

## **Abstract**

This report covers the evolving landscape of digital and cybercrime, exploring its historical roots and the progression of malware. The report includes case studies on ALPHV BlackCat, and LockBit, portraying their impact. The investigation extends to LockBit through detailed demonstrations, analysis, and strategies for detection and prevention. The findings are synthesized in the concluding chapter, offering insights into the evolving nature of digital/cybercrime.

**Keywords:** Malware, Ransomware, Ransomware as a Service (RaaS), Cyber Crime.

## Table of Contents

Chapter 1 : Introduction .....	1
1.1. Aim.....	1
1.2. Objectives.....	1
Chapter 2 : Background .....	2
2.1. Malware: The first Proof of Concept .....	2
Chapter 3 : Literature Review.....	3
3.1. Case Study: ALPHV BlackCat .....	3
3.2. Case Study: LockBit.....	4
Chapter 4 : Analysis, Detection and Prevention .....	5
4.1. Analysis.....	5
4.1.1. Lab Setup .....	5
4.1.2. LockBit Demonstration.....	6
4.1.3. LockBit Analysis .....	8
4.2. Detection .....	13
4.3. Prevention.....	14
Chapter 5 : Conclusion.....	15
Chapter 6 : References .....	16
Chapter 7 : Appendix .....	19
7.1. Malware Types.....	19
7.2. Evolution of Ransomware .....	20
7.2.1. World’s First Ransomware .....	20
7.2.2. CryptoLocker - The Arrival of Cryptocurrency as a Payment option .....	20
7.2.3. GandCrab and The Emergence of Ransomware as a Service.....	21
7.3. ALPHV BlackCat RaaS .....	23
7.4. LockBit RaaS .....	24
7.5. Lab Setup for LockBit.....	25
7.5.1. Isolate Flare-VM.....	25
7.5.2. Configure INetSim Fake Net .....	26

7.5.3. Build LockBit.....	30
7.5.4. Snapshot before Ransomware Execution.....	33
7.6. YARA Rule Set for Detection.....	34

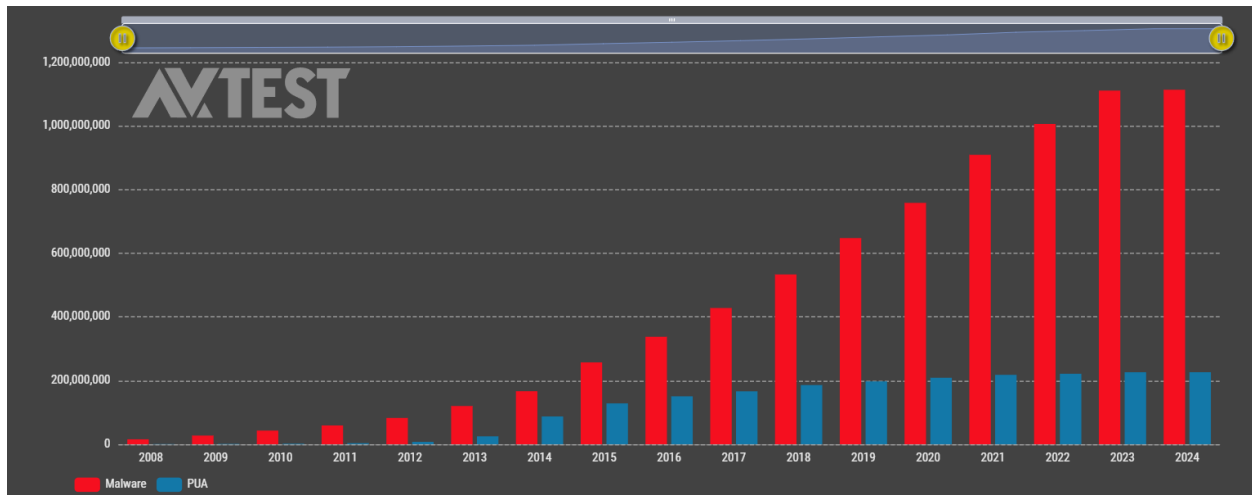
## Table of Figures

Figure 1 Total Amount of Malware and PUA (AV-ATLAS, 2024).....	1
Figure 2 Example of BlackCat Ransomware Note (Martinez, 2022).....	3
Figure 3 Boeing’s Data Publication in LockBit Site (Ilascu, 2023). ....	4
Figure 4 Lab Setup for Malware Demonstration and Analysis .....	5
Figure 5 Dummy files for the malware test .....	6
Figure 6 LockBit Black wallpaper automatically set after execution.....	7
Figure 7 Files encrypted after LockBit execution.....	8
Figure 8 LockBit Black Ransom Note.....	8
Figure 9 LockBit wallpaper location path in the windows registry .....	9
Figure 10 LockBit wallpaper and it's location .....	9
Figure 11 ProcMon filter for querying file encryption .....	10
Figure 12 Dummy files modification events in ProcMon .....	10
Figure 13 Contents of dummy files after malware execution.....	11
Figure 14 Monitoring Network and Disk I/O Statistics.....	11
Figure 15 Log Report of INetSim's Fake Network.....	12
Figure 16 Yara detection using custom rule set for the built LockBit executable.....	13
Figure 17 The AIDS Ransomware Note (Patrick Seguin, 2023).....	20
Figure 18 CryptoLocker bitcoin ransom demand (Belcic, 2020). ....	21
Figure 19 GandCrab Service Launch News (Luca Nagy, 2019). ....	22
Figure 20 BlackCat's Website Seized by FBI.....	23
Figure 21 Setting Host-Only Network for Flare-VM .....	25
Figure 22 Enable Guest Isolation.....	25
Figure 23 Setting Host-Only Network for Remnux.....	26
Figure 24 Binding service address to Remnux address .....	26
Figure 25 Enabling services for fake net .....	27
Figure 26 IP address of Flare-VM .....	27
Figure 27 Network configuration for Flare-VM.....	28
Figure 28 Verifying network configuration in Flare-VM.....	28

Figure 29 INetSim default HTML page.....	29
Figure 30 Verifying that the fake net works properly.....	29
Figure 31 LockBit Builder Configuration.....	30
Figure 32 LockBit Builder file.....	31
Figure 33 LockBit 3.0 compiled executable files .....	31
Figure 34 Content of Password_dll.txt .....	32
Figure 35 Content of Password_exe.txt .....	32
Figure 36 Decryption ID for the ransomware.....	32
Figure 37 Machine snapshot before executing LockBit .....	33

## Chapter 1 : Introduction

Malware is a broad term for malicious software like virus, trojan, spyware, ransomware and other intrusive codes written by threat actors that are widespread today (Mira, 2021). These harmful pieces of software often sneak into a system without the user's knowledge or consent, wreaking havoc and causing damage in the process.



*Figure 1 Total Amount of Malware and PUA (AV-ATLAS, 2024).*

Over time cybercrimes have evolved rapidly and malware can be seen as the preferred medium for the crimes. The statistics from year 2008 to 2024 shown in the figure above indicates that the number of malwares and potentially unwanted applications (PUA) has been rising tremendously.

### 1.1. Aim

The aim of this report is to portray the evolution of malware, analysing malware from recent cases and provide appropriate detection and prevention techniques.

### 1.2. Objectives

The main objectives to achieve the aim mentioned above have been listed below.

- Research about malware, its history and evolution.
- Provide case studies for understanding malware.
- Setup lab and perform analysis on a malware.
- Determine the malware detection and prevention methods.

## Chapter 2 : Background

### 2.1. Malware: The first Proof of Concept

Before the modern internet, ARPANET (Advanced Research Projects Agency Network) was established in 1967 to connect remote computers. By 1969, the first computers were linked, and the Network Control Program (NCP), a precursor to the modern TCP/IP stack, was developed the following year, marking the first network transport layer enabling data flow (Saengphaibul, 2022).

In 1971, the Intel 4004, the first commercially produced general-purpose CPU, was introduced, revolutionizing computing with its compact size, \$60 price, and impressive performance. Coincidentally, 1971 saw the world's first virus Proof of Concept, "The Creeper," behaving more like a worm. Created by engineer Bob Thomas at BBN (later acquired by Raytheon), it spread through ARPANET, displaying the message: "I'm the creeper, catch me if you can!" The experiment successfully tested whether this message could propagate across ARPANET-connected computers (Saengphaibul, 2022).

[ *Note: To learn about malware types, please refer to [Malware Types](#) and for evolution of ransomware, refer to [Evolution of Ransomware](#). ]*

## Chapter 3 : Literature Review

### 3.1. Case Study: ALPHV BlackCat

On 26<sup>th</sup> March of 2023, the data breach notification came after Western Digital suffered a cyberattack, when the company discovered its network was hacked and company data was stolen. In response, Western Digital temporarily halted its cloud services, including My Cloud, My Cloud Home, and others, for two weeks. An unidentified hacking group claimed to have stolen ten terabytes of data, sharing samples with TechCrunch. The stolen information included files signed with Western Digital's code-signing keys, corporate phone numbers, and screenshots of internal data (Abrams, 2023).

Despite the intruder denying ties to the ALPHV ransomware operation, a message on the gang's data leak site warned of data leakage unless a ransom negotiation occurred.

[ *Note: To learn more about BlackCat, please refer to [ALPHV BlackCat RaaS](#). ]*

```
Hello, [REDACTED]

>> What happened

Important files on your network was ENCRYPTED and now they have grp3smk extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- MICROS DATABASE, Accounting, Drawings
- Check Copies, Engineering, HR, Banking Information
- Payroll Scan, Sales and Marketing, Financia
- And more...

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next

1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: http://d75itpgjjfe2ys2qivqplbvmw3yyx7o5e4ppt2esi[REDACTED].onion/?access-key=${ACCESS_KEY}
```

Figure 2 Example of BlackCat Ransomware Note (Martinez, 2022).



### 3.2. Case Study: LockBit

In 2023, LockBit ransomware targeted Boeing, a major aerospace company, and published over 43GB of stolen data after the company refused to pay the ransom. The hackers had warned Boeing about the data becoming public and leaked a sample of 4GB when their threats were ignored. Despite warnings and negotiations, Boeing's sensitive data, including backups with an October 22 timestamp, was released on November 10 (Ilascu, 2023).

The U.S. government reported the gang extorted about \$91 million since 2020 in nearly 1,700 attacks. The LockBit gang, active for over four years, has a history of targeting various sectors globally, including automotive, government, and healthcare.

[ *Note: To learn more about LockBit, please refer to [LockBit RaaS](#). ]*

The screenshot displays a ransomware site with a prominent red banner at the top that reads "UNTIL FILES 5D19H02M22S PUBLICATION". Below this, a red text box states "Deadline: 02 Nov, 2023 13:25:39 UTC". The main content area features the Boeing logo and the text "boeing.com" followed by a description of the company. A warning message states: "A tremendous amount of sensitive data was exfiltrated and ready to be published if Boeing do not contact within the deadline! For now we will not send lists or samples to protect the company BUT we will not keep it like that until the deadline." Below this, a red text box reads "ALL AVAILABLE DATA WILL BE PUBLISHED!". At the bottom, a red text box indicates "Until the files will be available left 5D 19h 02m 22s".

*Figure 3 Boeing's Data Publication in LockBit Site (Ilascu, 2023).*

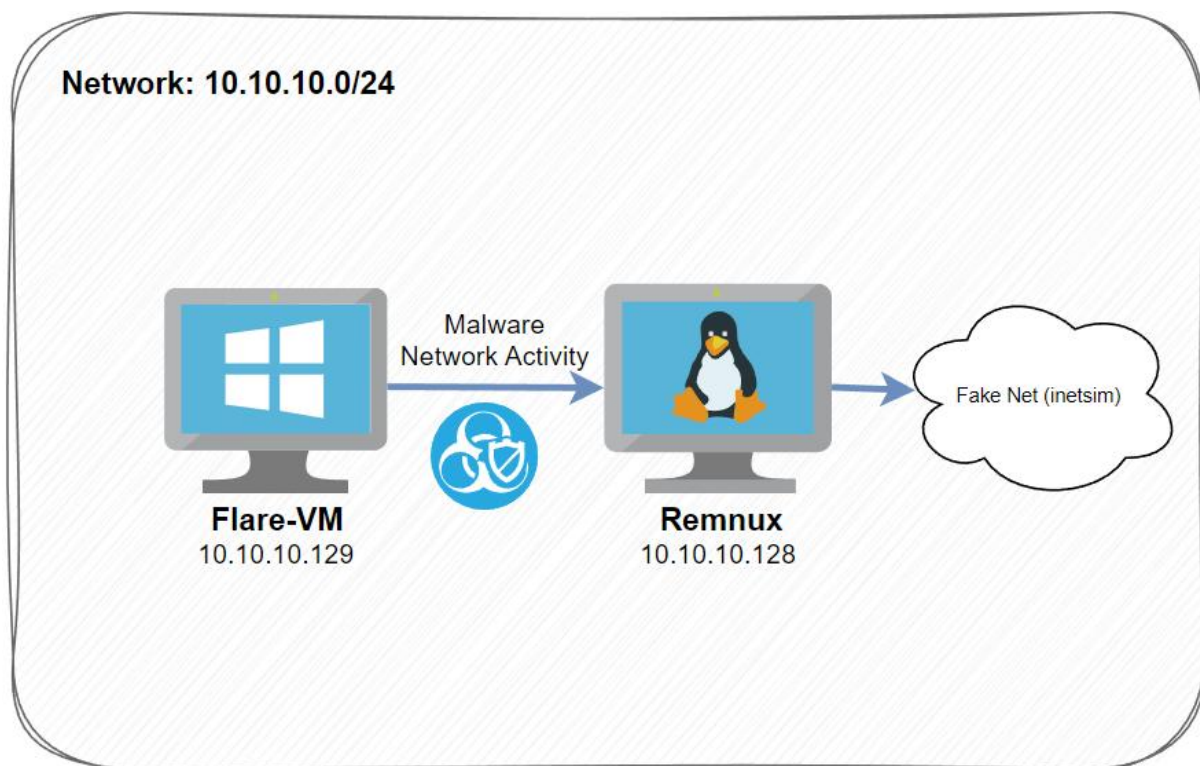
## Chapter 4 : Analysis, Detection and Prevention

### 4.1. Analysis

#### 4.1.1. Lab Setup

Running the malware directly on the host poses significant risks. To conduct the analysis, a virtual lab was established using Flare and Remnux OS, as illustrated in [Figure 4](#). Given that many contemporary malware instances verify network connectivity and terminate themselves if absent, posing an anti-analysis measure, a simulated network was created using INetSim in Remnux to check possible network requests to C2 servers.

The complete lab setup can be found at [Lab Setup for LockBit](#).



*Figure 4 Lab Setup for Malware Demonstration and Analysis*

### 4.1.2. LockBit Demonstration

A leaked builder for LockBit was downloaded from Vx Underground and used to simulate the actual ransomware's attack. The Builder can be found at <https://vx-underground.org/Archive/Builders>.

[ *Disclaimer: The builders present on the website are actual builders for legit ransoms being exploited worldwide. Any malicious activity done through these builders are strongly discouraged.* ]

Kazy Bot Lite Builder.7z	Size: 3.46 MB	Last modified: 2023/11/30	Download
KillerRat Builder.j.7z	Size: 2.44 MB	Last modified: 2023/11/30	Download
Lockbit 3 Builder.7z	Size: 0.14 MB	Last modified: 2023/11/30	Download
LokiRAT Builder.2021.7z	Size: 3.49 MB	Last modified: 2023/11/30	Download
LokiRATBuilder (Unknown Variant).7z	Size: 2.53 MB	Last modified: 2023/11/30	Download

Table 1 LockBit 3.0 Builder

[ *Note: Please refer to [Build LockBit](#) to find the complete LockBit 3.0 build.* ]

Before executing LockBit, some dummy files were created and placed at Documents to check their contents after the malware's execution.

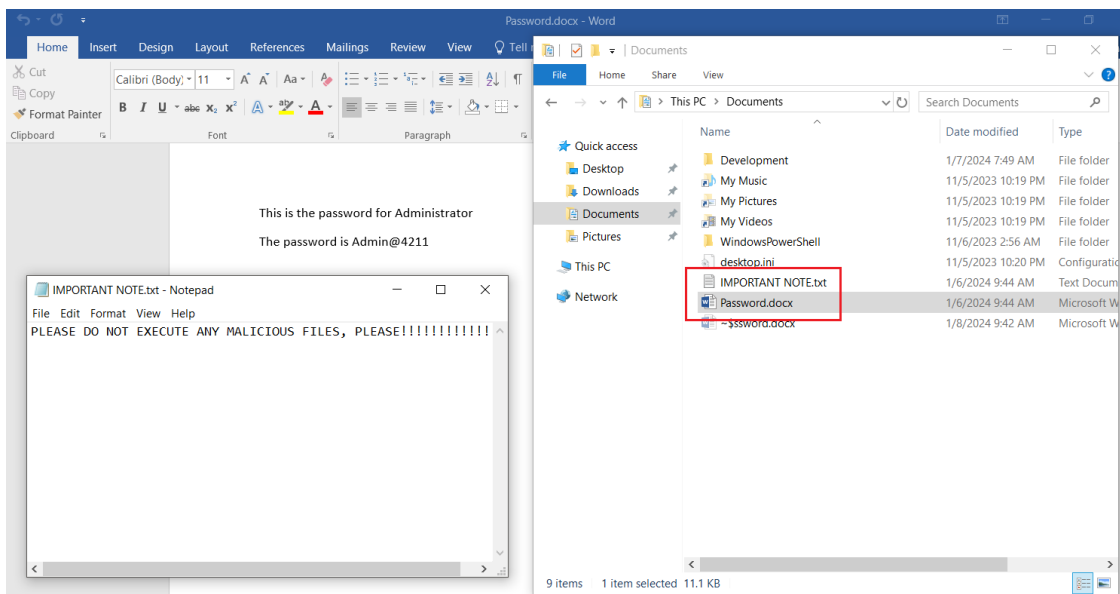
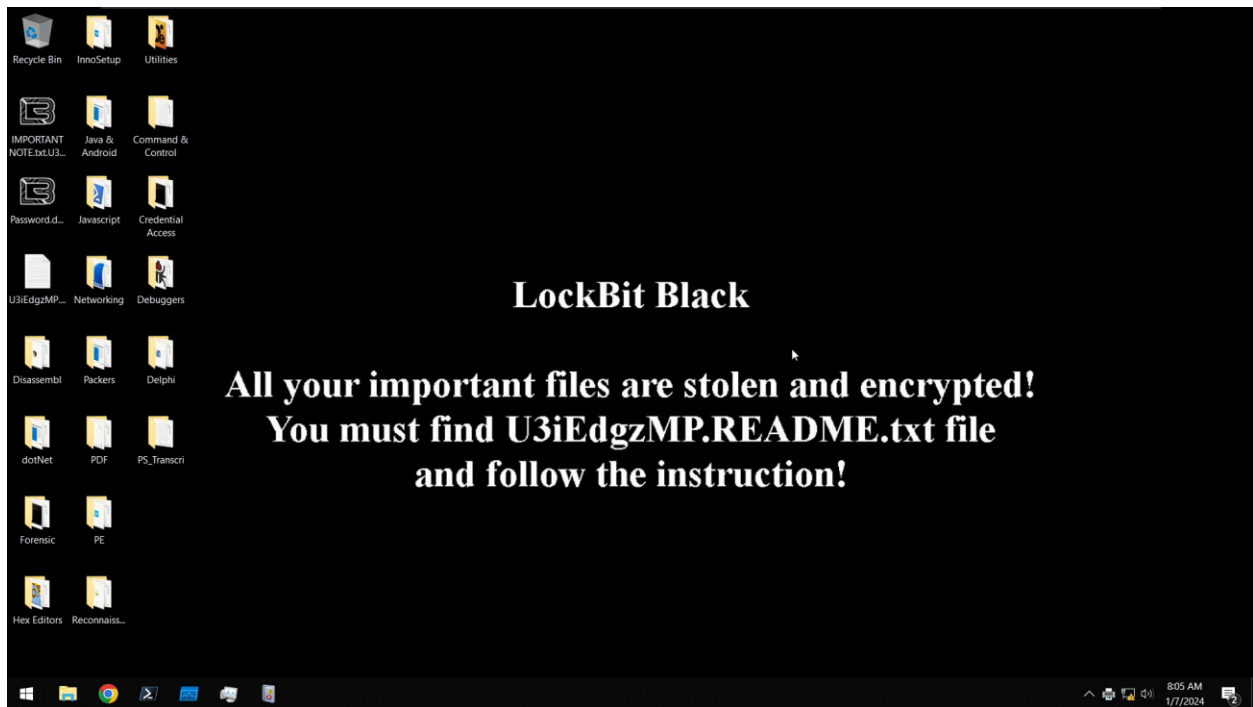


Figure 5 Dummy files for the malware test

After the dummy files, fake net in the Remnux, the network and the VM configurations were setup. The LockBit 3.0 compiled executable file i.e. LB3.exe was executed and the file started getting encrypted and various operations was carried out by the malware. Also, screen of the machine and icons of the encrypted files were changed which can be seen in the figure below. Normally ransomwares only encrypt files but not application, this can also be verified by looking the figure below.



*Figure 6 LockBit Black wallpaper automatically set after execution*

### 4.1.3. LockBit Analysis

As shown in the figure below, the dummy files were renamed with “.U3iEdgzMP” extension and a README file was dropped by the malware.

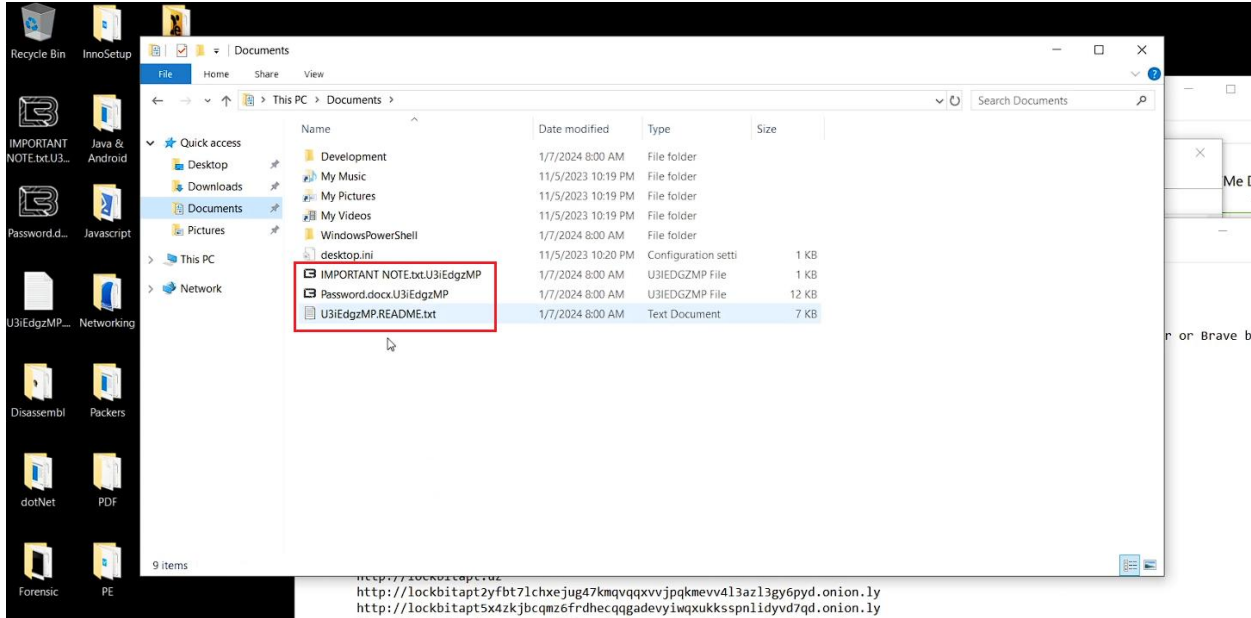


Figure 7 Files encrypted after LockBit execution

U3iEdgzMP.README.txt was the ransom note file generated by LockBit and was saved in different locations and the content of it is shown in the figure below.

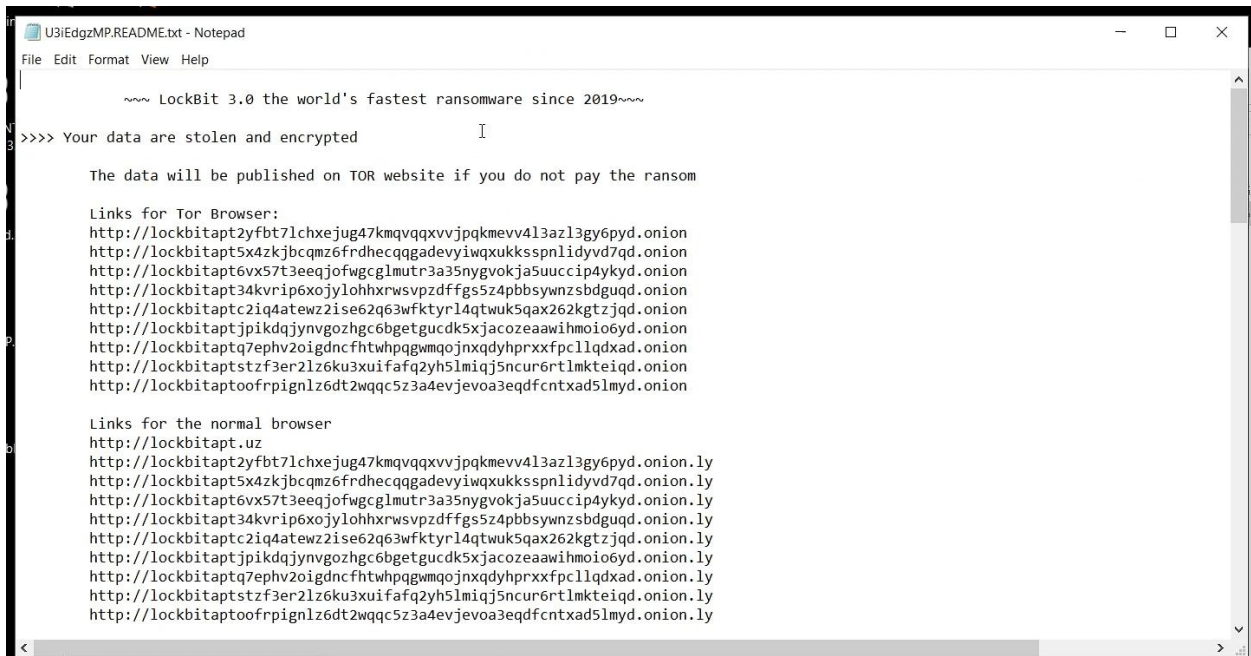


Figure 8 LockBit Black Ransom Note

Checking the windows registry, it was found that Wallpaper was set to LockBit Black Wallpaper after execution. The wallpaper of the machine after execution is shown in [Figure 6](#).

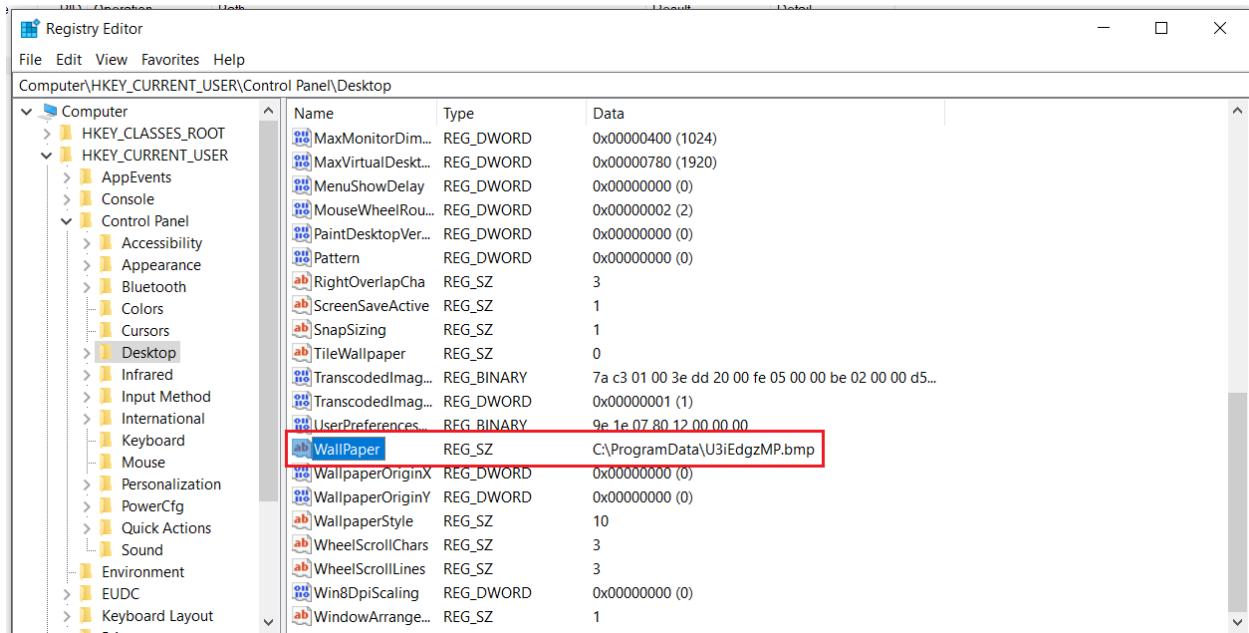


Figure 9 LockBit wallpaper location path in the windows registry

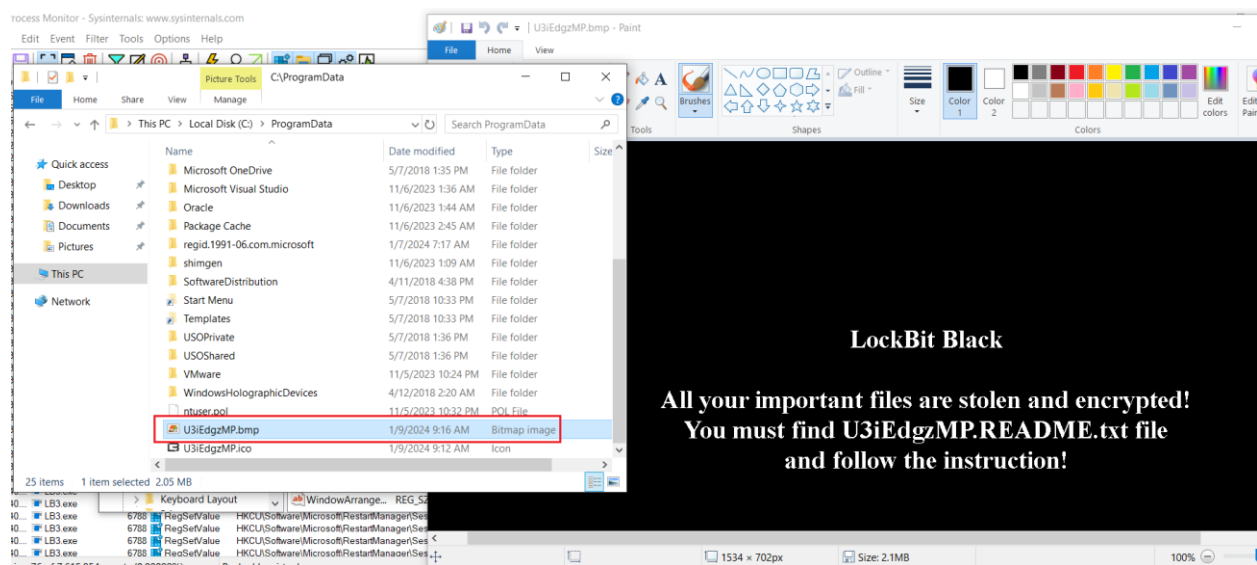


Figure 10 LockBit wallpaper and its location

Using ProcMon filters, it was verified that the files were indeed modified by the LockBit ransomware.

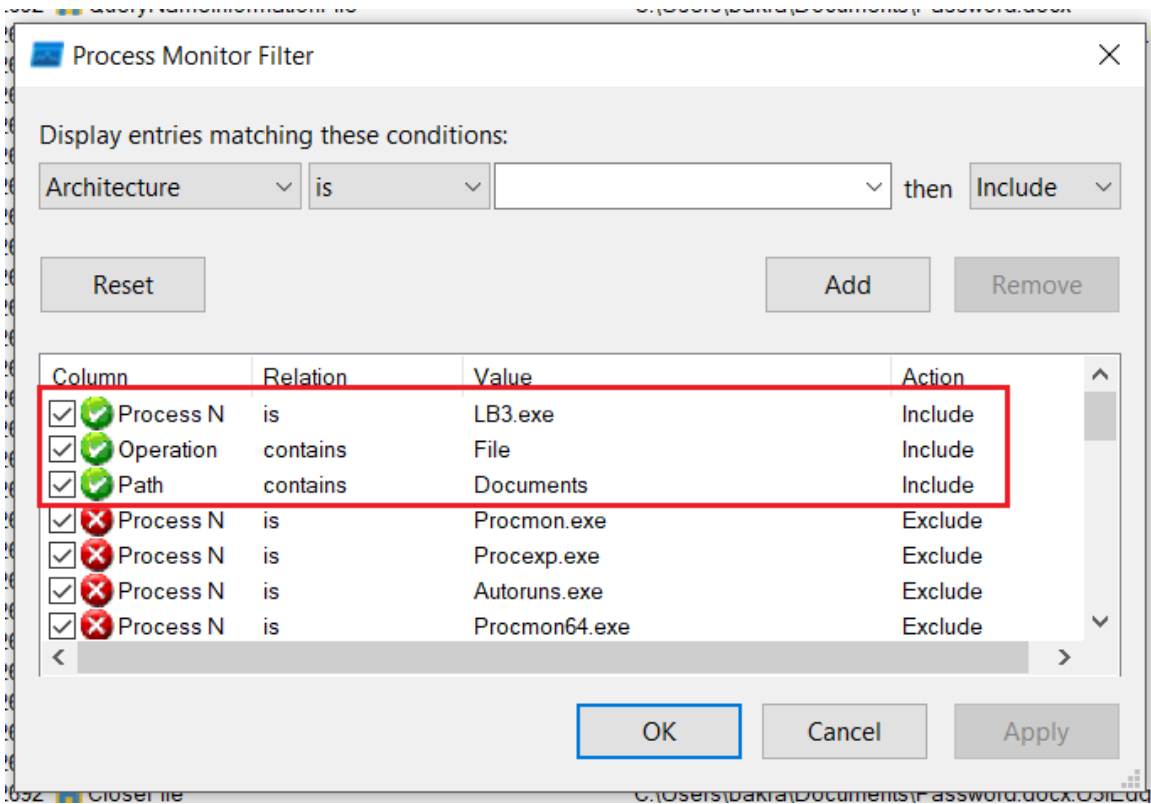


Figure 11 ProcMon filter for querying file encryption

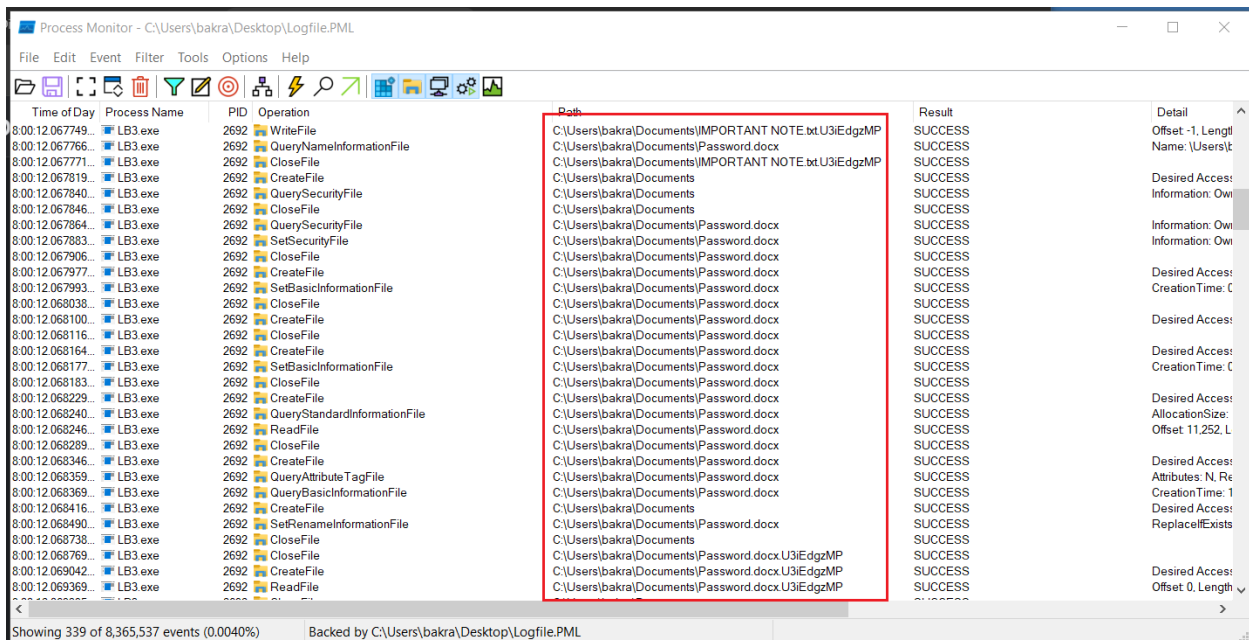


Figure 12 Dummy files modification events in ProcMon

The contents of the dummy files were encrypted after the execution and can be seen in the figure below.

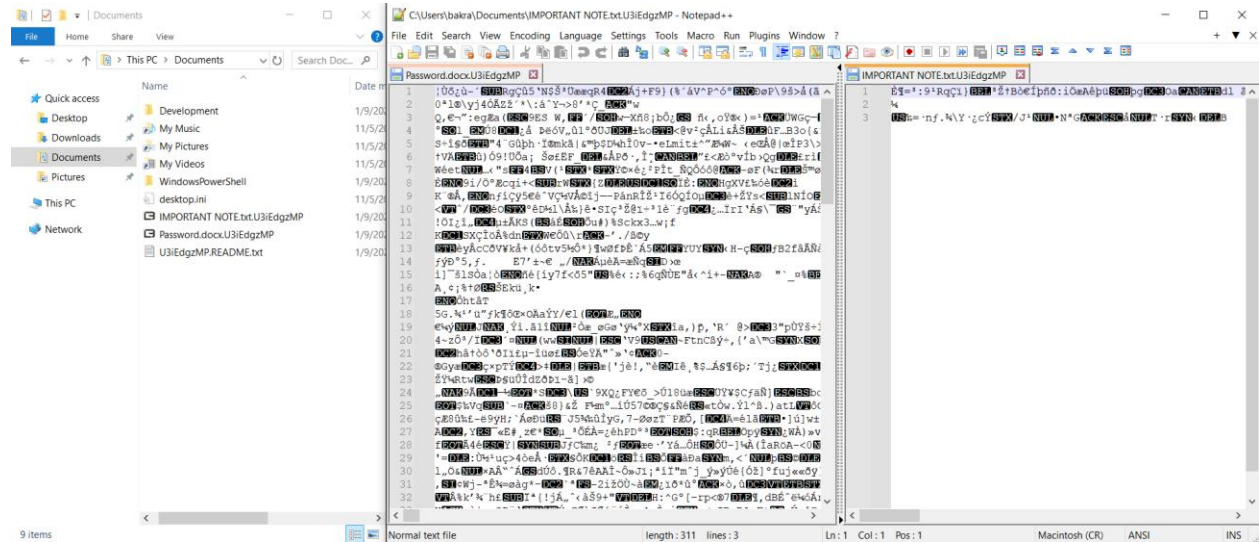


Figure 13 Contents of dummy files after malware execution

While LockBit was still running, Process Explorer was used to check the Network and Disk I/O rates by the LockBit process and, the Disk I/O rate is high which is one of the first indicator for any ransomware. However, analysing Network I/O and INetSim's log report, LockBit didn't send requests to any domain or ip address.

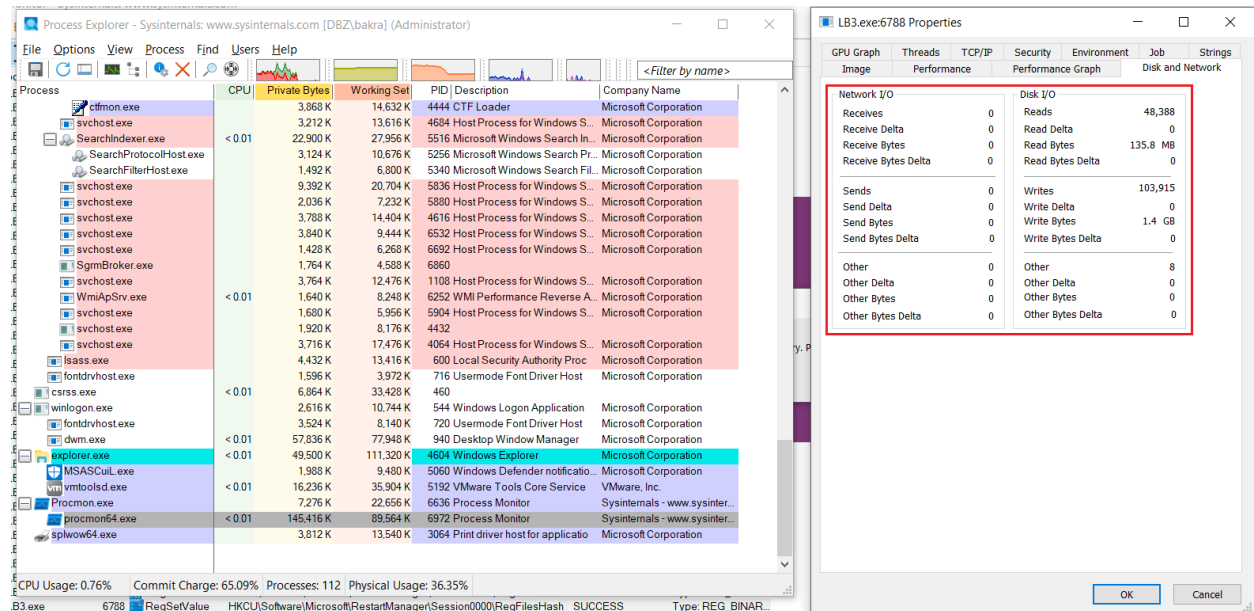


Figure 14 Monitoring Network and Disk I/O Statistics



```
Jan 7 11:14
remnux@remnux:/etc/inetsim
2024-01-07 10:53:47 HTTP connection, method: GET, URL: http://www.msftconnecttest.com/redirect, file name: /var/lib/inetsim/http/fakefiles/sample.html
2024-01-07 10:53:47 DNS connection, type: A, class: IN, requested name: clientservices.googleapis.com
2024-01-07 10:53:49 DNS connection, type: A, class: IN, requested name: update.googleapis.com
2024-01-07 10:53:51 DNS connection, type: A, class: IN, requested name: www.google.com
2024-01-07 10:53:54 DNS connection, type: A, class: IN, requested name: google.com
2024-01-07 10:53:54 DNS connection, type: A, class: IN, requested name: google.com
2024-01-07 10:53:54 HTTP connection, method: GET, URL: http://google.com/, file name: /var/lib/inetsim/http/fakefiles/sample.html
2024-01-07 10:53:54 HTTP connection, method: GET, URL: http://google.com/favicon.ico, file name: /var/lib/inetsim/http/fakefiles/favicon.ico
2024-01-07 10:53:56 DNS connection, type: A, class: IN, requested name: optimizationguide-pa.googleapis.com
2024-01-07 10:54:11 HTTP connection, method: GET, URL: http://www.msftconnecttest.com/connecttest.txt, file name: /var/lib/inetsim/http/fakefiles/sample.txt
2024-01-07 10:54:12 DNS connection, type: A, class: IN, requested name: dc.services.visualstudio.com
2024-01-07 10:54:13 DNS connection, type: A, class: IN, requested name: ctldl.windowsupdate.com
2024-01-07 10:54:13 HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl_cab?2c3dabc230e0de72, file name: /var/lib/inetsim/http/fakefiles/sample.html
2024-01-07 10:54:21 DNS connection, type: PTR, class: IN, requested name: 1.10.10.10.in-addr.arpa
2024-01-07 10:54:21 DNS connection, type: PTR, class: IN, requested name: 250.255.255.239.in-addr.arpa
2024-01-07 10:54:21 DNS connection, type: PTR, class: IN, requested name: b.8.c.4.0.d.7.f.2.d.b.8.c.4.0.c.b.8.1.4.0.2.c.e.0.8.a.0.a.0.a.0.ip6.arpa
2024-01-07 10:54:21 DNS connection, type: PTR, class: IN, requested name: f.f.f.f.b.8.6.8.d.b.6.8.0.d.8.f.0.0.0.0.0.1.0.1.8.a.0.a.0.a.0.ip6.arpa
2024-01-07 10:54:22 DNS connection, type: PTR, class: IN, requested name: 128.10.10.10.in-addr.arpa
2024-01-07 10:54:41 HTTP connection, method: GET, URL: http://www.msftconnecttest.com/connecttest.txt, file name: /var/lib/inetsim/http/fakefiles/sample.txt
2024-01-07 10:54:46 DNS connection, type: PTR, class: IN, requested name: 251.0.0.224.in-addr.arpa
2024-01-07 10:54:46 DNS connection, type: PTR, class: IN, requested name: e.9.2.b.4.2.3.6.8.f.8.4.6.7.4.a.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa
2024-01-07 10:54:46 DNS connection, type: PTR, class: IN, requested name: b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.ip6.arpa
```

*Figure 15 Log Report of INetSim's Fake Network*

The network requests that can be seen in the above figure are normal requests that was logged after testing the INetSim’s fake net status and while executing the LockBit ransomware. But there were no signs of malicious network requests made by the ransomware. Note that this probably defers from various versions of LockBit.

The above analysis for the LockBit is rather a simple process to verify the process of the ransomware. There are possibly many analysis procedures and various checks that could be done for this ransomware since LockBit has many variants and has been growing and evolving overtime. The variant used for this report was LockBit Black, there are other variants of LockBit such as LockBit Green, LockBit for Mac, etc. A rather good analysis for this ransomware can include downloading an active sample used by the LockBit’s affiliates than a sample generated by the Leaked builder that was used for this report. Static code analysis could also be done using decompilers and disassemblers such as Ghidra, IDA, etc for better view of the malware’s workflow.

## 4.2. Detection

LockBit along with other ransomwares never encrypt files until they are executed. Hence, Yara rules can be used to detect these ransomwares before they can get chance to execute. A popular repository for Yara rules can be found at <https://github.com/Neo23x0/signature-base/tree/master/yara>.

[ *Note: The rule set for detecting the executable used in this report can be found at [YARA Rule Set for Detection](#). ]*

```
$s14 = "4.4=4L4" fullword ascii
$s15 = "\\Q\"k*o" fullword ascii
$s16 = "SQRVW3" fullword ascii
$s17 = "_^ZY[]" fullword ascii
$s18 = "9|$0r4" fullword ascii
$s19 = "=$c=v=" fullword ascii
$s20 = "X_^ZY[" fullword ascii
condition:
  uint16(0) == 0x5a4d and filesize < 500KB and
  8 of them
}

remnux@remnux:~/LockBit3.0$ ls
Crypto_Ransomware_Lockbit3.yar  LB3.exe  test.yar
remnux@remnux:~/LockBit3.0$
remnux@remnux:~/LockBit3.0$
remnux@remnux:~/LockBit3.0$ yara Crypto_Ransomware_Lockbit3.yar LB3.exe
Crypto Ransomware LockBit3 LB3.exe
remnux@remnux:~/LockBit3.0$
remnux@remnux:~/LockBit3.0$
remnux@remnux:~/LockBit3.0$
```

*Figure 16 Yara detection using custom rule set for the built LockBit executable*

Other possible ways to detect malwares before execution can be by:

- Uploading the malware into online sandbox and analysis platforms such as Any Run, Joe Sandbox, Virus Total, Hybrid Analysis, etc.
- Hunting for Indicator of Compromises by going through open-source projects such as Abuse project.
- Navigating through MITRE ATT&CK Framework.

### 4.3. Prevention

In the August 21, 2021 "Russian OSINT" interview, LockBit openly communicated that organizations can reduce the likelihood of being targeted by the group through strategic measures. This includes engaging a dedicated red team service, ensuring comprehensive employee training to counter social engineering, and integrating high-quality anti-ransomware and antivirus software (Flashpoint, 2023).

As ransomware continues to advance, foundational cybersecurity defences, often deemed as "basic," can have a profound impact. If not already in place, give priority to adopting essential preventive measures such as:

- Patch management
- Network segmentation
- Least privilege access and control
- Strong password and MFA requirements
- User training on social engineering and phishing attacks
- Regular system backups

A project initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, Kaspersky, and McAfee named "No More Ransom" contains decryption tools for various ransomwares that can be beneficial for the victims and can be used for data recovery.

The project can be found at <https://www.nomoreransom.org/en/decryption-tools.html> .

## **Chapter 5 : Conclusion**

Malware is any code that modifies or deletes data to damage or prevent system from operating as intended. Since malware's origin, it has been constantly evolving and increasing loss along with cybercrimes, which is portrayed by two case studies of ALPHV BlackCat and LockBit on the Western Digital and Boeing.

The demonstration and analysis of custom built LockBit 3.0 using the leaked builder revealed that LockBit like other ransomware encrypts file and renames them with random string extension but does it faster than other ransomware that exist in the wild. Additionally, it demonstrated a persistent mechanism by querying and adding various windows registry keys.

LockBit like any other malware can be detected using various techniques, some of them being making use of YARA rules and various online analysis platforms. And it can be prevented by implementing various preventive measures.

## Chapter 6 : References

Abrams, L., 2023. *Hackers leak images to taunt Western Digital's cyberattack response.*

[Online]

Available at: <https://www.bleepingcomputer.com/news/security/hackers-leak-images-to-taunt-western-digitals-cyberattack-response/>

[Accessed 7 January 2024].

AV-ATLAS, 2024. *Malware & PUA.* [Online]

Available at: <https://portal.av-atlas.org/malware>

[Accessed 7 January 2024].

Baker, K., 2023. *THE 12 MOST COMMON TYPES OF MALWARE.* [Online]

Available at: <https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/>

[Accessed 10 January 2024].

Behling, D., 2022. *LockBit 3.0 Ransomware Unlocked.* [Online]

Available at: <https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html>

[Accessed 7 January 2024].

Belcic, I., 2020. *What is CryptoLocker Ransomware and How to Remove it.* [Online]

Available at: <https://www.avast.com/c-cryptolocker>

[Accessed 7 January 2024].

Cybersecurity and Infrastructure Security Agency, 2023. *Understanding Ransomware Threat Actors: LockBit, s.l.: s.n.*

Flashpoint, 2023. *LockBit Ransomware: Inside the World's Most Active Ransomware Group.*

[Online]

Available at: <https://flashpoint.io/blog/lockbit/>

[Accessed 9 January 2024].

Ilascu, I., 2023. *LockBit ransomware leaks gigabytes of Boeing data*. [Online]  
Available at: <https://www.bleepingcomputer.com/news/security/lockbit-ransomware-leaks-gigabytes-of-boeing-data/>  
[Accessed 7 January 2024].

Kaspersky, 2020. *LockBit ransomware — What You Need to Know*. [Online]  
Available at: <https://www.kaspersky.com/resource-center/threats/lockbit-ransomware>  
[Accessed 10 January 2024].

Luca Nagy, S. N. V. S., 2019. *GandCrab 101: All about the most widely distributed ransomware of the moment*. [Online]  
Available at: <https://news.sophos.com/en-us/2019/03/05/gandcrab-101-all-about-the-most-widely-distributed-ransomware-of-the-moment/>  
[Accessed 7 January 2024].

Martinez, F., 2022. *BlackCat ransomware*. [Online]  
Available at: <https://cybersecurity.att.com/blogs/labs-research/blackcat-ransomware>  
[Accessed 7 January 2024].

Mira, F., 2021. *A Systematic Literature Review on Malware*, Luton, UK: IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS).

Namanya, A. P. a. C. A. a. A. I. a. P. D. J., 2018. *The World of Malware: An Overview*, Barcelona: 2018 IEEE 6th International Conference on Future Internet of Things and Cloud.

Patrick Seguin, N. L., 2023. *The Essential Guide to Ransomware*. [Online]  
Available at: <https://www.avast.com/c-what-is-ransomware>  
[Accessed 7 January 2024].

Saengphaibul, V., 2022. *A Brief History of The Evolution of Malware*. [Online]  
Available at: <https://www.fortinet.com/blog/threat-research/evolution-of-malware>  
[Accessed 7 January 2024].

SentinelOne, 2023. *BlackCat Ransomware: In-Depth Analysis, Detection, Mitigation, and Removal*. [Online]

Available at: <https://www.sentinelone.com/anthology/blackcat/>

[Accessed 10 January 2024].

The MITRE Corporation, 2023. *BlackCat, Software S1068 | MITRE ATT&CK*. [Online]

Available at: <https://attack.mitre.org/software/S1068/>

[Accessed 07 January 2024].

## Chapter 7 : Appendix

### 7.1. Malware Types

- **Virus:** The oldest malware is a virus. Although it can self-replicate, it needs human interaction. This makes it passive. It spreads by human actions like file transfers and file executions. Attackers can use it to disrupt networks or systems, steal data, or build a botnet (Namanya, 2018). Example: Omega, Casino, Stoned, etc.
- **Worm:** Worm is also self-replicating malicious program, but it does not require human interaction. Once it takes over a system, it uses vulnerabilities in operating system or network to propagate further (Namanya, 2018). Example: Blaster, Morris worm, Stuxnet, etc.
- **Trojan:** Trojans are malware that disguises themselves as legitimate software. It can conceal itself in application, games and even software patches, as well as in phishing email attachments. Trojan horse usually spread through social engineering (Baker, 2023). Example: ZeroAccess, Emotet, Vundo, etc.
- **Ransomware:** Ransomwares are malware that encrypts all the data of targeted system to disrupt the availability until a ransom is paid. However, there is no assurance that payment will provide the required decryption key or that the offered decryption key will work properly (Baker, 2023). Example: WannaCry, Cryptolocker, Revil, etc.
- **Rootkit:** Rootkits are a type of malware that utilize a variety of technologies to evade detection and blend in with legitimate computer processes. It can be injected into legitimate firmware, kernel, or application (Namanya, 2018). Example: Zacinlo, Spicy Hot Pot, etc.
- **Bots:** Bots are malicious software that take orders from C2 servers for malicious tasks on compromised systems. Attackers create botnet, by creating a lot of bots to perform malicious activity like DDOS (Baker, 2023). Example: Echobot, Zeus, etc.

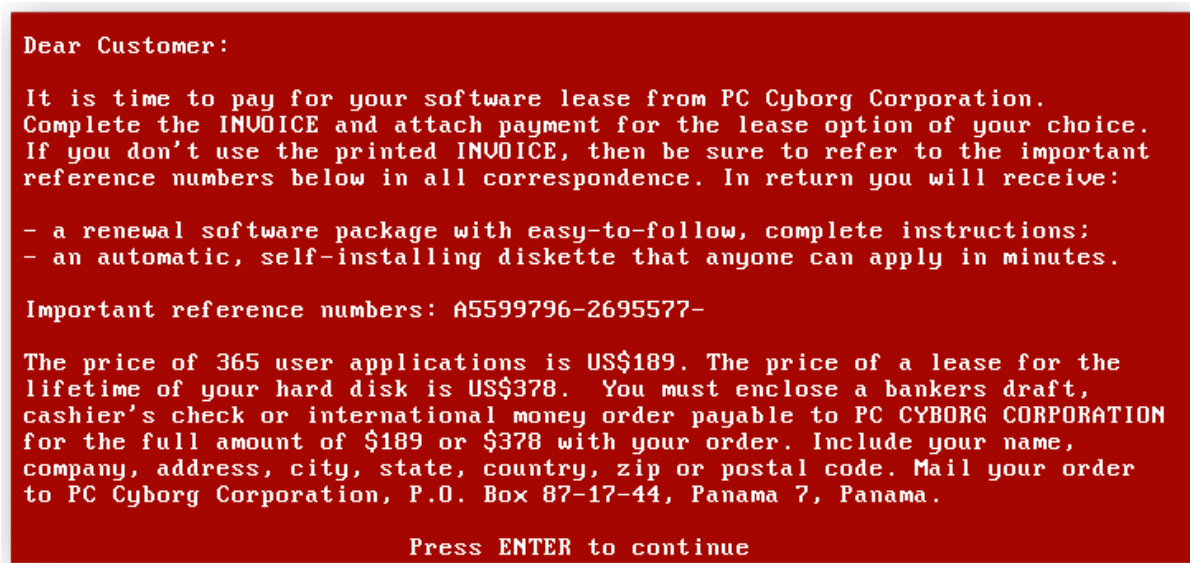


## 7.2. Evolution of Ransomware

### 7.2.1. World's First Ransomware

In 1989, the AIDS Trojan became the world's first ransomware, coinciding with the debut of public internet access via TheWorld ISP in the United States. Although internet connectivity was available, ransomware didn't exploit it until 2005. The Trojan, sent through physical mail on 20,000 infected floppy disks to AIDS researchers, encrypted files on the ninetieth reboot (Saengphaibul, 2022).

Attributed to Dr. Joseph Popp, it demanded \$189 for a yearly lease or \$385 for a lifetime license, with payments sent to a Panama PO Box. Despite claiming funds for AIDS research, forensic analysis linked the encryption key to Dr. Popp. Arrested in the UK, he was declared mentally unfit during proceedings and deported to the United States (Saengphaibul, 2022).



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue
```

*Figure 17 The AIDS Ransomware Note (Patrick Seguin, 2023).*

### 7.2.2. CryptoLocker - The Arrival of Cryptocurrency as a Payment option

CryptoLocker was the initial ransomware to request payment in Bitcoin. The decryption cost was set at two BTC, amounting to a modest sum for the threat actors in 2013, ranging between \$13 and \$1,100, depending on the timeframe (Saengphaibul, 2022).



Figure 18 CryptoLocker bitcoin ransom demand (Belcic, 2020).

### 7.2.3. GandCrab and The Emergence of Ransomware as a Service

GandCrab marked a turning point in cyber-attacks by popularizing ransomware for mass use through the Ransomware-as-a-Service (RaaS) model. This approach allowed GandCrab authors to refine their code while outsourcing attacks to affiliates, who handled tasks like reconnaissance and ransom collection. The authors stayed in the background, taking a cut (estimated between 25% and 40%) of the ransom. GandCrab, following an Agile development process, claimed to retire in 2019 after reportedly earning \$2 billion. The authors later loosely affiliated with Sodinokibi/REvil, which, in turn, had ties to DarkSide, known for the 2021 Colonial Pipeline attack. Notable RaaS variants post-GandCrab include BlackCat, Blackmatter, Conti, and Lockbit (Saengphaibul, 2022).



## GandCrab Launch of our dashboard as a service ransomware

By GandCrab, February 05 in [Software] - malware, exploits, bundles, crypts

Start new topic

GandCrab

(V)\_(S)\_(-)(V)



Seller

391 posts

Activity

вирусология

Posted February 05 (edited)

We announce the launch official of our new Dashboard, GandCrab as a service Ransomware:

Quote

You can see our prices, trust only the domain link

<http://gandcrabfd72vjxp.onion/>

<http://gandcr4cponzb2it.onion/>

You can contact us since: gandcrab@tutanota.com - gandcrabraas@exploit.im

We will inform you of the latest news our services are regularly updated.

**Warning** (For security, the url always starts with (gandcra or gandcr) you will be informed of news url.) We host the dashboard servers ourselves to ensure security.

С уважением, команда GandCrab.

Edited February 05 by GandCrab

*Figure 19 GandCrab Service Launch News (Luca Nagy, 2019).*

### 7.3. ALPHV BlackCat RaaS

BlackCat is a type of ransomware written in Rust and distributed through the Ransomware-as-a-Service (RaaS) model. It was initially detected in November 2021 and has been utilized to attack diverse sectors and organizations across continents, including Africa, the Americas, Asia, Australia, and Europe (The MITRE Corporation, 2023).

As of December 19, 2023, the FBI and Office of Public Affairs have officially declared the intervention and disruption of BlackCat/ALPHV ransomware activities. In conjunction with this announcement, decryption tools have been released and are accessible to all individuals affected by BlackCat/ALPHV ransomware operations. Those who have fallen victim to BlackCat ransomware are urged to reach out to their local FBI field office for additional details and guidance on the subsequent actions and available support options (SentinelOne, 2023).



Figure 20 BlackCat's Website Seized by FBI

## 7.4. LockBit RaaS

LockBit, previously recognized as the “ABCD” ransomware, has evolved into a distinctive threat among extortion cyberattacks, specifically classified as a ‘crypto virus’ due to its ransom demands linked to financial payments for decryption. Primarily targeting enterprises and government entities rather than individuals, LockBit's attacks commenced in September 2019 under the alias “.abcd virus,” referencing the file extension used during file encryption. Past notable targets encompass organizations in the United States, China, India, Indonesia, Ukraine, as well as several European countries like France, the UK, and Germany (Kaspersky, 2020). The LockBit Ransomware-as-a-Service (RaaS) and its associates have adversely affected organizations worldwide, irrespective of their size.

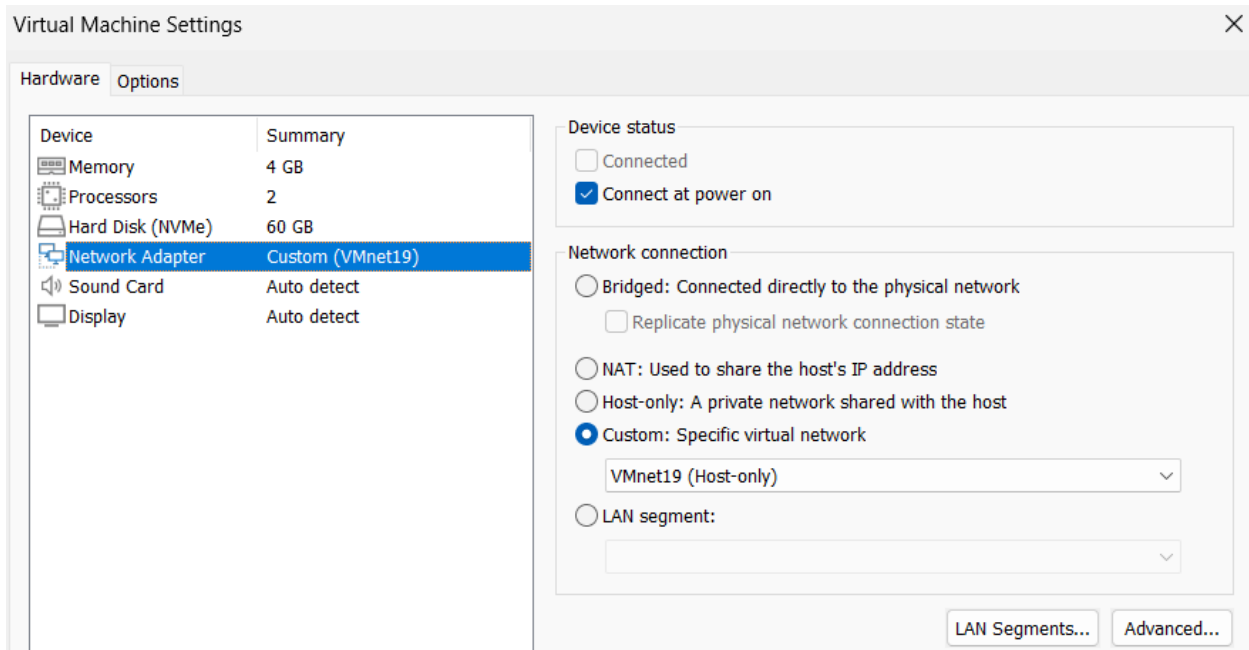
In the year 2022, LockBit emerged as the most prolific global ransomware group and RaaS provider, boasting the highest number of claimed victims on their data leak site. A RaaS cybercrime group essentially maintains and offers access to a specific ransomware variant, making it available to individuals or groups of operators known as "affiliates." In return, these affiliates contribute upfront payments, subscription fees, or a share of profits, or a combination of these (Cybersecurity and Infrastructure Security Agency, 2023).

LockBit has effectively attracted affiliates through various methods, including, but not limited to ensuring payment reliability by permitting affiliates to receive ransom payments upfront before distributing a share to the central group. This differs markedly from other Ransomware-as-a-Service (RaaS) groups that prioritize their own payment before allocating funds to affiliates. Criticizing other RaaS groups in online forums. Participating in attention-grabbing activities, such as offering incentives for people to get LockBit tattoos and placing a \$1 million reward for information disclosing the real-world identity of LockBit’s leader, known by the alias “LockBitSupp.” Developing and sustaining an uncomplicated, point-and-click interface for its ransomware, making it user-friendly for individuals with limited technical expertise (Cybersecurity and Infrastructure Security Agency, 2023).

## 7.5. Lab Setup for LockBit

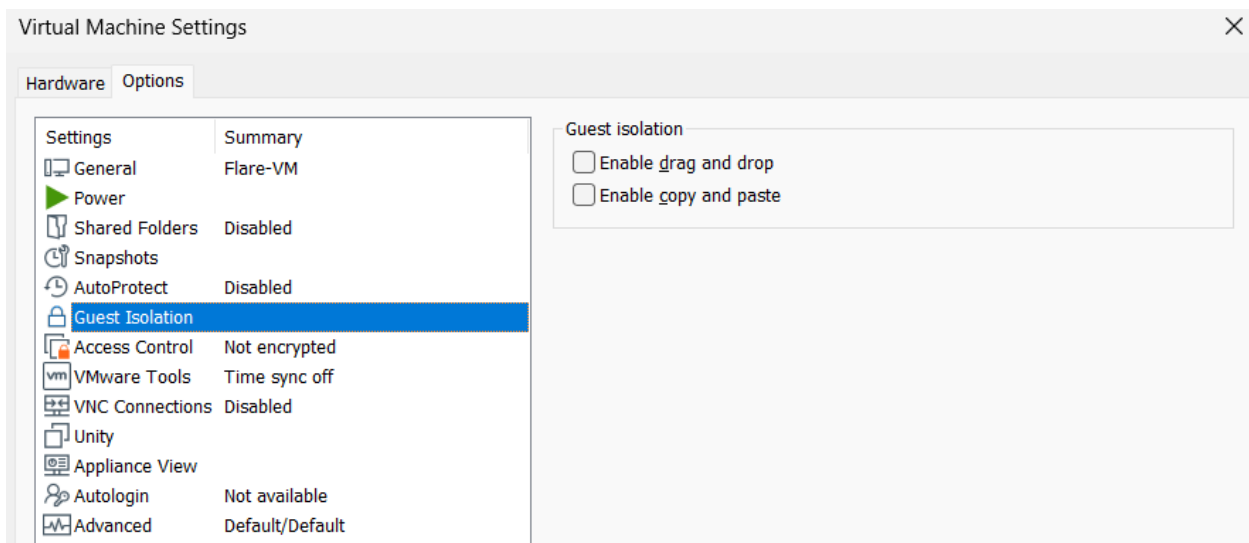
### 7.5.1. Isolate Flare-VM

First, the network adapter was changed to Host-Only so that, the VM will not be able to reach other networks.



*Figure 21 Setting Host-Only Network for Flare-VM*

Then, the VMware feature to drag and drop, copy and paste to the VM from Host machine was disabled, so that the malware wouldn't be able to reach the host at any cost.



*Figure 22 Enable Guest Isolation*

## 7.5.2. Configure INetSim Fake Net

Remnux's network adapter was also changed to Host-Only network so that, the Flare-VM would be able to communicate with it.

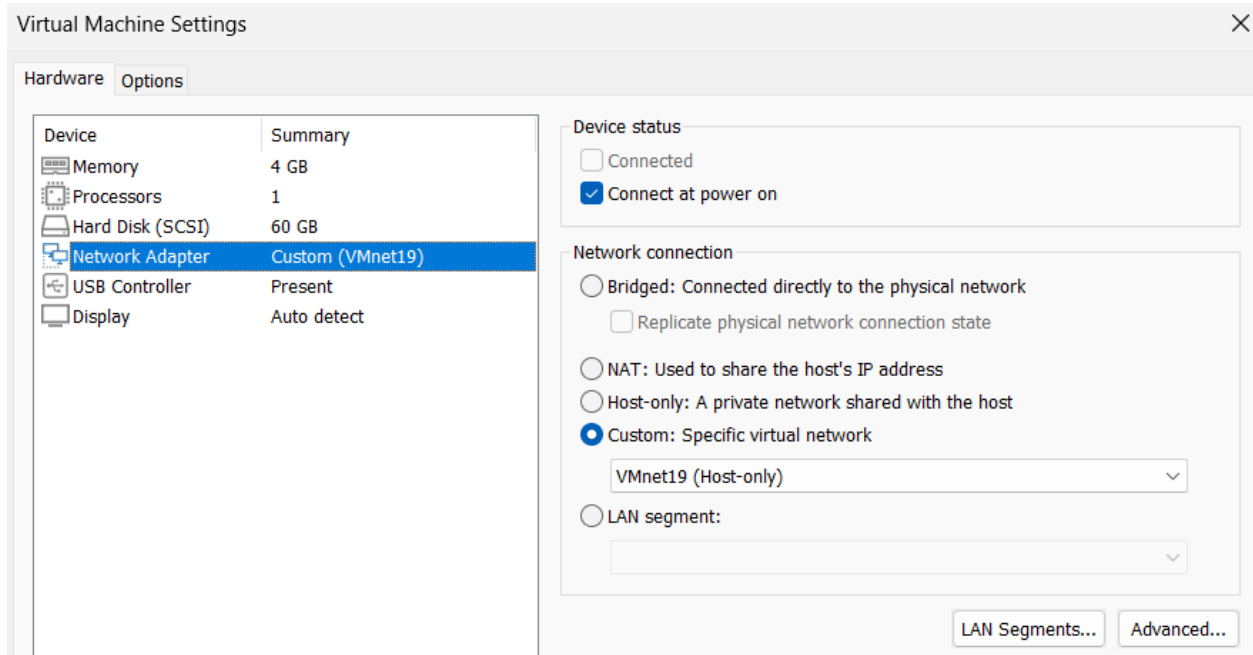


Figure 23 Setting Host-Only Network for Remnux

INetSim comes by default in Remnux, so the configuration file at `/etc/inetsim/inetsim.conf` was modified to capture the network requests that the ransomware could make.

```
#####  
# service_bind_address  
#  
# IP address to bind services to  
#  
# Syntax: service_bind_address <IP address>  
#  
# Default: 127.0.0.1  
#  
service_bind_address    10.10.10.128
```

Figure 24 Binding service address to Remnux address

Services such as DNS, HTTP, HTTPS was enabled for the fake net.

```
#
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
#start_service daytime_udp
start_service echo_tcp
start_service echo_udp
```

Figure 25 Enabling services for fake net

In Flare-VM, the network configuration was done so that the requests would go to through the fake net.

```
PS C:\Users\bakra>
PS C:\Users\bakra>
PS C:\Users\bakra> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::b516:7c0b:76b2:2b9e%8
    Default Gateway . . . . . : 10.10.10.128
PS C:\Users\bakra>
PS C:\Users\bakra>
PS C:\Users\bakra> _
```

Figure 26 IP address of Flare-VM



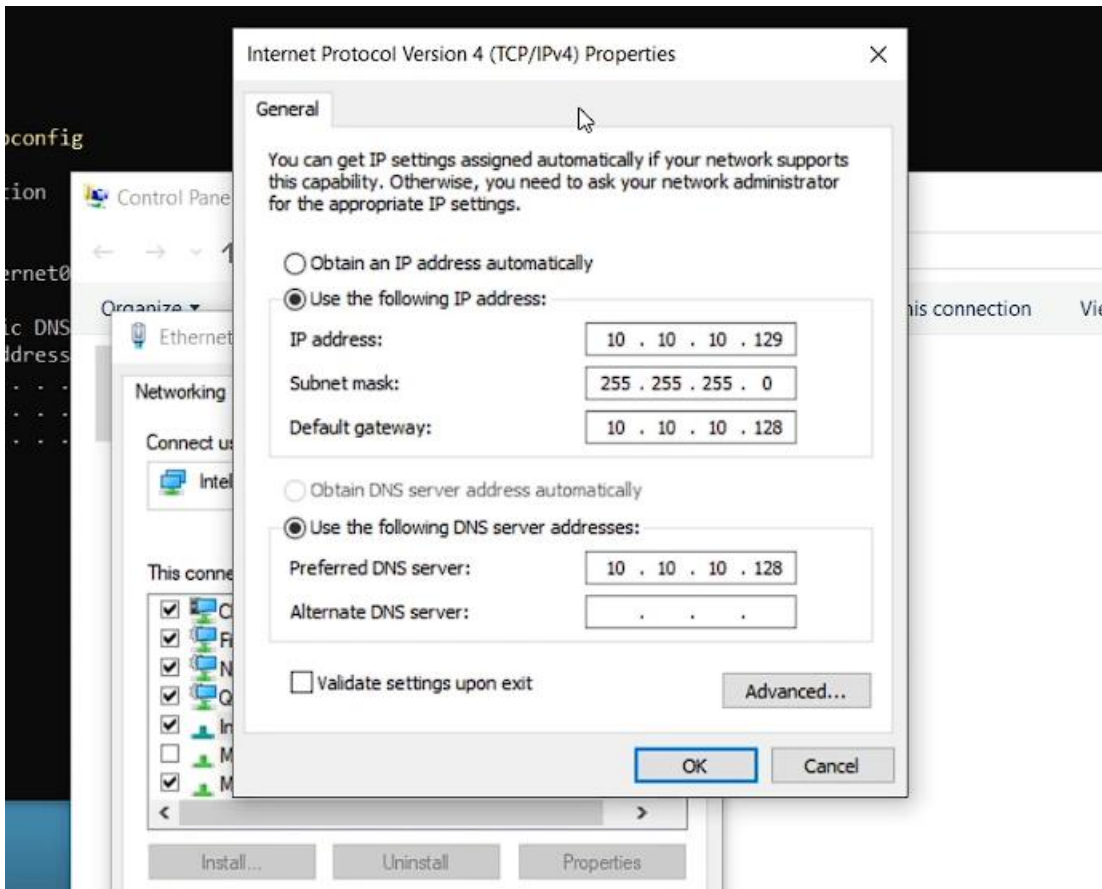


Figure 27 Network configuration for Flare-VM

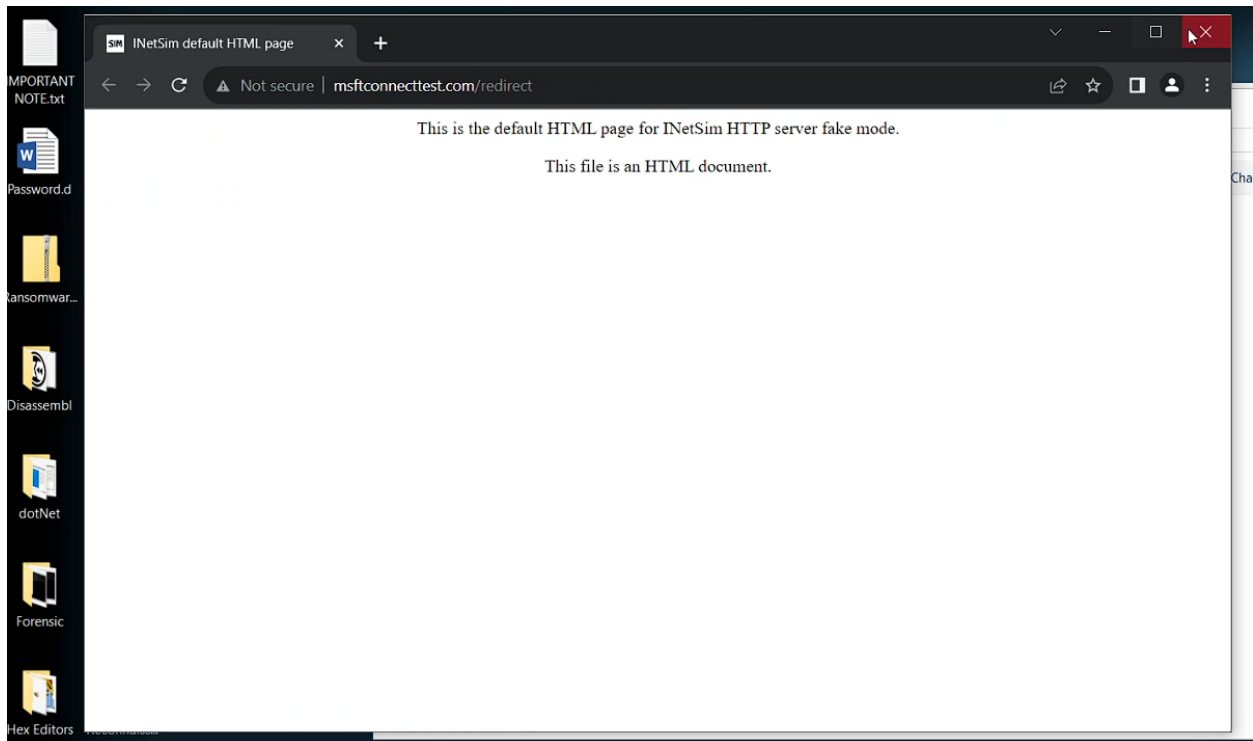
```
PS C:\Users\bakra> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

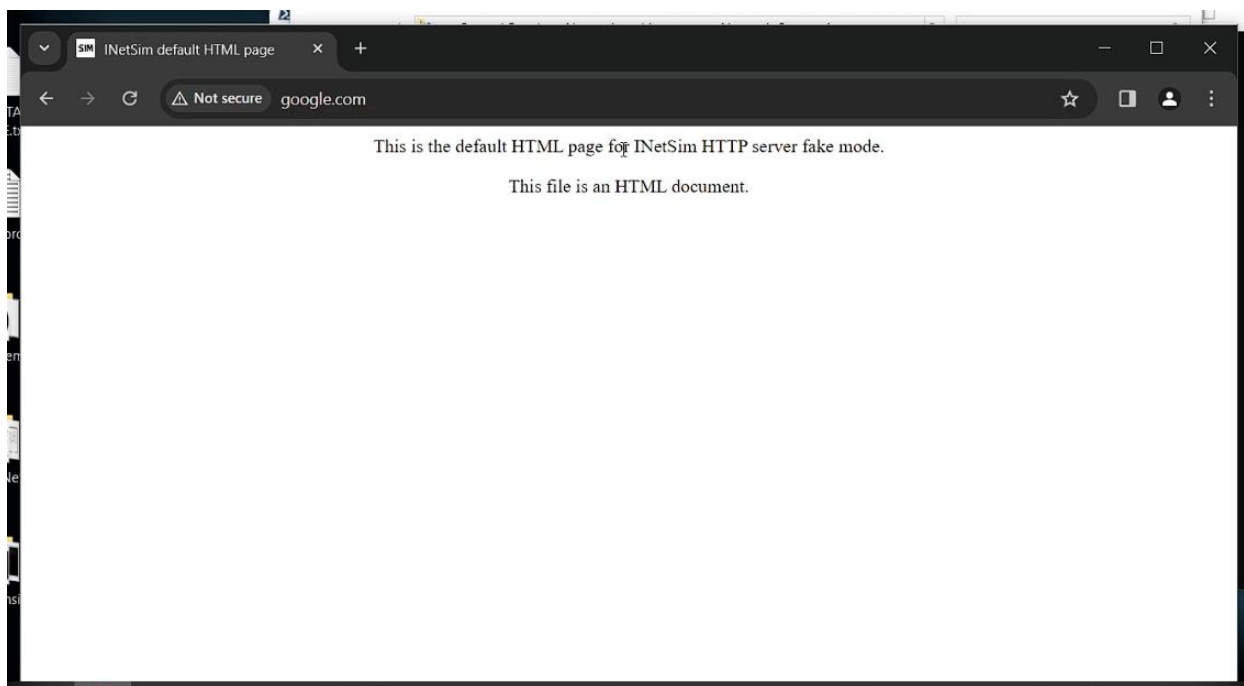
    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::b516:7c0b:76b2:2b9e%8
    IPv4 Address. . . . . : 10.10.10.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.128
PS C:\Users\bakra>
```

Figure 28 Verifying network configuration in Flare-VM



*Figure 29 INetSim default HTML page*

After all the network configuration, the machine automatically made request to msftconnecttest.com to check the internet connectivity, but it redirected to our INetSim fake net page. Then, google.com was visited to test to verify that INetSim worked properly.



*Figure 30 Verifying that the fake net works properly*

### 7.5.3. Build LockBit

The Leaked LockBit builder was already downloaded in Flare-VM. So after, the isolation and network configuration for fake net was complete. The config.json file for the builder was slightly modified and is shown in the figure below. The configuration file had many features, the custom ransom note could also be printed, and custom wallpapers could be changed as well.

```
5   },
6   "config": {
7     "settings": {
8       "encrypt_mode": "auto",
9       "encrypt_filename": false,
10      "impersonation": true,
11      "skip_hidden_folders": false,
12      "language_check": false,
13      "local_disks": true,
14      "network_shares": false,
15      "kill_processes": true,
16      "kill_services": true,
17      "running_one": false,
18      "print_note": true,
19      "set_wallpaper": true,
20      "set_icons": true,
21      "send_report": false,
22      "self_destruct": true,
23      "kill_defender": true,
24      "wipe_freespace": false,
25      "psexec_netspread": false,
26      "gpo_netspread": true,
27      "gpo_ps_update": true,
28      "shutdown_system": false,
29      "delete_eventlogs": false,
30      "delete_gpo_delay": 1
31    },
```

*Figure 31 LockBit Builder Configuration*

Features such as Network shares was disabled and Kill defender was enabled which can be seen in the figure above.

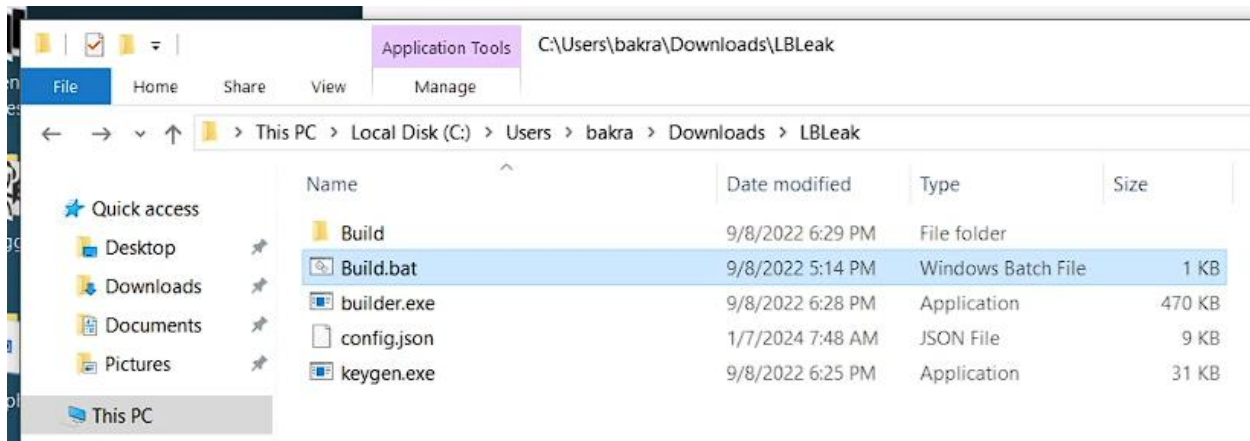


Figure 32 LockBit Builder file

After configuring everything for the builder, the build.bat was executed and the ransomware was built, and the compiled executables can be found in the Build directory along with the decryptor.

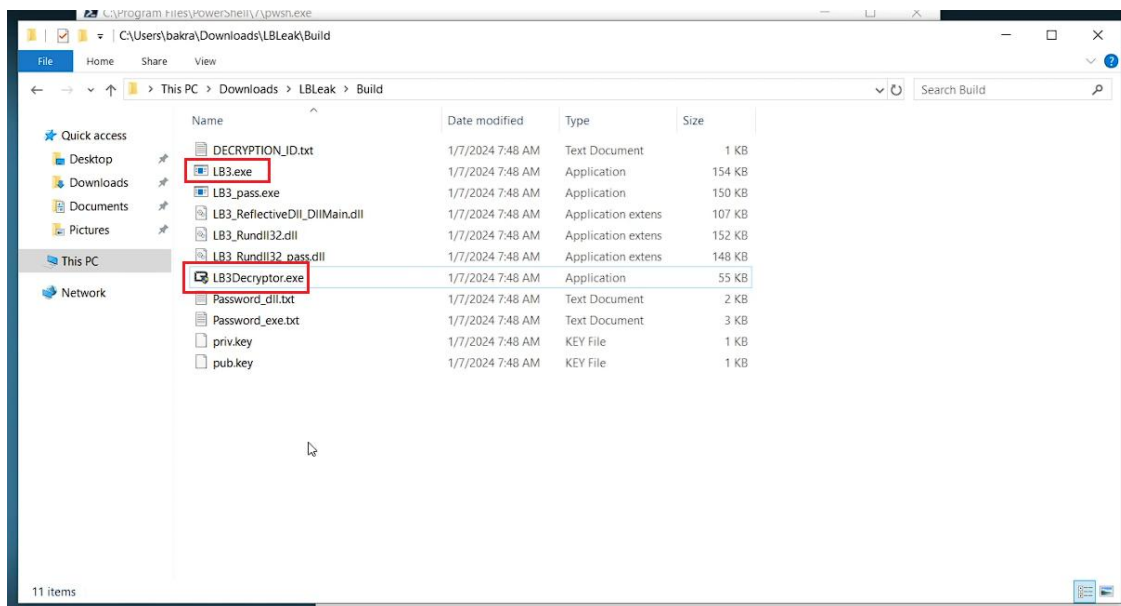


Figure 33 LockBit 3.0 compiled executable files

LB3.exe was the malware and LB3Decryptor.exe was the decryptor for the malware. LB3.exe depended on the various DLLs to run successfully, this included files such as LB3\_ReflectiveDll\_DllMain.dll and LB3\_Rundll32.dll. The priv.key and pub.key are for encrypting the files with extension that have been whitelisted in the configuration file.

```

Password_dll.txt - Notepad
File Edit Format View Help
Important information!

When using Safe Mode it is obligatory to write the full path to the file.
It is not recommended to use the root of the system disk to run the file, since on some versions of Windows it is forbidden to run from the
When using self-spread and impersonation, the files should be run with at least local administrator privileges on any computer on the netwo
Don't leak files and passwords to run, this will help bypass anti-viruses for as long as possible.

Важная информация!

При использовании Safe Mode обязательно нужно прописывать полный путь к файлу.
Не рекомендуется использовать корень системного диска для запуска файла, так как на некоторых версиях Windows запуск оттуда запрещён.
При использовании самораспространения и имперсонации, файлы нужно запускать как минимум с правами локального администратора на любом из ком
Не допускайте утечки файлов и паролей для запуска, это поможет обходить антивирусы как можно дольше.

### Global Mode:
rundll32 C:\Users\Administrator\Desktop\LB3_Rundll32_pass.dll,gd11 -pass da89d8ec761b3e82f21a552d27151830

### Safe Mode:
rundll32 C:\Users\Administrator\Desktop\LB3_Rundll32_pass.dll,sd11 -pass da89d8ec761b3e82f21a552d27151830

```

Figure 34 Content of Password\_dll.txt

```

Password_exe.txt - Notepad
File Edit Format View Help
Important information!

When using Safe Mode it is obligatory to write the full path to the file.
It is not recommended to use the root of the system disk to run the file, since on some versions of Windows it is forbidden to run from the
When using self-spread and impersonation, the files should be run with at least local administrator privileges on any computer on the netwo
Don't leak files and passwords to run, this will help bypass anti-viruses for as long as possible.

Важная информация!

При использовании Safe Mode обязательно нужно прописывать полный путь к файлу.
Не рекомендуется использовать корень системного диска для запуска файла, так как на некоторых версиях Windows запуск оттуда запрещён.
При использовании самораспространения и имперсонации, файлы нужно запускать как минимум с правами локального администратора на любом из ком
Не допускайте утечки файлов и паролей для запуска, это поможет обходить антивирусы как можно дольше.

### Global Mode:
LBB_pass.exe -pass 8f6d19ac779d90f0d63183f07fd1a5b4

### Safe Mode:
LBB_pass.exe -safe -pass 8f6d19ac779d90f0d63183f07fd1a5b4

### Target Mode:
LBB_pass.exe -path C:\file -pass 8f6d19ac779d90f0d63183f07fd1a5b4
LBB_pass.exe -path C:\folder -pass 8f6d19ac779d90f0d63183f07fd1a5b4
LBB_pass.exe -path C:\ -pass 8f6d19ac779d90f0d63183f07fd1a5b4
LBB_pass.exe -path \\?\Volume{11111111-2222-3333-4444-555555555555}\ -pass 8f6d19ac779d90f0d63183f07fd1a5b4

```

Figure 35 Content of Password\_exe.txt

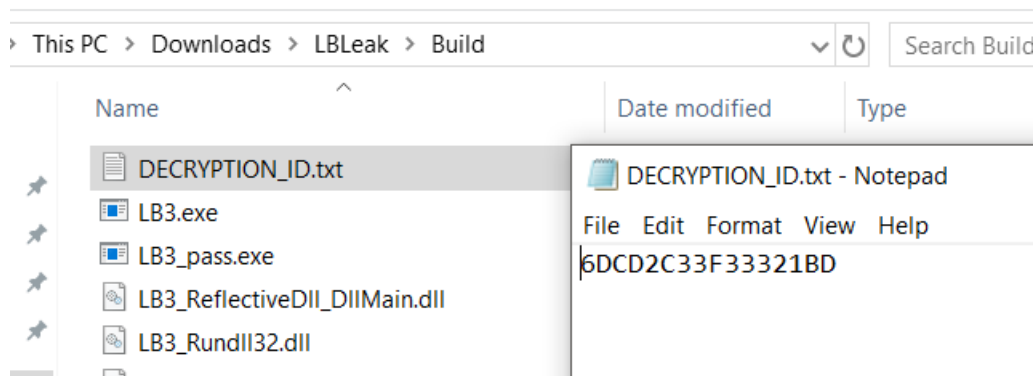
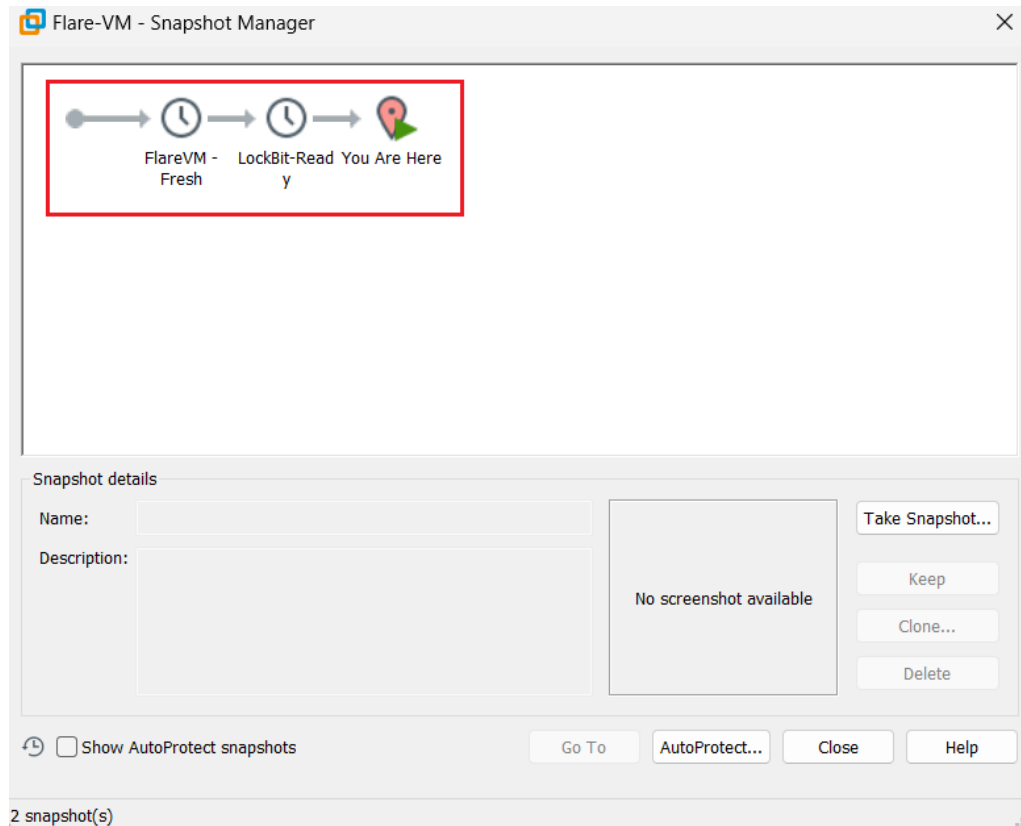


Figure 36 Decryption ID for the ransomware

Decryption ID in the case of LockBit are used by its affiliates to refer the campaigns they run and are possibly used to provide decryptor to its victim in the case where they pay the ransom.

### 7.5.4. Snapshot before Ransomware Execution

After the compiled executables were ready, the snapshot for the machine was taken so that the VM can be reverted to its fresh state.



*Figure 37 Machine snapshot before executing LockBit*

## 7.6. YARA Rule Set for Detection

YARA Rule Set for detecting the LockBit 3.0 generated for the demonstration in this report.

```
rule Crypto_Ransomware_LockBit3_0 {  
  
  meta:  
    description = "LockBit - file LB3.exe"  
    author = "Mingmar Lama"  
    reference = "https://github.com/Neo23x0/yarGen"  
    date = "2024-01-09"  
    hash1 = "852be3a373bd4ff6ad563592a9de4a348566603b04dedfdaca1a6d13f17ec819"  
  
  strings:  
    $s1 = "AmOJSs1" fullword ascii  
    $s2 = "?0N0]0I0" fullword ascii  
    $s3 = "5E6L6S6Z6" fullword ascii  
    $s4 = "4 444u4" fullword ascii  
    $s5 = "Loyn?P00" fullword ascii  
    $s6 = "o}c.eIt=" fullword ascii  
    $s7 = "2'2b2v2" fullword ascii  
    $s8 = "=V=\\={=" fullword ascii  
    $s9 = "D$PWSP" fullword ascii  
    $s10 = ";&;P;_;" fullword ascii  
    $s11 = "xoif\"_5;" fullword ascii  
    $s12 = "4f5l5x5~5" fullword ascii  
    $s13 = "9D$$ua" fullword ascii  
    $s14 = "4.4=4L4" fullword ascii  
    $s15 = "\\Q\"k*o" fullword ascii  
    $s16 = "SQRVW3" fullword ascii  
    $s17 = "_^ZY[]" fullword ascii  
    $s18 = "9|$0r4" fullword ascii  
    $s19 = "=$=c=v=" fullword ascii  
    $s20 = "X_^ZY[" fullword ascii  
  
  condition:  
    uint16(0) == 0x5a4d and filesize < 500KB and  
    8 of them  
}
```