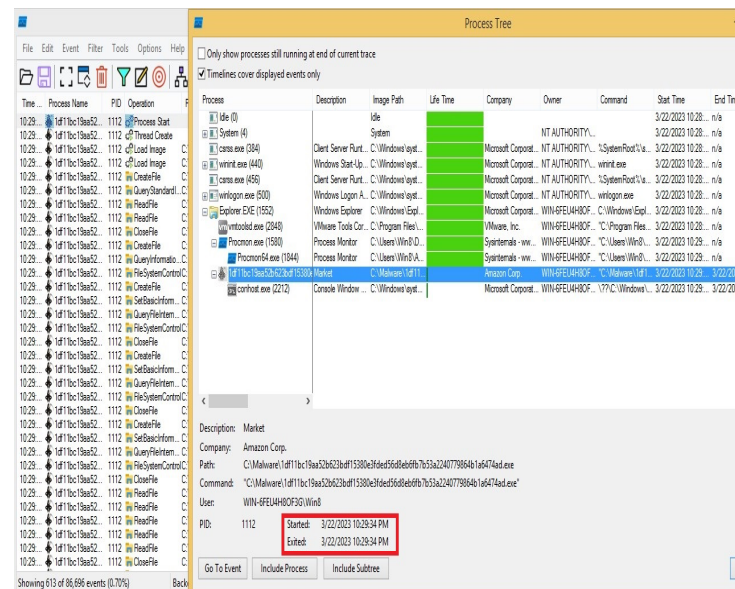


Figure 4 – Screenshot showing Process monitor Result (ProcMon)

Executing the malware sample on a real host showed that it tried to establish a connection to several IP addresses, a C2 domain and it also identified whether the victim was connected to the internet.

It also attempts to encrypt files on the victim's machine. However, instead of encrypting all the files and consuming the computer's resources, it uses an optimized version of encryption to speed up the process, which works according to the file size [20].

### B. Clop Ransomware Family

The APT group responsible for this ransomware is called TA505, which has existed since 2014 [25]. The group is renowned for leading international trends in the criminal propagation of malware. Clop



ransomware was first identified as a member of CryptoMix family. The ransomware group started utilizing the double extortion tactic when the threat actors published a medicine company sensitive information in 2020 [23]. The objective of the APT group is to propagate the ransomware payload by taking advantage of systems' vulnerabilities through various channels such as spear phishing emails [24]. The MD5 hash value of the sample used for the analysis is c41a0e1dddeb85b6326a3dc403a5fd0fa. It is also an executable file that was gotten from Tria.ge.

### 1) Static analysis:

Opening the file in Pestudio resulted in the checksum value of the malware sample which could then be used for analysis on online virus databases. Some of these databases like VirusTotal can identify the ransomware family of the malware. In most cases, the families are not easily detected using online virus databases, further analysis is usually required.

The figure below shows some of the domains and IP addresses the malware tried to connect to when it was executed.

Contacted Domains (1) ⓘ			
Domain	Detections	Created	
img-prod-cms-rt-microsoft-com.akamaized.net	0 / 84	2014-03-18	

Contacted IP addresses (19) ⓘ			
IP	Detections	Autonomous System	Country
13.107.4.50	6 / 84	8068	US
185.125.188.58	0 / 84	41231	GB
185.125.190.26	0 / 84	41231	GB
185.125.190.44	0 / 84	41231	GB
192.168.0.41	0 / 84	-	-
192.168.0.57	0 / 84	-	-
20.62.24.77	0 / 84	8075	US
20.80.129.13	0 / 84	8075	US
20.99.132.105	1 / 84	8075	US
20.99.133.109	0 / 84	8075	US
209.197.3.8	5 / 84	20446	US
23.215.176.163	0 / 83	20940	US
23.216.147.64	3 / 84	20940	US
23.216.147.76	2 / 84	20940	US

Figure 5 – Screenshot showing the Domains and IP addresses the Malware Contacted

Considering the indicators section in pestudio as shown in Figure 6 below, several indicators showed that there were no protection measurements enabled by the ransomware sample. This could mean that the

malware tried to exploit system protection measurement.

The directories section indicated high entropy in .data and .text but not in .rsrc, meaning that the first two parts are likely to be packed. Since Pestudio was unable to detect it, it could mean that the packer used by the executable is not a regular packer. In the library section, no suspicious library was found which confirms the fact that malware was packed.

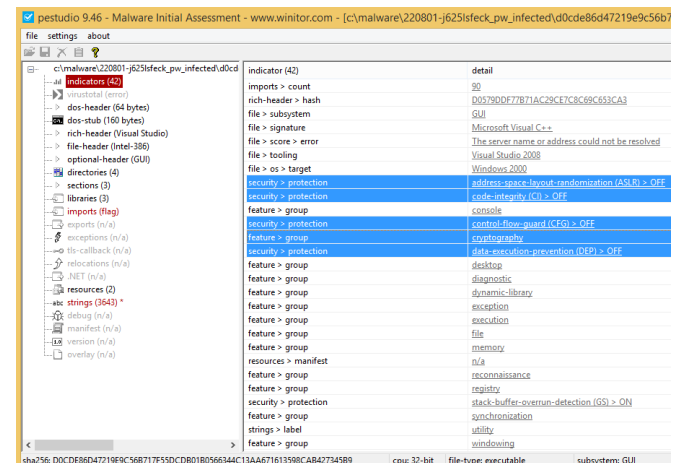


Figure 6 – Screenshot showing Clop ransomware Indicators

Also, several red flags were detected in the imports section as seen in Figure 6 below. One of the most important imports is “VirtualProtect”, which can be used to change the access permission of memory region for executing arbitrary codes. There was no human-readable information in the strings section.

### 2) Behavioral analysis:

Initially, the malware was executed with system administrator privileges on Windows virtual environment using VMware Workstation. It encrypted files that did not have the .exe, .dll, .sys, or file that had no extension at all. Then, the malware left a note for payment instruction and further communication.

We also examined the behavior of the malware while Windows Defender was enabled, and User Access Control was turned up to the highest setting. Surprisingly, the ransomware could still encrypt the files, and bypass the security measures. The ransomware also attempted to encrypt all the shared files on the network and left a note indicating that all files were encrypted.

In addition to encrypting the victim's files, the malware establishes a connection to its C2 server to exfiltrate data, since the threat actors employ double

extortion methods. Meaning that not only do they sell the decryption key, but they also demand money to delete the files from their own servers. A list of IP addresses that it connects to them are shown in figure 8 [13].

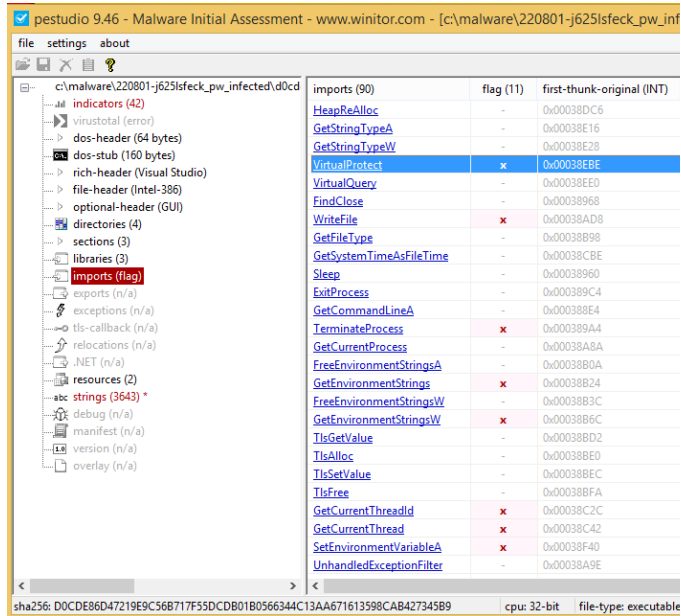


Figure 7 – Image showing Clop Ransomware Imports

Contacted IP addresses (13) ⓘ			
IP	Detections	Autonomous System	Country
104.86.182.8	2 / 87	20940	US
13.107.4.50	7 / 86	8068	US
192.168.0.106	0 / 86	-	-
192.168.0.11	0 / 86	-	-
192.168.0.13	0 / 86	-	-
192.168.0.29	0 / 87	-	-
192.168.0.45	0 / 86	-	-
192.229.211.108	1 / 86	15133	US
20.99.132.105	1 / 87	8075	US
20.99.133.109	0 / 86	8075	US
20.99.184.37	2 / 86	8075	US
23.216.147.76	1 / 86	20940	US
58.42.55.240	0 / 85	139203	CN

Figure 8 – Image Showing Clop C2 Servers

## V. EVASION TECHNIQUES USED BY RANSOMWARE DEVELOPERS

### A. Blackbyte Evasion Techniques

During our behavioral analysis, we found that as soon as the malware was executed, it unpacked itself and tried to scan running processes on the host. Packing is one of the popular ways that malware uses to bypass

initial detection by anti-virus software. Also, instead of following a routine flow of the code, it jumps to a different part of the code to throw off advanced security software. Then, by monitoring running processes on the host, the malware can detect whether it is being executed on a honeypot. When everything is executed as designed by the threat actor, it then checks for existing mutex to confirm that only one instance operates at any given moment [20].

BlackByte also attempts to disable windows firewall, Microsoft Defender, and other anti-viruses. These actions are done in several steps, including disabling applications through windows command line, modifying registry keys, and terminating running processes [21]. Furthermore, it specifically looks for Raccine, which is a ransomware detection tool and removes it from the victim's system [20][21].

Another evasion technique used by the Blackbyte ransomware variant is disabling debugging tools by erasing some of registry values under "Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options" to avoid being monitored [20]. They also bypass EDR and ETW by getting the Master Boot Record's (MBR) file handle after the anti-analysis tests are completed. If that does not work, it then attempts to relaunch itself with greater privileges using the existing vulnerabilities on the victim's machine. After that stage is successful, it bypasses the EDR by detecting the kernel version and then deleting kernel call-backs [19].

At any point during execution, if the malware is unable to perform a given command/action or the action is unsuccessful, it terminates itself to avoid detection.

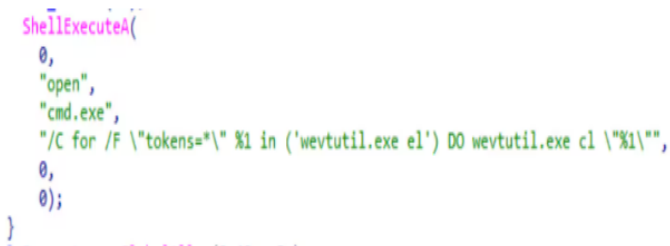
### B. Clop Evasion Techniques

Clop ransomware is one of the most popular ransomware families for so many reasons and one of them is its use of new evasion techniques for each variant it releases. This feature almost certainly guarantees that it would not be detected by anti-viruses and other security products. The early versions of this ransomware were signed by a digital certificate and used to be changed in each variant even though all those certificates have been revoked, malicious actors have still found other ways to make each ransomware variant unique [26].

The first technique used by the Clop ransomware is obfuscation using XOR operation to avoid initial

detection. After extracting itself, it performs several tests to prevent being executed in a virtual environment or being supervised by monitoring tools. Also, in a Ransomware report published by BlackBerry [26], they claimed that the ransomware tried to uninstall Microsoft Security Essentials and disable Windows Defender.

Finally, examining the malware code showed that it uses Shell32.dll library to execute commands to delete log files as shown in figure 8 below [24].



```
ShellExecuteA(
    0,
    "open",
    "cmd.exe",
    "/C for /F %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\"",
    0,
    0);
}
```

Figure 8 – Image showing the Command used in Clop ransomware to clear logs

## VI. SUMMARY OF THE EVASION TECHNIQUES FOUND

### A. Obfuscation:

This is one of the evasion techniques we discovered. This is a technique used by ransomware developers to make malware difficult to read, detect and analyze. It usually involves changing the code's structure and other elements to make it difficult for security professionals to decipher.

### B. Polymorphism:

This is a technique that allows a ransomware to modify its signature each time it infects a new system, making it difficult for the anti-virus software to detect. This was also used by the Blackbyte and Clop families as each sample we analyzed had a different signature.

### C. Anti-analysis:

This is a technique ransomware developers use to prevent researchers from analyzing their code and grasping how it functions. This technique utilizes packers to make the code nearly impossible to read. This technique is also responsible for making it impossible to analyze the malware in a Virtual environment. Anti-analysis techniques were featured heavily in the two families we analyzed.

### D. Natural Language Identification:

During our analysis of Blackbyte, we discovered that the malware flagged the language "Russian". Further research revealed that this is a technique used by ransomware attackers to avoid attacking their own country members. That is, if the ransomware was being executed on a Russian machine, it will terminate itself. This is also a definite giveaway of where the malware originated from.

### E. Registry Modification:

This is a technique used by ransomware writers to control the victim's system. It entails changing registry keys and values to achieve persistence and disable security features and software like EDR and ETW. It ensures that the malware runs every time the system starts, making it tough to detect and remove.

## VII. DETECTION (YARA RULES)

YARA rules are utilized for the purpose of categorizing and detecting malicious software instances by developing characterizations of groups of malwares based on either binary or textual patterns. To examine a malware specimen, analysts will pinpoint distinct patterns and sequences of characters present in the malware which enables them to determine the group of threat and category of malware family to which the specimen belongs.

If a YARA rule is formulated from multiple samples originating from a single malware family, it is feasible to identify multiple specimens that are linked with potentially the same attack or adversary.

We wrote two YARA rules to detect Blackbyte and Clop ransomware types using the samples we examined.

- BlackByte:

```
rule detect_blackbyte {
    meta:
        author = "Faith and Danyal"
        description = "Detects Blackbyte ransomware based on known strings and behavior"

    strings:

        $string1 = "Local\TM.750ce7b0-e5fd-454f-9fad-2f66513dfa1b"
        $string2 = "CicLoadWinStaWinSta0"
        $string3 = "Local\SM0:2524:120:WilError_01"

    condition:
```



```
any of ($string*) and (entrypoint == 0x0648A913)
}
```

- Clop:

```
rule clop_ransomware {
  meta:
    author = "Faith and Danyal "
    description = "Detects Clop ransomware based
on known strings and behavior"

  strings:

    $string1 = " CLOP#666"
    $string2 = " Local\ShimViewer"
    $string3 = "If you do not contact us until" ascii
  wide
    $s4 = " Global\SvcctrlStartEvent_A3752DX"

  condition:
    any of ($string1, $string2, $string3, $string4)
and (uint16(0) == 0x5A4D) // checks for valid DOS
header
}
```

## VIII. MITIGATION STRATEGIES

Having conducted an analysis of the nefarious tactics' malware writers employ to avoid detection, we will now consider some ways to avoid becoming victims of these attacks as well as ways to reduce the impact of the attacks if they occur. The following are some mitigation techniques to protect our systems and infrastructure from ransomware attacks:

### 1) *Audit and inventory:*

It is important to conduct an inventory of all assets and data, identify authorized and unauthorized devices and software, audit logs of events and incidents, and configure and monitor network ports, protocols, and services in order to maintain an accurate and up-to-date understanding of the IT infrastructure.

### 2) *Configure and monitor:*

The careful management of hardware and software configurations is vital to maintaining security. Admin privileges and access should only be granted to employees when it is necessary for their role. Implementing security configurations on network infrastructure devices like firewalls and routers, and maintaining a software allow

list to prevent malicious applications from being executed, are also key steps.

### 3) *Patch and update:*

Regular assessments of vulnerabilities are important, and operating systems and applications should be patched or virtually patched as needed. Keeping software and applications up to date with the latest versions is also necessary for maintaining security.

### 4) *Protect and recover:*

Effective data protection requires backups and recovery measures, and multifactor authentication should be implemented for added security. Analyzing and blocking malicious emails with sandbox analysis is also an important part of protecting against cyber threats.

### 5) *Secure and defend:*

To effectively secure and defend against cyber attacks, it is important to use the latest security solutions to protect all layers of the system. Early detection of attacks is crucial, and advanced detection technologies like AI and machine learning can be highly effective.

### 6) *Train and test:*

Regular assessments of security skills and training for employees are necessary to ensure that security measures are properly implemented and maintained. Conducting red team exercises and penetration testing is also an effective way to identify potential vulnerabilities and improve security measures [22][23].

## IX. LIMITATIONS

Although this paper provides an adequate analysis of the ransomware families and their corresponding evasion techniques, there are a few limitations and challenges we encountered while performing the analysis that may have prevented us from providing a more wholistic view of the subject. Firstly, due to the anti-analysis techniques employed by the malware, we had problems executing the malware on a real host system to obtain more information into how the malware behaves. We also encountered some

difficulty finding enough samples to perform more robust research on all the malware variants in the Blackbyte and Clop families. Despite these limitations, this paper provides valuable insight into the evasion techniques employed by malware writers and emphasizes the need for a proactive approach to mitigating the burgeoning threat of ransomware attacks.

## X. CONCLUSION

Ransomware attacks have been plaguing individuals, companies, and countries as well. Some research suggests that the attacks are becoming more rampant and sophisticated, the effects are also getting worse. The use of evasion techniques to avoid detection makes it nearly impossible for security professionals to detect and mitigate these ransomware attacks.

In this paper, we analyzed ransomware families to discover how they have been successful at evading detection. We focused on the two popular families: Blackbyte and Clop families. The result of the analysis revealed a lot of interesting functionalities embedded in the malware by the developers ranging from polymorphism techniques such as obfuscation to anti-analysis capabilities. We also recommended ways companies could prevent these attacks. Overall, the battle against ransomware attacks requires a collective effort from all the stakeholders. Remaining alert and vigilant to take proactive actions towards better security is of utmost importance.

## DISCLAIMER

This report is intended solely for the purpose of providing an analysis of a ransomware attack and the response. Any use of this report for illegal activities or malicious purposes is strictly prohibited and not condoned by the author. The author assumes no responsibility or liability for any misuse of the information presented in this report. It is the responsibility of the reader to ensure that they comply with all applicable laws and regulations regarding the use of this information.

## REFERENCES

1. D. D. Bunker and J. McRee, "Ransomware: A Growing International Threat," *Journal of Strategic Security*, vol. 9, no. 4, pp. 31-40, 2016.
2. T. Kharif, "Ransomware: Why Hackers Love It," *Bloomberg Businessweek*, pp. 30-33, May 2016, doi: 10.1109/MSPEC.2016.7488582.
3. S. J. Stolfo and A. W. Appel, "Anomaly Detection in the Host Environment," *Proceedings of the DARPA Information Survivability Conference and Exposition*, vol. 1, pp. 43-60, 2003.
4. T. Ghafir, M. M. H. Ali, and M. A. Rahman, "A Review on Detection and Prevention of Ransomware Attacks," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 3, pp. 303-316, 2020.
5. E. Ng and C. S. Tan, "Ransomware: A Comprehensive Review," *IEEE Access*, vol. 7, pp. 82749-82770, 2019.
6. P. Zavorsky and D. Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization," vol. 94, pp. 465-472, 2016.
7. T. Alsmadi and N. Alqudah, "A Survey on malware detection techniques," *2021 International Conference on Information Technology (ICIT)*, Amman, Jordan, 2021, pp. 371-376, doi: 10.1109/ICIT52682.2021.9491765.
8. Trend Micro. (2023, February 21). A Deep Dive into the Evolution of Ransomware Part 1. Retrieved from [https://www.trendmicro.com/en\\_us/research/23/b/ransomware-evolution-part-1.html](https://www.trendmicro.com/en_us/research/23/b/ransomware-evolution-part-1.html)
9. Risk Frontiers. (2021, July 12). A brief history of ransomware. Retrieved from <https://riskfrontiers.com/insights/a-brief-history-of-ransomware/>
10. Swiss Cyber Institute. (2021, September 27). 5 Biggest Ransomware Attacks in History. Retrieved from <https://swisscyberinstitute.com/blog/5-biggest-ransomware-attacks-in-history/#:~:text=This%20ransomware%20infected%207000%20computers>
11. Song, S., Kim, B., & Lee, S. (2016). The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform. 2016.
12. S. Aurangzeb, R. N. B. Rais, M. Aleem, M. A. Islam and M. A. Iqbal, "On the classification of Microsoft-Windows ransomware using hardware profile," in *PeerJ Computer Science*, vol. 7, pp. e361, 2021, doi: 10.7717/peerj-cs.361.
13. C. Chen, A. Zhang, Y. Xiang and Y. Li, "Anti-Analysis Techniques in Ransomware: A Comprehensive Survey," in *IEEE Access*, vol. 7, pp. 65207-65224, 2019, doi: 10.1109/ACCESS.2019.2917343.

14. Abidin, M. S. Z., Aman, F. N., Omar, N., & Haron, N. (2020). A novel approach to detecting ransomware using machine learning. *Journal of Telecommunication, Electronic and Computer Engineering*, 12(2-11), 83-87. doi: 10.11591/ijece.v11i2.pp83-87
15. M. H. Alsharif, M. M. Hassan, F. Xhafa and F. Al-Turjman, "A survey on ransomware attack and defense: Trends, challenges, and future directions," in *Computers & Security*, vol. 111, 2022, doi: 10.1016/j.cose.2022.102636.
16. Sophos News. (2022, October 4). BlackByte ransomware returns. [Online]. Available: <https://news.sophos.com/en-us/2022/10/04/blackbyte-ransomware-returns/>
17. Splunk. (n.d.). Detecting Clop Ransomware. [Online]. Available: [https://www.splunk.com/en\\_us/blog/security/detecting-clop-ransomware.html](https://www.splunk.com/en_us/blog/security/detecting-clop-ransomware.html)
18. Bleeping Computer. (2022, October 5). BlackByte Ransomware Gang is Back with New Extortion Tactics. [Online]. Available: <https://www.bleepingcomputer.com/news/security/blackbyte-ransomware-gang-is-back-with-new-extortion-tactics/>
19. Zscaler. (n.d.). Analysis: BlackByte Ransomware's Go-Based Variants. [Online]. Available: <https://www.zscaler.com/blogs/security-research/analysis-blackbyte-ransoms-g-based-variants>
20. Trustwave SpiderLabs Blog. (n.d.). BlackByte Ransomware PT 1: In-Depth Analysis. [Online]. Available: <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/blackbyte-ransomware-pt-1-in-depth-analysis/>
21. Trend Micro. (n.d.). Ransomware Spotlight: BlackByte. [Online]. Available: <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbyte>
22. Trend Micro. (n.d.). Ransomware: Double Extortion and Beyond REvil, Clop, and Conti. [Online]. Available: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti>
23. Splunk. (n.d.). Detecting Clop Ransomware. [Online]. Available: [https://www.splunk.com/en\\_us/blog/security/detecting-clop-ransomware.html](https://www.splunk.com/en_us/blog/security/detecting-clop-ransomware.html)
24. MITRE. (n.d.). Group: G0092. [Online]. Available: <https://attack.mitre.org/groups/G0092/> BlackBerry. (2021, July).
25. Threat Thursday: Cryptomix/Clop Ransomware. [Online]. Available: <https://blogs.blackberry.com/en/2021/07/threat-thursday-cryptomix-clop-ransomware>
26. VirusTotal. (n.d.). File: d0cde86d47219e9c56b717f55dcdb01b0566344c13aa671613598cab427345b9. [Online]. Available: <https://www.virustotal.com/gui/file/d0cde86d47219e9c56b717f55dcdb01b0566344c13aa671613598cab427345b9/relations>
27. Trend Micro, "Lifecycle of Ransomware," [Online]. Available: [https://www.trendmicro.com/en\\_us/research/16/i/the-lifecycle-of-ransomware.html](https://www.trendmicro.com/en_us/research/16/i/the-lifecycle-of-ransomware.html). [Accessed: Apr. 11, 2023].
28. Symantec, "The Evolution of Ransomware," [Online]. Available: <https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/the-evolution-of-ransomware-en.pdf>. [Accessed: Apr. 11, 2023].
29. FBI, "Ransomware: A Growing Menace," [Online]. Available: <https://www.fbi.gov/news/stories/ransomware-on-the-rise>. [Accessed: Apr. 11, 2023].
30. M. F. Zolkipli and A. Jantan, "A Framework for Defining Malware Behavior Using Run Time Analysis and Resource Monitoring," in 2011 International Conference on Software Engineering and Computer Systems (ICSECS), Springer, 2011, pp. 338-347.