IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ANALYSIS OF LOCKBIT BLACK RANSOMWARE TO IDENTIFY ITS STATIC, DYNAMIC AND NETWORK FOOTPRINTS FOR GENERATING ITS DETECTION SIGNATURES

[1]Arun Tyagi

School of Information Technology, Artificial Intelligence & Cyber Security,
Rashtriya Raksha University, Gandhinagar, India

Abstract: This paper focuses on analyzing the LockBit Black ransomware, a recent and potent threat that has particularly targeted the healthcare sector. As ransomware continues to evolve and combine various malicious functionalities, it becomes crucial to detect its patterns of infection and persistence methods to prevent data, system, and network contamination. By identifying these infections early, containment can be achieved, and further spread can be avoided. The paper discusses reports and data leaks highlighting LockBit Black's significant contributions to attacks. The method chapter explores different approaches to detecting ransomware, such as static, dynamic, and network-based methods. The paper then describes the specific approach taken in this study, including the tools utilized. The results and discussion section presents the creation of two sandbox environments for manual analysis and the corresponding findings. Additionally, the paper introduces five free online malware analysis platforms, whose reports were compared with the manual results. The IoCs (Indicators of Compromise) identified during the analysis are provided, enabling other researchers to create signatures for early detection, prevention, and the recording of forensic evidence. This study aims to analyze LockBit Black ransomware comprehensively and identify its footprints to serve as a valuable resource.

***Index Terms* - LockBit Black; Ransomware; Malware; Attack Signatures; Analysis.**

I. Introduction

A type of malicious software that encrypts the files of a victim is a ransomware. The attackers promise to restore the victim's access to the files but only after receiving the ransom payment. Because ransomware attacks frequently employ sophisticated strategies, they can be challenging to identify and stop. Ransomware comes in a wide variety of forms, and new varieties are continually being created. Ransomware has greatly changed throughout the years, moving from basic forms to complex Ransomware-as-a-Service (RaaS) models whose multiple stages and noticed changes of malware development are depicted in a study [1]. A few of the popular ransomware are illustrated in Table 1.

Table 1 Well Known Ransomware Families

No.	Ransomware	No.	Ransomware
1.	WannaCry	2.	SamSam
3.	Ryuk	4.	NotPetya
5.	LockerGoga	6.	AstraLocker
7.	REvil	8.	CheckMate
9.	Petya	10.	Maui
11.	CryptoLocker	12.	Zeppelin
13.	Locky	14.	Quantum
15.	CovidLock	16.	Sojusz

1.1 Reports:

According to a Sophos State of Ransomware report 2022 India ranked first with 80% of Encryption Rate in Ransomware Attacks i.e. Out of total Ransomware attacks 80% were successful in encrypting the valuable data, as shown in Figure 1.

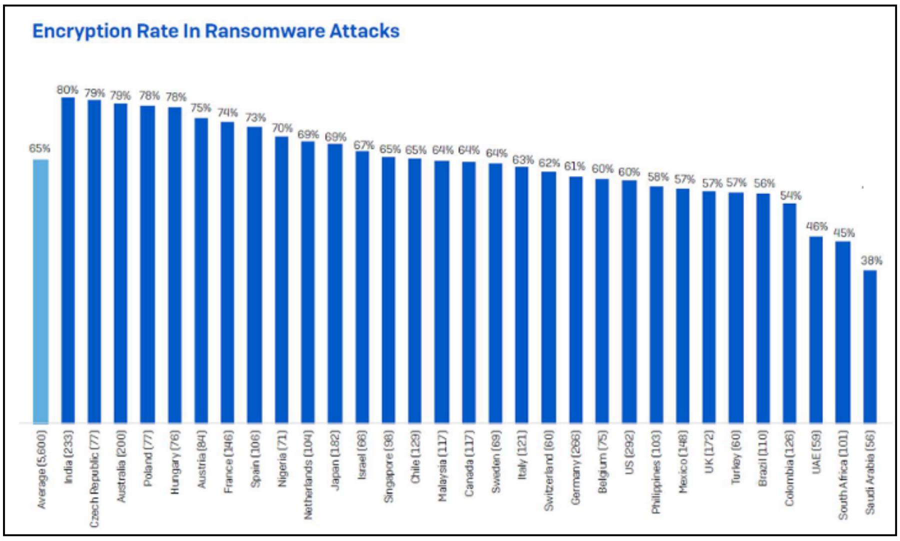


Figure 1. Encryption rate in ransomware attacks – report by Sophos

And the same report stated that Healthcare sector ranks top in Data restoring by paying the Ransom as shown in Figure 2.

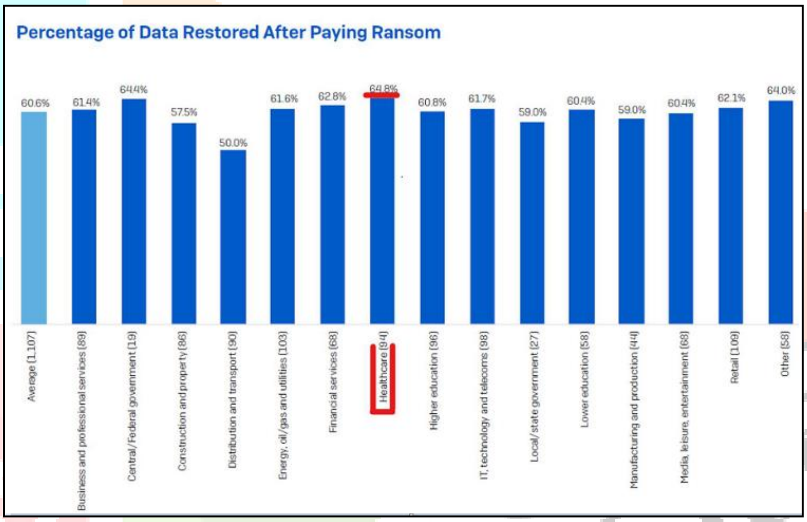


Figure 2. Percentage of data restored after paying ransom – report by Sophos

In addition, a report by Trend Micro identified three ransomware families, all of which were well-known for using the RaaS model, and that asserted to have conducted the most successful attacks in the first quarter of 2022. Figure 3 shows that, according to information obtained from the leak sites of their operators, LockBit was responsible for 35.8% of these attacks, Conti for 19%, and BlackCat for 9.6%.

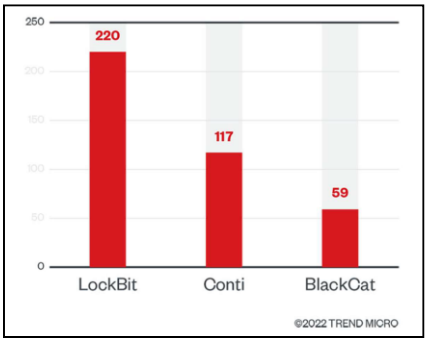


Figure 3. Trend Micro Report on Ransomware Attacks

LockBit dominated the most counts in February and March of 2022, according to further ransomware data that tracked detections of ransomware attempts to breach organisations, as seen in Figure 4.

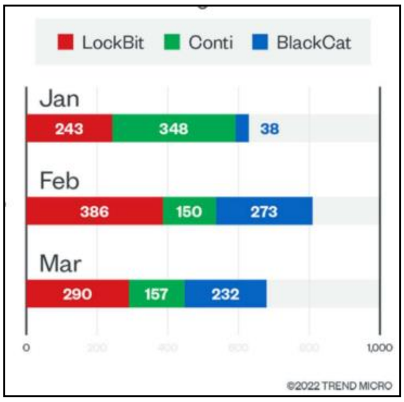


Figure 4. First Quarter Report on Ransomware Attacks – by Trend Micro

There report further states that Healthcare has been more targeted in recent years. Some examples of ransomware attacks that have targeted the healthcare sector include:

- WannaCry: The attack affected hospitals and other healthcare facilities in the United Kingdom, the United States, and other countries, causing significant disruptions to healthcare services.
- Ryazan: In 2020, Ryazan was used in an attack against the German University Hospital of Jena, which disrupted services and caused the theft of patient data.
- Ryuk: In 2019, Ryuk was used in an attack against Universal Health Services (UHS), a large healthcare provider in the United States. The attack disrupted services at UHS facilities across the country and resulted in the theft of patient data.

It is important for individuals and organizations to protect themselves against ransomware by regularly updating their software and security measures, and by being cautious when clicking on links or downloading attachments from unknown sources.

1.2 About LockBit version 3.0, a.k.a. LockBit Black:

With 220 self-reported successful RaaS and extortion assaults during the first quarter of 2022, the LockBit ransomware group dominated the RaaS sector. In one attack that received media attention, LockBit operators allegedly broke into the French Ministry of Justice in January.

LockBit issued yet another improved ransomware variant in June 2022, this time with a bug bounty scheme, Zcash payments, and additional extortion strategies. The new ransomware contains anti-analysis tactics to avoid detection, password-less execution, and an integrated command-line argument feature. It is derived from earlier malware such as BlackMatter and DarkSide.

A report by CyberSecurityWorks states that LockBit 3.0 additionally verifies the UI language of the target before launching an attack so as to avoid infecting any systems with the languages: Arabic (Syria), Armenian (Armenia), Azerbaijani (Cyrillic Azerbaijan), Azerbaijani (Latin Azerbaijan), Belarusian (Belarus), Georgian (Georgia), Kazakh (Kazakhstan), Kyrgyz (Kyrgyzstan), Romanian (Moldova), Russian (Moldova), Russian (Russia), Tajik (Cyrillic Tajikistan), Turkmen (Turkmenistan), Tatar (Russia), Ukrainian (Ukraine), Uzbek (Cyrillic Uzbekistan), Uzbek (Latin Uzbekistan)

1.3 Recent Attacks:

Lockbit has marked its presence in the wild and infected a huge number of systems and networks of reputed organization. It accounts to numerous incidents with some of the recent LockBit attacks as below:

- Whitworth University: In July 2022, a LockBit ransomware assault shut down all of this private university's operations for more than two weeks. The organization asserted that they had taken 715 GB of Whitworth data, including accounting, marketing, infrastructure, documentation, and more.
- Italian Revenue Agency: In July 2022, the LockBit gang launched the biggest cyberattack against the Italian Revenue Agency. The agency's servers had 78 GB of data taken during this incident.
- Entrust: In June 2022, the LockBit ransomware group broke into the network of security company Entrust and stole important data. In a surprising turn of events, Entrust countered with a Denial-of-Service attack on LockBit's servers, preventing them from disclosing the stolen information.
- Library lending app, Onleihe: After the service provider EKZ was attacked online in March 2022, the online library experienced operating problems. The attack had an effect on a number of related websites, statistics page and catalogue data, and ID-Delivery.
- Accenture: In August 2021, LockBit attacked Accenture and demanded $50M in ransom. Some confidential information was taken during this attack and posted on LockBit's leak site.

II. Method

2.1 Possible Methods of detecting & analysing ransomware:

To safeguard systems and priceless data, ransomware attacks must be identified and minimized. Many techniques have been created and used to recognize and stop ransomware attacks. The following methods have been shown to be efficient in finding ransomware:

1) Log File Monitoring: Analysis of log files is crucial in the detection of ransomware. A plethora of data on system events, user activities, and application behaviour can be found in log files. Security teams can spot any strange or unauthorized actions that can point to a ransomware attack by routinely monitoring and analysing log files. For instance, suspicious activity may be indicated by odd access attempts, changes to important files, or unexpected network traffic. Furthermore, log files serve as valuable forensic evidence, allowing investigators to reconstruct attack timelines, trace their activities, and identify affected systems [2]. The digital footprint captured in log files aids in understanding attack vectors, identifying ransomware variants, and strengthening defensive strategies through threat intelligence and proactive measures.

2) Monitoring the Windows Registry: In order to build persistence and carry out malicious operations, ransomware frequently modifies the Windows Registry. Monitoring registry changes can reveal information about ransomware attacks [3]. Security solutions detect unexpected or unauthorised changes that are connected to ransomware activities by monitoring and analysing these registry updates. This makes it possible to recognise the attack early and act quickly to lessen its effects.

3) Monitoring File System Activity: Keeping an eye on file system activity also helps in spotting ransomware assaults. The normal behaviour of ransomware is to encrypt or modify files, which causes an abrupt increase in file alterations or changes to file extensions. Organisations can spot these tendencies and alert to potential ransomware infestations by putting in place file system monitoring techniques. Early identification enables immediate action to stop more encryption or harm to important files. Any report of huge changes made to multiple files in a file system of a computer could indicate that a ransomware attack is underway. These may be detected by checking for:

   a. File entropy: This measures the randomness of a file. Encrypted and compressed files have high entropy compared to plaintext files. Comparing the value to previous calculations of a file to identify infection.

   b. File type: detecting change in extensions

   c. Similarity check: of any file using fuzzy hashing tools like Sdhash, Ssdeep

4) Static and dynamic analysis techniques are frequently used to recognise and examine dangerous software, including ransomware. Static analysis entails looking at a file's code, structure, and behaviour without actually running it. It aids in locating well-known ransomware signatures, harmful coding patterns, or suspicious activity. On the other hand, dynamic analysis entails executing files in a controlled setting in order to track their behaviour during runtime. Security analysts can identify ransomware behaviour, such as file encryption or communication with command-and-control servers, by keeping an eye on system interactions, network connections, and file activities during execution. Book titled "Learning Malware Analysis" is a concise guide that covers static and dynamic analysis techniques for malware and provides practical insights into dissecting malicious code, examining file structures, and observing runtime behavior equipping the reader with the necessary skills to enhance malware detection and analysis capabilities [4].

5) Network traffic analysis is a valuable method for detecting ongoing malware attacks by intercepting and analyzing network packets. Several key indicators can be utilized for effective detection:

   a. Message Frequency: The frequency of packets, such as TCP, HTTP, and UDP, can provide insights into malware attacks. Notably, as observed in the study that Locky ransomware significantly increases the number of HTTP POST request packets within the traffic stream compared to regular traffic [5]. Additionally, an abnormal number of TCP RST and TCP ACK packets in Locky's traffic may indicate the abnormal termination of malicious TCP connections.

   b. Packet Size: By examining the message size derived from HTTP packet headers, the average size of messages exchanged between the infected host and the command-and-control (C&C) server can be determined. Analyzing these statistics enables the creation of an anomaly detection system based on message size. Unusually large or small packet sizes compared to normal traffic can indicate malicious activity.

   c. Malicious Domains: Recording and analyzing all domains present in network traffic and comparing them against a blacklist database can help identify malicious domains associated with ransomware activities. By flagging any matches, potential communication with malicious servers can be identified, facilitating prompt action.

   d. Log Files: Analyzing DNS and NetBIOS logs can aid in detecting ransomware attacks. By scrutinizing these logs, unusual activities or unauthorized access attempts related to these protocols can be identified.

   e. DGA Detection: Some ransomware variants leverage a Domain Generation Algorithm (DGA) to generate a vast number of domain names, serving as rendezvous points for their C&C servers. Detection systems as proposed in study, work by identifying the DGA patterns and subsequently blocking all generated domains [6]. This approach mitigates the risk of relying on hardcoded domain addresses susceptible to blacklisting.

2.2 Approach followed:

For this study, two samples of LockBit Black (or LockBit 3.0) ransomware were collected from the app.any.run website and malware bazaar. Two separate sandbox environments were created for analysis purposes. The first environment consisted of Windows 11, Kali Linux, and a VyOS router running on VMware. The second environment included Windows 7 and a REMnux machine on VirtualBox. The Windows and Linux machines were isolated from the host machine and the internet but kept on the same network. The virtual machines served different purposes:

1) Windows 11 Professional and Windows 7 were used as testing machines to intentionally infect them with the ransomware samples. These machines were also equipped with the necessary tools and had clean snapshots taken for comparison.
2) The VyOS router was configured to connect the Windows and Linux machines in an isolated network environment. This is not a necessary part but can assist in collecting network logs.
3) Kali Linux and REMnux were utilized for running network simulations and packet sniffing. These machines were responsible for collecting logs during the analysis process. REmote Network Unified eXecutor (REMnux) is a Linux-based operating system designed for analyzing and investigating malicious software. A study suggests REMnux for malware analysis as it provides a range of open-source tools specifically tailored for malware analysis, reverse engineering, and threat intelligence [7]. REMnux includes tools for examining file formats, analyzing network traffic, unpacking malware, and extracting valuable artifacts for further analysis. It also supports virtualization technologies, making it easy to set up and manage sandbox environments for safe malware execution.

In order to analyze the malware, the sandbox environment was set up, utilizing the aforementioned machines and deploying various tools. It is worth mentioning that a research paper contains an extensive compilation of tools that can be referred to for effective malware detection and analysis [8]. Further, the detailed list of the tools used in this study can be found in Table 2.

Table 2 Tools for malware analysis

No.	Tools	Function
1.	Wireshark	Used for capturing and analysing packets on Linux System
2.	Process Monitor + Noriben script	Used for capturing filtered (necessary) activities in windows system. The activities include Registry, Files, Process, DLLs, etc.
3.	Process Hacker	Used on Windows system to monitor Process activity.
4.	Pestudio	Comes with VirusTotal plugin and is used for static analysis on Windows system.
5.	Get-FileHash/ HashCalc	Used for calculating hashes on windows system.
6.	RSyslog	Used on Linux system for collecting logs from Windows VM and Router.
7.	Inet Simulator	Used on Linux System to simulate various Network and Internet services for Windows system.

The main objective of the paper is to analyze and identify indicators of compromise (IoCs) related to the LockBit Black ransomware, including file names, file hashes, infection flow, communication patterns, and protocols used. To achieve this objective, several methods were employed:

1) Static analysis: This involved examining the ransomware sample's characteristics, structure, and embedded information without execution.
2) Dynamic analysis: The sample was executed in a controlled environment to observe its behavior, such as file modifications, network connections, and system interactions.
3) Packet analysis: Network traffic generated by the ransomware was captured and analyzed to identify communication patterns, such as the type of packets exchanged and the protocols used.
4) Flow analysis: The flow of infection within the sandbox environment was studied to understand how the ransomware propagated and affected the system.
5) Fuzzy hash: Fuzzy hashing techniques, such as sdhash or ssdeep, were employed to compare file similarities and detect potential variations of the ransomware. These techniques are proven valuable in detecting and analyzing variations among malicious files [9].

Additionally, to validate the findings from manual analysis, the ransomware sample was also analyzed using five different online malware analysis platforms. These platforms provided free access and generated comprehensive reports on the behavior and characteristics of the sample. The list of these platforms is provided in Table 3.

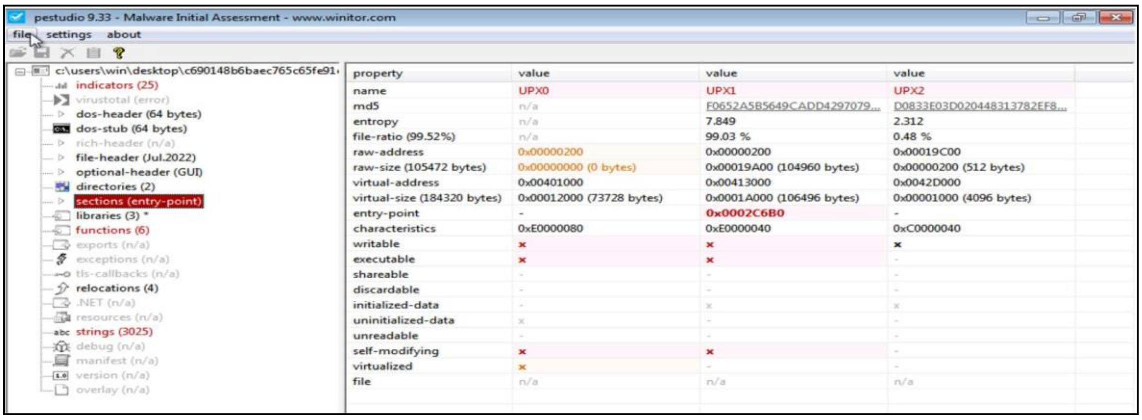
Table 3 Online Malware analysis platforms

No.	Platform	Website
1.	Any Run	https://app.any.run/
2.	Triage	https://tria.ge/
3.	JoeSandbox	https://www.joesandbox.com/
4.	Hybrid Analysis	https://www.hybrid-analysis.com/
5.	Intezer Analyze	https://analyze.intezer.com/

III. Result and Discussion

3.1 Static analysis: Analysis performed on local Sandbox environment.

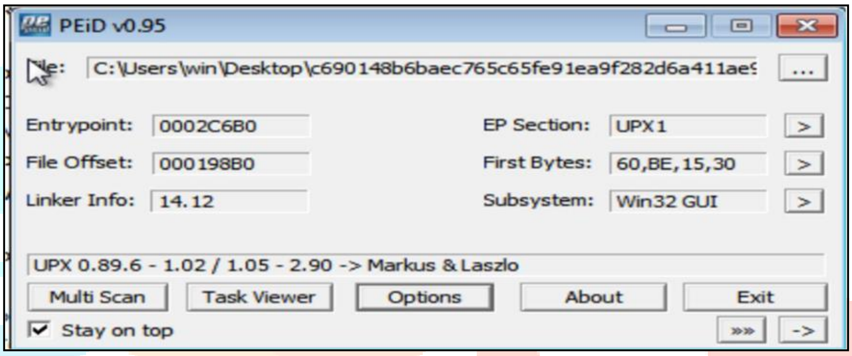
Static analysis is a technique employed to examine code or application software without executing them, allowing for the identification of issues or vulnerabilities. This approach is commonly used by developers and malware researchers to gain insights into the structure, syntax, and semantics of the code. Various tools are available for static analysis based on the application platform. In the case of Windows executables, PE-Studio is a notable tool [10]. The free version of PE-Studio can be downloaded from https://www.winitor.com/download. For the analysis of executable sample files, it was subjected to PE-Studio (free version), which provided valuable details. Notably, PE-Studio identified sections labeled as UPX0, UPX1, and UPX2, indicating that the ransomware was packed using the UPX packer. Furthermore, the entry-point at the UPX1 section was identified as the unpacking stub for UPX2, providing key insights into the malware's unpacking process as shown in Figure 5.



property	value	value	value
name	UPX0	UPX1	UPX2
md5	n/a	F0652A5B5649CADD4297079...	D0833E03D020448313782EF8...
entropy	n/a	7.849	2.312
file-ratio (99.52%)	n/a	99.03 %	0.48 %
raw-address	0x00000200	0x00000200	0x00019C00
raw-size (105472 bytes)	0x00000000 (0 bytes)	0x00019A00 (104960 bytes)	0x00000200 (512 bytes)
virtual-address	0x00401000	0x00413000	0x0042D000
virtual-size (184320 bytes)	0x00012000 (73728 bytes)	0x0001A000 (106496 bytes)	0x00001000 (4096 bytes)
entry-point	-	0x0002C6B0	-
characteristics	0xE0000080	0xE0000040	0xC0000040
writable	x	x	x
executable	x	x	-
shareable	-	-	-
discardable	-	-	-
initialized-data	-	x	x
uninitialized-data	x	-	-
unreadable	-	-	-
self-modifying	x	x	-
virtualized	x	-	-
file	n/a	n/a	n/a

Figure 5. Identifying packed sections on PEstudio

In addition to PE-Studio, another tool called PEiD was utilized for further analysis. PEiD also confirmed the presence of the UPX packer in the examined sample, with the entry point section identified as UPX1 as shown in Figure 6. The convergence of findings from multiple tools strengthens the reliability of the analysis and provides valuable insights into the malware's packing and unpacking mechanisms.



File: C:\Users\win\Desktop\c690148b6baec765c65fe91ea9f282d6a411ae

Entrypoint: 0002C6B0

EP Section: UPX1

File Offset: 000198B0

First Bytes: 60,BE,15,30

Linker Info: 14.12

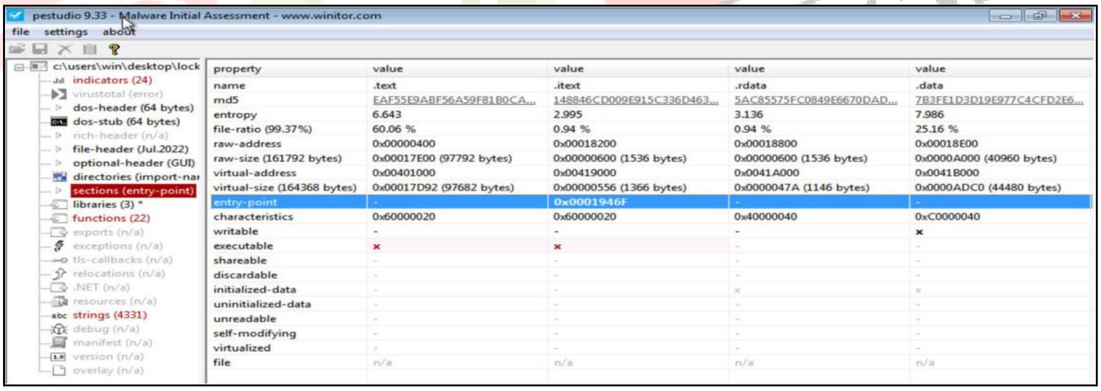
Subsystem: Win32 GUI

UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & Laszlo

☑ Stay on top

Figure 6. Identifying Packer and Entry point on PEiD

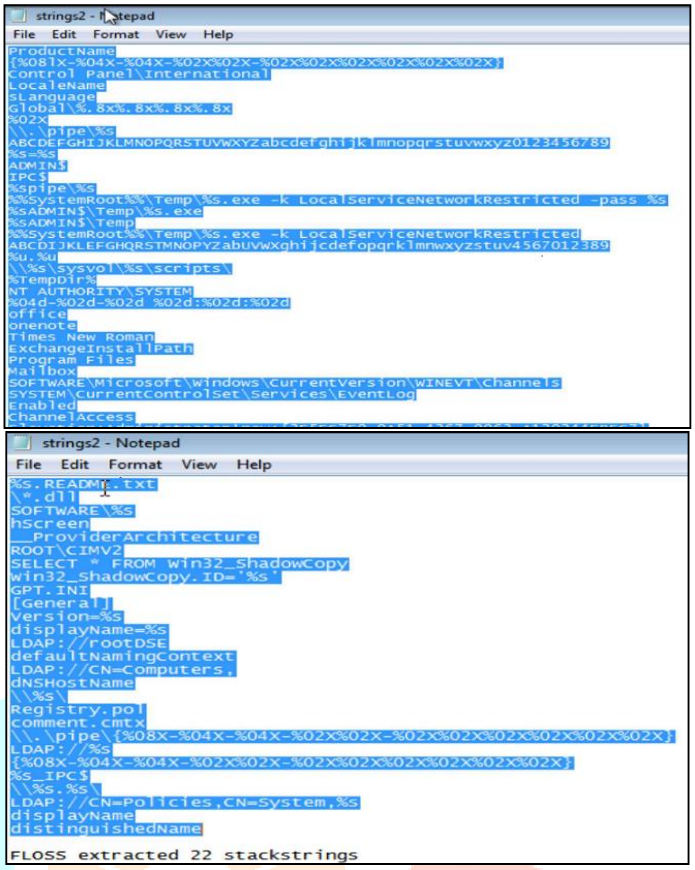
After identifying that the file was packed using the UPX packer, an unpacking process was performed using the UPX tool, which can be obtained from https://upx.github.io/. The unpacked version of the file was then subjected to further analysis using PE-Studio. The results of this analysis revealed significant enhancements compared to the packed version. Specifically, the unpacked file exhibited multiple sections and a notable increase in the number of functions and strings as shown in Figure 7.



property	value	value	value	value
name	.text	.itext	.rdata	.data
md5	EAF55E9ABF56A59F81B0CA...	148846CD009E915C336D463...	5AC85575FC0849E6670DAD...	7B3FE1D3D19E977C4CFD2E6...
entropy	6.643	2.995	3.136	7.986
file-ratio (99.37%)	60.06 %	0.94 %	0.94 %	25.16 %
raw-address	0x00000400	0x00018200	0x00018800	0x00018E00
raw-size (161792 bytes)	0x00017E00 (97792 bytes)	0x00000600 (1536 bytes)	0x00000600 (1536 bytes)	0x0000A000 (40960 bytes)
virtual-address	0x00401000	0x00419000	0x0041A000	0x0041B000
virtual-size (164368 bytes)	0x00017D92 (97682 bytes)	0x00000556 (1366 bytes)	0x0000047A (1146 bytes)	0x0000ADC0 (44480 bytes)
entry-point	-	0x0001946F	-	-
characteristics	0x60000020	0x60000020	0x40000040	0xC0000040
writable	-	-	-	x
executable	x	x	-	-
shareable	-	-	-	-
discardable	-	-	-	-
initialized-data	-	-	x	x
uninitialized-data	-	-	-	-
unreadable	-	-	-	-
self-modifying	-	-	-	-
virtualized	-	-	-	-
file	n/a	n/a	n/a	n/a

Figure 7. Identifying sections of Unpacked malware on PEstudio

It is worth mentioning that the professional version of PE-Studio offers additional features such as exports, resources, and VirusTotal integration. In the analysis of strings present in the source code, two additional tools, namely strings.exe (available at https://docs.microsoft.com/en-us/sysinternals/downloads/strings) and floss.exe (accessible at https://github.com/mandiant/flare-floss/releases), were utilized. These tools enabled the extraction of both ASCII and Unicode strings. As a result, a list of strings were identified as shown in Figure 8.



```
ProductName
{%081x-%04x-%04x-%02x%02x-%02x%02x%02x%02x%02x%02x}
Control Panel\International
LocaleName
sLanguage
Global\%.8x%.8x%.8x%.8x
%02x
\\.\pipe\%s
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789
%s=%s
ADMIN$
IPC$
%spipe\%s
%%SystemRoot%%\Temp\%s.exe -k LocalServiceNetworkRestricted -pass %s
%sADMIN$\Temp\%s.exe
%sADMIN$\Temp
%%SystemRoot%%\Temp\%s.exe -k LocalServiceNetworkRestricted
ABCDIJKLEFGHQRSTMNOPYZabUVwXghijcdefopqrklmnwxyzstuv4567012389
%u.%u
\\%s\sysvol\%s\scripts\
%TempDir%
NT AUTHORITY\SYSTEM
%04d-%02d-%02d %02d:%02d:%02d
office
onenote
Times New Roman
ExchangeInstallPath
Program Files
Mailbox
SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels
SYSTEM\CurrentControlSet\Services\EventLog
Enabled
ChannelAccess
```

```
%s.README.txt
\*.dll
SOFTWARE\%s
hScreen
__ProviderArchitecture
ROOT\CIMV2
SELECT * FROM Win32_ShadowCopy
Win32_ShadowCopy.ID='%s'
GPT.INI
[General]
Version=%s
displayName=%s
LDAP://rootDSE
defaultNamingContext
LDAP://CN=Computers,
dNSHostName
\\%s\
Registry.pol
comment.cmtx
\\.\pipe\{%08X-%04X-%04X-%02X%02X-%02X%02X%02X%02X%02X%02X}
LDAP://%s
{%08X-%04X-%04X-%02X%02X-%02X%02X%02X%02X%02X%02X}
%s_IPC$
\\%s.%s\
LDAP://CN=Policies,CN=System,%s
displayName
distinguishedName

FLOSS extracted 22 stackstrings
```

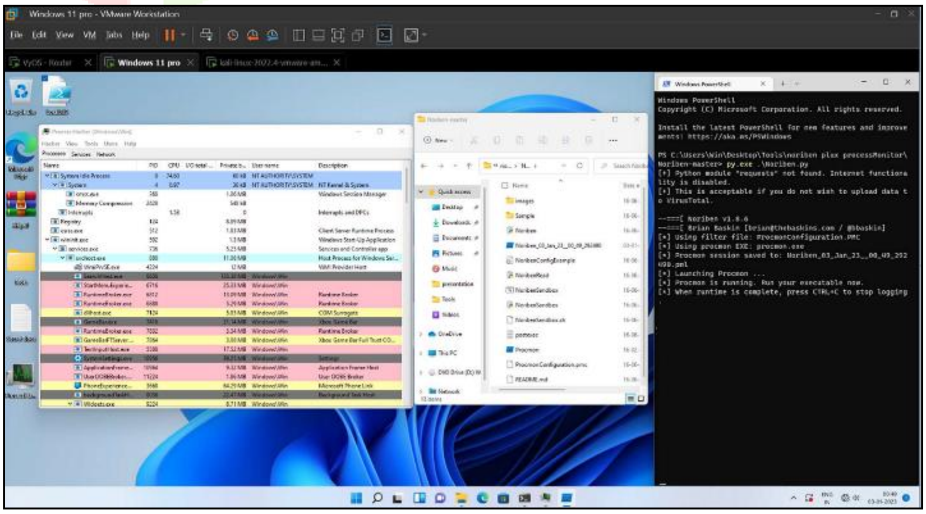
Figure 8. Identifying ASCII and Unicode Strings using STRINGS and FLOSS

Subsequently, multiple hash values were computed using tools such as HashCalc and Ssdeep. These hash values serve as important indicators of compromise and their corresponding results are elaborated at the end of this section. By analyzing the hash values, researchers can establish connections, identify similarities, and gain insights into the nature of the ransomware, facilitating its detection and prevention in real-world scenarios.

3.2 Dynamic Analysis: Analysis performed on local Sandbox environment.

The analysis approach involved dynamic analysis, where the code or application was executed within a controlled environment to observe its behavior in real-time. This allowed for the monitoring of its execution, inputs, outputs, and interactions with external systems, facilitating the identification of vulnerabilities, issues, or any unexpected behaviors. The analysis process followed the same steps in both sandbox environments, yielding similar results. Therefore, the findings presented in the paper focus on the results obtained from a single environment, with any disparities between the two environments emphasized and addressed accordingly. The analysis was performed as below:

On Windows PC prior to executing the sample, Process Hacker, the Noriben script, and Procmon were used to observe and record the actions of processes and objects as shown in Figure 9. This made it possible to observe the interactions and behaviour of the process in great detail, giving vital information for subsequent study.


Windows 11 pro - VMware Workstation
File Edit View VM Tabs Help
Windows 11 pro
Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improve
ments! https://aka.ms/PSWindows

PS C:\Users\Win\Desktop\Tools\noriben plus processMonitor\
Noriben-master> py.exe .\Noriben.py
[+] Python module "requests" not found. Internet functiona
lity is disabled.
[+] This is acceptable if you do not wish to upload data t
o VirusTotal.

--===[ Noriben v1.8.6
--===[ Brian Baskin [brian@thebaskins.com / @bbaskin]
[*] Using filter file: ProcmonConfiguration.PMC
[*] Using procmon EXE: procmon.exe
[*] Procmon session saved to: Noriben_03_Jan_23__00_49_292
490.pml
[*] Launching Procmon ...
[*] Procmon is running. Run your executable now.
[*] When runtime is complete, press CTRL+C to stop logging
```

Figure 9. Process Hacker & Process Monitor with Noriben script on Windows 11

On the Linux machine, the simulation tools, namely the Inet simulator and FakeDNS, were activated to create simulated Internet services and manipulate DNS responses, respectively. Additionally, Wireshark was utilized to capture and analyze the communication packets exchanged between the machines, replicating real-world Internet communication scenarios.

After initiating the execution of the sample ransomware executable file, several noteworthy activities were observed which are discussed below. A study very well describes some of such activities as the red flags reflecting the occurrence of ransomware attacks [11].

3.2.1 Malware behavior - Stop active services

One such behavior was the ransomware's attempt to halt and remove various active services. This action was likely performed to prevent any interruptions or potential corruption of open files during the encryption process, while also ensuring persistence within the compromised system. The following services were specifically targeted for termination and deletion as shown in Table 4.

Table 4 List of services stopped or deleted

No.	Service	Status
1.	Windows Security center	Stopped
2.	Vmvss (VMware Snapshot Provider)	Deleted
3.	VSS (Volume Shadow Copy)	Deleted
4.	Vmicvss (Hyper-V volume shadow copy requester)	Deleted
5.	WdBoot (Microsoft Defender Antivirus Boot Defender)	Deleted
6.	WdNisSvc (Microsoft Defender Antivirus Network Inspection Service)	Deleted
7.	EventLog (Windows Event Log)	Deleted

3.2.2 Dropped another executable

Following the initial execution, the analyzed ransomware sample proceeded to drop an additional executable file in the directory path "C:\Users\Win\AppData\Local\Temp\" and the specific filename of the dropped executable was identified as:

- c690148b6baec765c65fe91ea9f282d6a411ae90c08d74d600515b3e075e21b2.exe

3.2.3 Dropping .tmp file and DLLs used.

Furthermore, during its execution, the ransomware dropped a temporary file named "4EFC.tmp" under the directory path "C:\ProgramData\". Additionally, it utilized multiple DLL files for its operations under file path “C:\windows\system32\”, as listed in Table 5.

Table 5 DLLs used

No.	DLL	No.	DLL
1.	ntdll.dll	2.	msctf.dll
3.	kernel32.dll	4.	shell32.dll
5.	kernelbase.dll	6.	shlwapi.dll
7.	user32.dll	8.	advapi32.dll
9.	gdi32.dll	10.	sechost.dll
11.	lpk.dll	12.	rpcrt4.dll
13.	usp10.dll	14.	rstrtmgr.dll
15.	msvcrt.dll	16.	bcrypt.dll
17.	imm32.dll	18.	ncrypt.dll
19.	msasn1.dll	20.	ole32.dll
21.	oleaut32.dll		

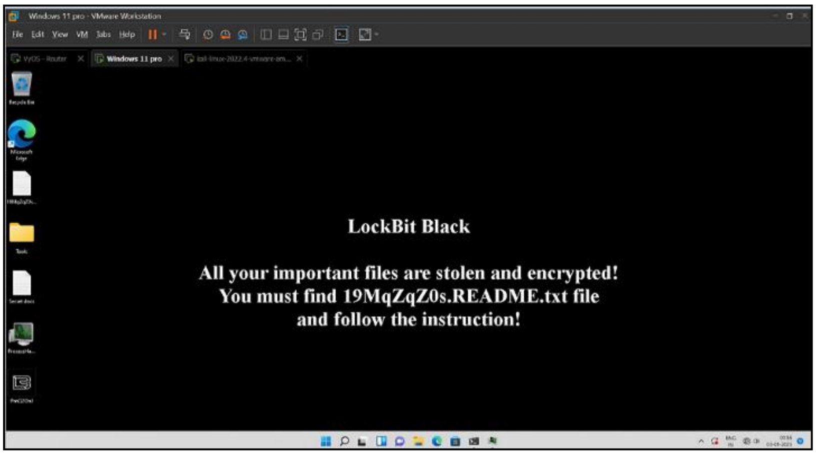
3.2.4 Ransom note:

As part of its encryption process, the ransomware targeted and encrypted all the files present on the system. It then proceeded to create a text file in each affected location, which contained the ransom note. The ransom note included several URLs, predominantly consisting of onion links that can only be accessed using specialized browsers like TOR. These URLs were provided as a means for the victims to communicate with the attackers and potentially make ransom payments or obtain further instructions. The list of URLs is shown in Table 6. A study specifically highlights the significance of ransom notes in the context of ransomware attacks [12].

Table 6 URLs related to ransomware

No.	URL
	TOR browser links
1.	http://LockBitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
2.	http://LockBitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
3.	http://LockBitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
4.	http://LockBitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
5.	http://LockBitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
6.	http://LockBitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
7.	http://LockBitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
8.	http://LockBitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
9.	http://LockBitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion
	Normal Browser links
10.	http://LockBitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
11.	http://LockBitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
12.	http://LockBitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
13.	http://LockBitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
14.	http://LockBitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
15.	http://LockBitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
16.	http://LockBitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
17.	http://LockBitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
18.	http://LockBitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly
	TOR browser links for chat
19.	http://LockBitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd.onion
20.	http://LockBitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd.onion
21.	http://LockBitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd.onion
22.	http://LockBitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad.onion
23.	http://LockBitsupq3g62dni2f36snrdb4n5qzqvovbtkt5xffw3draxk6gwqd.onion
24.	http://LockBitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd.onion
25.	http://LockBitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd.onion
26.	http://LockBitsupuhswh4izvoucoxsbnotkmgq6durg7kficg6u33zfvq3oyd.onion
27.	http://LockBitsupxcjntihbmat4rrh7ktowips2qzywh6zer5r3xafhviyhqd.onion

Additionally, the ransomware modified the desktop wallpaper, replacing it with a notification informing the user that their machine has been infected by LockBit Black. The wallpaper instructed the user to refer to the ransom note for further instructions. As part of the encryption process, all user files were encrypted, and their icons were changed to a distinct black-colored symbol in the shape of the letter "B". Figure 10 illustrates this altered look.

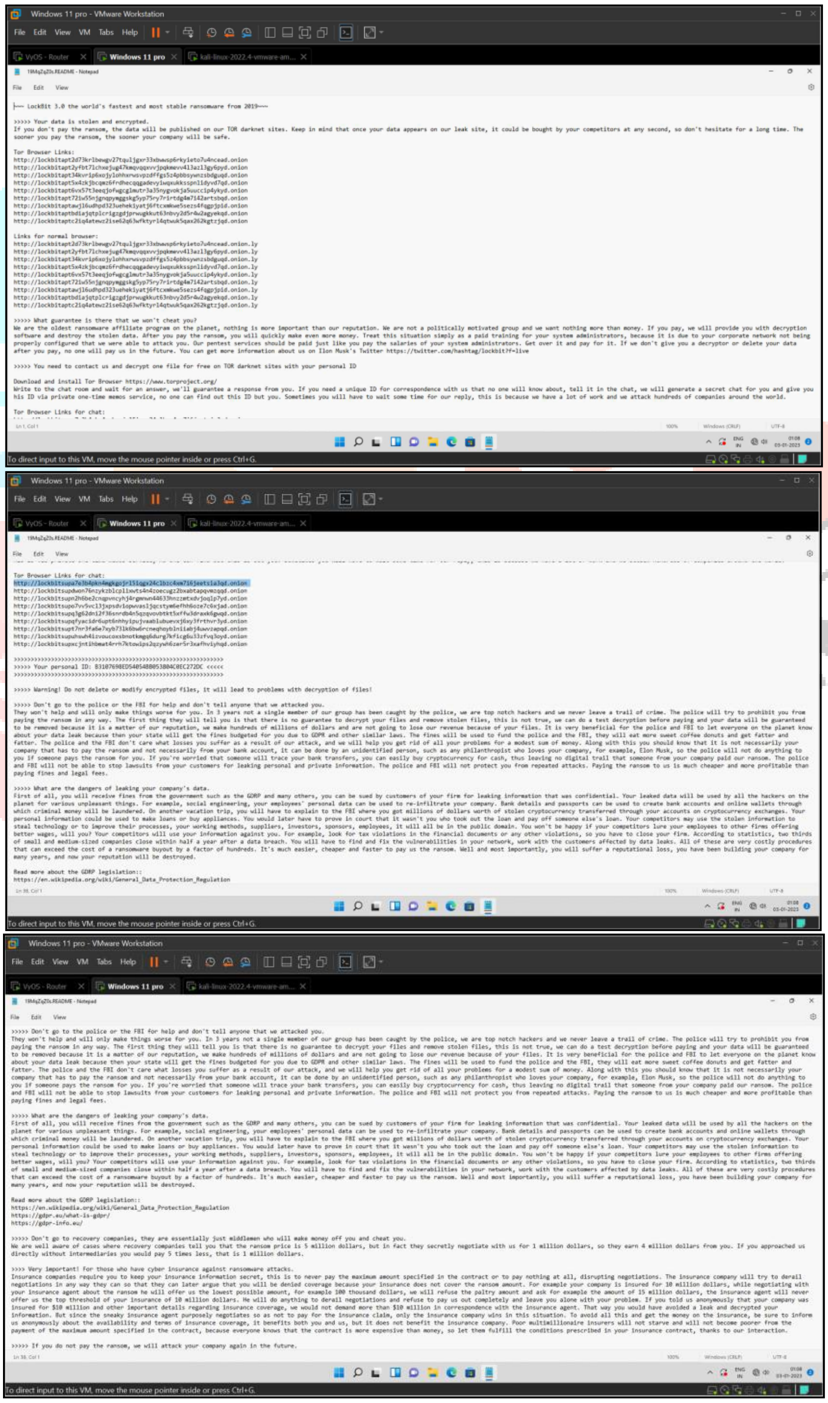

Windows 11 pro - VMware Workstation
File Edit View VM Tabs Help
VyOS - Router
Windows 11 pro
kali-linux-2022.4-vmware-am...

LockBit Black

All your important files are stolen and encrypted!
You must find 19MqZqZ0s.README.txt file
and follow the instruction!

Figure 10. Windows infected by LockBit Black

Figure 11 showcases excerpts of the ransom note displayed by the ransomware.


Windows 11 pro - VMware Workstation
File Edit View VM Tabs Help
VyOS - Router
Windows 11 pro
kali-linux-2022.4-vmware-am...
19MqZqZ0s.README - Notepad
File Edit View
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

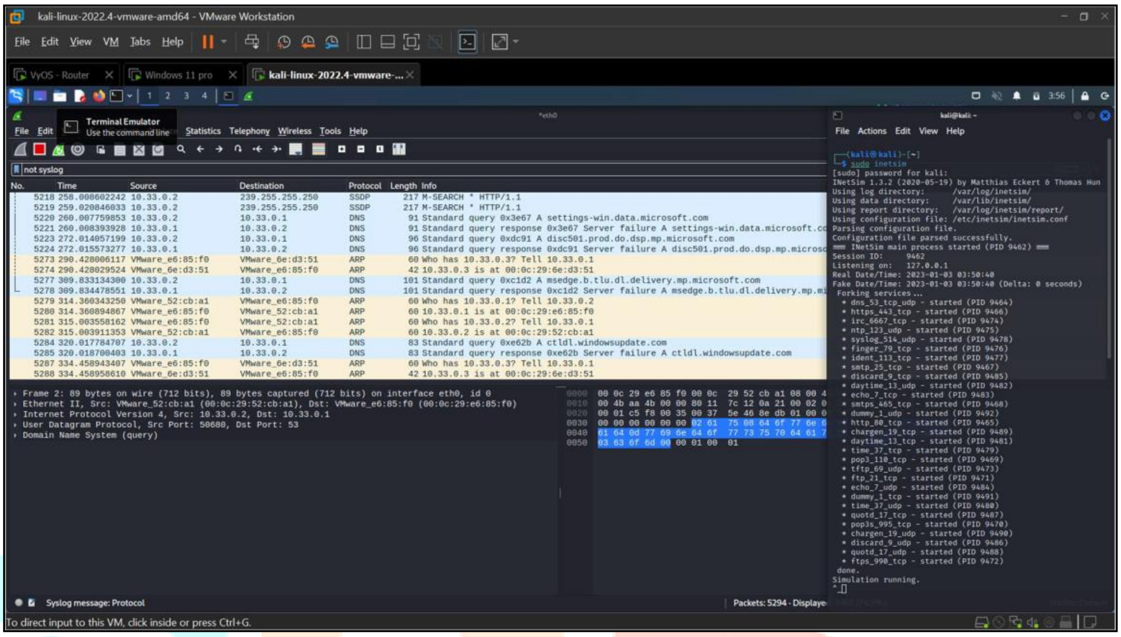
```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The
sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you with decryption
software and destroy the stolen data. After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being
properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data
after you pay, no one will pay us in the future. You can get more information about us on Ilon Musk's Twitter https://twitter.com/hashtag/lockbit?f=live

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID

Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that no one will know about, tell it in the chat, we will generate a secret chat for you and give you
his ID via private one-time memos service, no one can find out this ID but you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of companies around the world.

Tor Browser Links for chat:
http://lockbitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd.onion
http://lockbitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd.onion
http://lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd.onion
http://lockbitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad.onion
http://lockbitsupq3g62dni2f36snrdb4n5qzqvovbtkt5xffw3draxk6gwqd.onion
http://lockbitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd.onion
http://lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd.onion
http://lockbitsupuhswh4izvoucoxsbnotkmgq6durg7kficg6u33zfvq3oyd.onion
http://lockbitsupxcjntihbmat4rrh7ktowips2qzywh6zer5r3xafhviyhqd.onion

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>> Your personal ID: B3107698ED54054BB053B04C0EC272DC <<<<<
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

>>>>> Warning! Do not delete or modify encrypted files, it will lead to problems with decryption of files!

>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.
They won't help and will only make things worse for you. In 3 years not a single member of our group has been caught by the police, we are top notch hackers and we never leave a trail of crime. The police will try to prohibit you from
paying the ransom in any way. The first thing they will tell you is that there is no guarantee to decrypt your files and remove stolen files, this is not true, we can do a test decryption before paying and your data will be guaranteed
to be removed because it is a matter of our reputation, we make hundreds of millions of dollars and are not going to lose our revenue because of your files. It is very beneficial for the police and FBI to let everyone on the planet know
about your data leak because then your state will get the fines budgeted for you due to GDPR and other similar laws. The fines will be used to fund the police and the FBI, they will eat more sweet coffee donuts and get fatter and
fatter. The police and the FBI don't care what losses you suffer as a result of our attack, and we will help you get rid of all your problems for a modest sum of money. Along with this you should know that it is not necessarily your
company that has to pay the ransom and not necessarily from your bank account, it can be done by an unidentified person, such as any philanthropist who loves your company, for example, Elon Musk, so the police will not do anything to
you if someone pays the ransom for you. If you're worried that someone will trace your bank transfers, you can easily buy cryptocurrency for cash, thus leaving no digital trail that someone from your company paid our ransom. The police
and FBI will not be able to stop lawsuits from your customers for leaking personal and private information. The police and FBI will not protect you from repeated attacks. Paying the ransom to us is much cheaper and more profitable than
paying fines and legal fees.

>>>>> What are the dangers of leaking your company's data.
First of all, you will receive fines from the government such as the GDRP and many others, you can be sued by customers of your firm for leaking information that was confidential. Your leaked data will be used by all the hackers on the
planet for various unpleasant things. For example, social engineering, your employees' personal data can be used to re-infiltrate your company. Bank details and passports can be used to create bank accounts and online wallets through
which criminal money will be laundered. On another vacation trip, you will have to explain to the FBI where you got millions of dollars worth of stolen cryptocurrency transferred through your accounts on cryptocurrency exchanges. Your
personal information could be used to make loans or buy appliances. You would later have to prove in court that it wasn't you who took out the loan and pay off someone else's loan. Your competitors may use the stolen information to
steal technology or to improve their processes, your working methods, suppliers, investors, sponsors, employees, it will all be in the public domain. You won't be happy if your competitors lure your employees to other firms offering
better wages, will you? Your competitors will use your information against you. For example, look for tax violations in the financial documents or any other violations, so you have to close your firm. According to statistics, two thirds
of small and medium-sized companies close within half a year after a data breach. You will have to find and fix the vulnerabilities in your network, work with the customers affected by data leaks. All of these are very costly procedures
that can exceed the cost of a ransomware buyout by a factor of hundreds. It's much easier, cheaper and faster to pay us the ransom. Well and most importantly, you will suffer a reputational loss, you have been building your company for
many years, and now your reputation will be destroyed.

Read more about the GDRP legislation::
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
https://gdpr.eu/what-is-gdpr/
https://gdpr-info.eu/

>>>>> Don't go to recovery companies, they are essentially just middlemen who will make money off you and cheat you.
We are well aware of cases where recovery companies tell you that the ransom price is 5 million dollars, but in fact they secretly negotiate with us for 1 million dollars, so they earn 4 million dollars from you. If you approached us
directly without intermediaries you would pay 5 times less, that is 1 million dollars.

>>>> Very important! For those who have cyber insurance against ransomware attacks.
Insurance companies require you to keep your insurance information secret, this is to never pay the maximum amount specified in the contract or to pay nothing at all, disrupting negotiations. The insurance company will try to derail
negotiations in any way they can so that they can later argue that you will be denied coverage because your insurance does not cover the ransom amount. For example your company is insured for 10 million dollars, while negotiating with
your insurance agent about the ransom he will offer us the lowest possible amount, for example 100 thousand dollars, we will refuse the paltry amount and ask for example the amount of 15 million dollars, the insurance agent will never
offer us the top threshold of your insurance of 10 million dollars. He will do anything to derail negotiations and refuse to pay us out completely and leave you alone with your problem. If you told us anonymously that your company was
insured for $10 million and other important details regarding insurance coverage, we would not demand more than $10 million in correspondence with the insurance agent. That way you would have avoided a leak and decrypted your
information. But since the sneaky insurance agent purposely negotiates so as not to pay for the insurance claim, only the insurance company wins in this situation. To avoid all this and get the money on the insurance, be sure to inform
us anonymously about the availability and terms of insurance coverage, it benefits both you and us, but it does not benefit the insurance company. Poor multimillionaire insurers will not starve and will not become poorer from the
payment of the maximum amount specified in the contract, because everyone knows that the contract is more expensive than money, so let them fulfill the conditions prescribed in your insurance contract, thanks to our interaction.

>>>>> If you do not pay the ransom, we will attack your company again in the future.
```

Figure 11. Ransome Notes

3.2.5 Wireshark captured packets

With its ability to collect and analyse network traffic in real-time while also assisting in the discovery of suspicious patterns, peculiar behavior, and communication with hostile entities, Wireshark is a potent network protocol analyzer that is essential in the detection of ransomware. A study demonstrates the use of Wireshark in the detection and analysis of Loocipher ransomware [13].

Upon capturing and analyzing packets using Wireshark during the infection phase, no instances of malicious network communication were identified as shown in Figure 12. The captured packets were thoroughly examined, and their contents were compared with pcap files obtained from different online malware analyzer platforms. This comprehensive analysis confirmed that there was no evidence of any malicious communication occurring during the infection phase of the ransomware.


kali-linux-2022.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
VyOS - Router
Windows 11 pro
kali-linux-2022.4-vmware-...
1 2 3 4
3:56
Terminal Emulator
Use the command line
File Edit Statistics Telephony Wireless Tools Help
*eth0
kali@kali: ~
File Actions Edit View Help

not syslog

```
No.   Time           Source            Destination       Protocol Length Info
 5218 258.008602242 10.33.0.2         239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
 5219 259.020846033 10.33.0.2         239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
 5220 260.007759853 10.33.0.2         10.33.0.1         DNS       91 Standard query 0x3e67 A settings-win.data.microsoft.com
 5221 260.008393928 10.33.0.1         10.33.0.2         DNS       91 Standard query response 0x3e67 Server failure A settings-win.data.microsoft.co
 5223 272.014057199 10.33.0.2         10.33.0.1         DNS       96 Standard query 0xdc91 A disc501.prod.do.dsp.mp.microsoft.com
 5224 272.015573277 10.33.0.1         10.33.0.2         DNS       96 Standard query response 0xdc91 Server failure A disc501.prod.do.dsp.mp.microso
 5273 290.428006117 VMware_e6:85:f0   VMware_6e:d3:51   ARP       60 Who has 10.33.0.3? Tell 10.33.0.1
 5274 290.428029524 VMware_6e:d3:51   VMware_e6:85:f0   ARP       42 10.33.0.3 is at 00:0c:29:6e:d3:51
 5277 309.833134300 10.33.0.2         10.33.0.1         DNS      101 Standard query 0xc1d2 A msedge.b.tlu.dl.delivery.mp.microsoft.com
 5278 309.834478551 10.33.0.1         10.33.0.2         DNS      101 Standard query response 0xc1d2 Server failure A msedge.b.tlu.dl.delivery.mp.mi
 5279 314.360343250 VMware_52:cb:a1   VMware_e6:85:f0   ARP       60 Who has 10.33.0.1? Tell 10.33.0.2
 5280 314.360894867 VMware_e6:85:f0   VMware_52:cb:a1   ARP       60 10.33.0.1 is at 00:0c:29:e6:85:f0
 5281 315.003558162 VMware_e6:85:f0   VMware_52:cb:a1   ARP       60 Who has 10.33.0.2? Tell 10.33.0.1
 5282 315.003911353 VMware_52:cb:a1   VMware_e6:85:f0   ARP       60 10.33.0.2 is at 00:0c:29:52:cb:a1
 5284 320.017784707 10.33.0.2         10.33.0.1         DNS       83 Standard query 0xe62b A ctldl.windowsupdate.com
 5285 320.018700403 10.33.0.1         10.33.0.2         DNS       83 Standard query response 0xe62b Server failure A ctldl.windowsupdate.com
 5287 334.458943407 VMware_e6:85:f0   VMware_6e:d3:51   ARP       60 Who has 10.33.0.3? Tell 10.33.0.1
 5288 334.458958610 VMware_6e:d3:51   VMware_e6:85:f0   ARP       42 10.33.0.3 is at 00:0c:29:6e:d3:51
```

```
› Frame 2: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_52:cb:a1 (00:0c:29:52:cb:a1), Dst: VMware_e6:85:f0 (00:0c:29:e6:85:f0)
› Internet Protocol Version 4, Src: 10.33.0.2, Dst: 10.33.0.1
› User Datagram Protocol, Src Port: 50680, Dst Port: 53
› Domain Name System (query)
```

```
0000  00 0c 29 e6 85 f0 00 0c  29 52 cb a1 08 00 4
0010  00 4b aa 4b 00 00 80 11  7c 12 0a 21 00 02 0
0020  00 01 c5 f8 00 35 00 37  5e 46 8e db 01 00 0
0030  00 00 00 00 00 00 02 61  75 08 64 6f 77 6e 6
0040  61 64 0d 77 69 6e 64 6f  77 73 75 70 64 61 7
0050  03 63 6f 6d 00 00 01 00  01
```

```
┌──(kali㉿kali)-[~]
└─$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hun
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 9462) ===
Session ID:     9462
Listening on:   127.0.0.1
Real Date/Time: 2023-01-03 03:50:40
Fake Date/Time: 2023-01-03 03:50:40 (Delta: 0 seconds)
 Forking services ...
  * dns_53_tcp_udp - started (PID 9464)
  * https_443_tcp - started (PID 9466)
  * irc_6667_tcp - started (PID 9474)
  * ntp_123_udp - started (PID 9475)
  * syslog_514_udp - started (PID 9478)
  * finger_79_tcp - started (PID 9476)
  * ident_113_tcp - started (PID 9477)
  * smtp_25_tcp - started (PID 9467)
  * discard_9_tcp - started (PID 9485)
  * daytime_13_udp - started (PID 9482)
  * echo_7_tcp - started (PID 9483)
  * smtps_465_tcp - started (PID 9468)
  * dummy_1_udp - started (PID 9492)
  * http_80_tcp - started (PID 9465)
  * chargen_19_tcp - started (PID 9489)
  * daytime_13_tcp - started (PID 9481)
  * time_37_tcp - started (PID 9479)
  * pop3_110_tcp - started (PID 9469)
  * tftp_69_udp - started (PID 9473)
  * ftp_21_tcp - started (PID 9471)
  * echo_7_udp - started (PID 9484)
  * dummy_1_tcp - started (PID 9491)
  * time_37_udp - started (PID 9480)
  * quotd_17_tcp - started (PID 9487)
  * pop3s_995_tcp - started (PID 9470)
  * chargen_19_udp - started (PID 9490)
  * discard_9_udp - started (PID 9486)
  * quotd_17_udp - started (PID 9488)
  * ftps_990_tcp - started (PID 9472)
 done.
Simulation running.
^
```

Syslog message: Protocol

Packets: 5294 · Displaye

To direct input to this VM, click inside or press Ctrl+G.

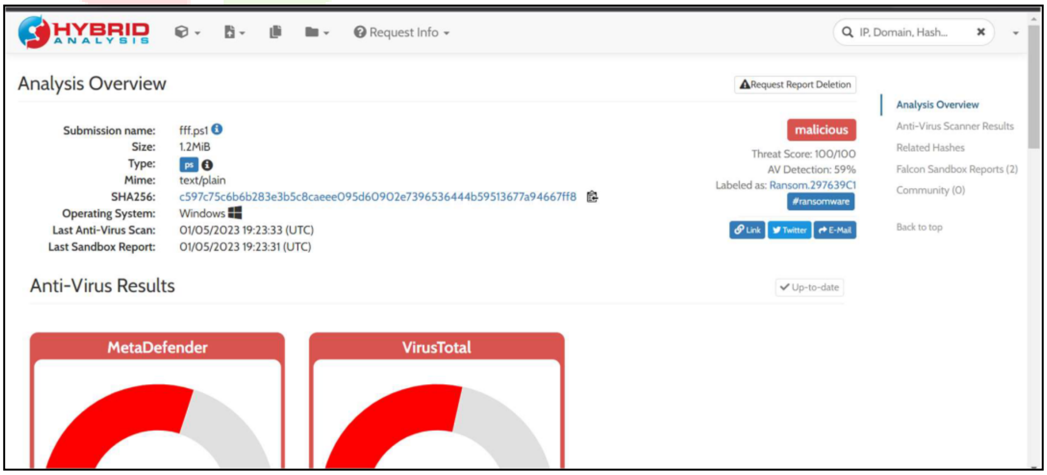
Figure 12. Wireshark captured packets

3.3 Analysis performed on the Online platforms:

In addition to the analysis conducted in the created sandbox environments, the ransomware samples were also subjected to analysis on various online platforms for further comparison. Several online analysis platforms, which offer free analysis services, were utilized to analyze the ransomware samples. A study describes many such online platforms like JoeSandbox, Hybrid Analysis, Any.run among others that can be used for automated malware analysis [14]. The following platforms were used, and their specific results can be accessed using the provided links:

3.3.1 Hybrid Analysis

Hybrid Analysis is an online malware analysis platform that combines both static and dynamic analysis techniques allowing users to submit suspicious files and URLs for analysis, providing detailed reports on the behavior, indicators of compromise (IOCs), and potential threats associated with the analyzed sample. The analysis report can be checked on its website via the link https://www.hybridanalysis.com/sample/c597c75c6b6b283e3b5c8caeee095d60902e7396536444b59513677a9 4667ff8. The snap of the analysis is shown in Figure 13.



Analysis Overview

Submission name: fff.ps1
Size: 1.2MiB
Type: ps
Mime: text/plain
SHA256: c597c75c6b6b283e3b5c8caeee095d60902e7396536444b59513677a94667ff8
Operating System: Windows
Last Anti-Virus Scan: 01/05/2023 19:23:33 (UTC)
Last Sandbox Report: 01/05/2023 19:23:31 (UTC)

malicious

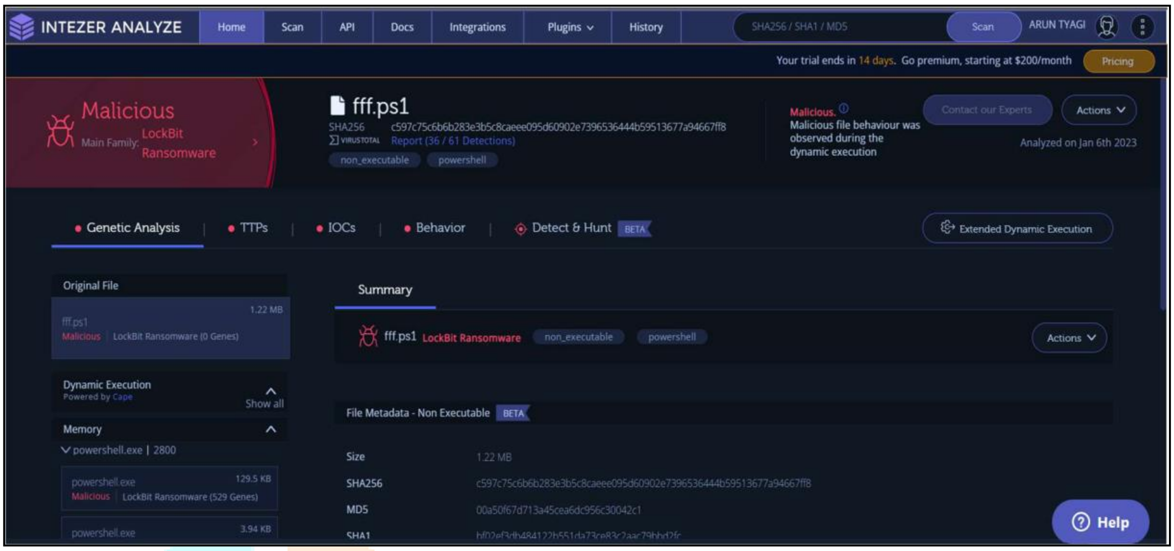
Threat Score: 100/100
AV Detection: 59%
Labeled as: Ransom.297639C1
#ransomware

Anti-Virus Results

Figure 13. Hybrid Analysis

3.3.2 Intezer Analyze:

Intezer Analyze is a platform that leverages genetic malware analysis to identify and classify new and known malware strains. It can detect code reuse and provide insights into the relationships between different malware families by comparing the code similarities. A paper gives a comparative analysis of Intezer with other automated malware analysis tools [15]. The analysis report can be checked on its website by the link https://analyze.intezer.com/analyses/232d5086-7442-4bc5-86d0-a84cf5744221/geneticanalysis. snap of the analysis is shown in Figure 14.



Your trial ends in 14 days. Go premium, starting at $200/month

Malicious
Main Family: LockBit Ransomware

fff.ps1
SHA256 c597c75c6b6b283e3b5c8caeee095d60902e7396536444b59513677a94667ff8
VIRUSTOTAL Report (36 / 61 Detections)
non_executable powershell

Malicious. Malicious file behaviour was observed during the dynamic execution

Analyzed on Jan 6th 2023

Original File
fff.ps1 1.22 MB
Malicious | LockBit Ransomware (0 Genes)

Dynamic Execution
Powered by Cape
Show all

Memory
powershell.exe | 2800
powershell.exe 129.5 KB
Malicious | LockBit Ransomware (529 Genes)
powershell.exe 3.94 KB

fff.ps1 LockBit Ransomware non_executable powershell

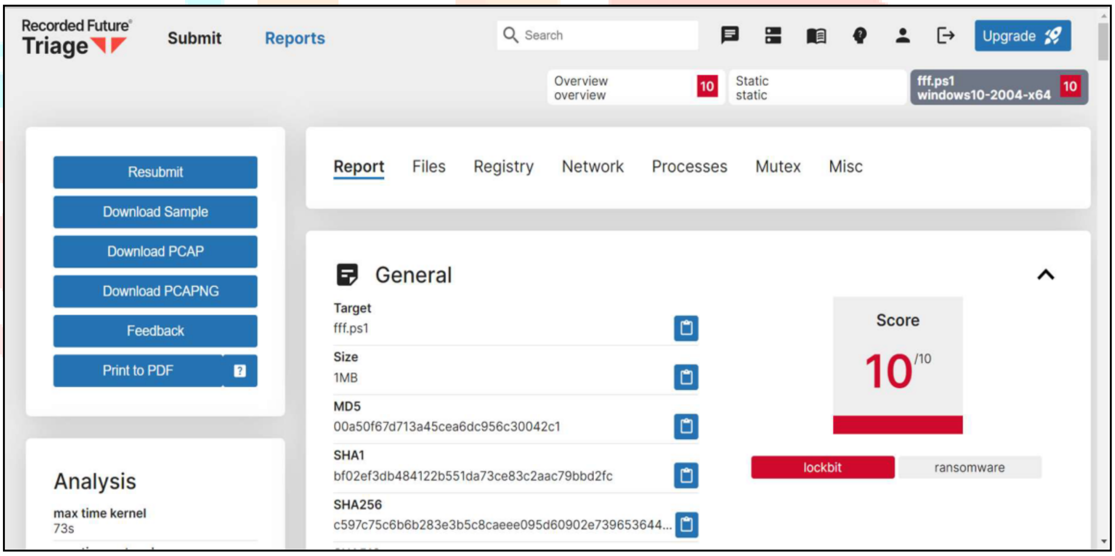
File Metadata - Non Executable BETA

Size 1.22 MB
SHA256 c597c75c6b6b283e3b5c8caeee095d60902e7396536444b59513677a94667ff8
MD5 00a50f67d713a45cea6dc956c30042c1
SHA1 bf02ef3db484122b551da73ce83c2aac79bbd2fc

Figure 14. Intezer Analyze

3.3.3 Triage:

As its name goes it refers to analyzing and prioritizing malware samples based on their potential impact, severity, or relevance helping security analysts focus on high-priority cases first and allocate resources effectively. The analysis details can be found at the URL https://tria.ge/230105-xtl5hsch82/behavioral1#report as show in Figure 15.



Overview overview 10
Static static
fff.ps1 windows10-2004-x64 10

General

Target
fff.ps1

Size
1MB

MD5
00a50f67d713a45cea6dc956c30042c1

SHA1
bf02ef3db484122b551da73ce83c2aac79bbd2fc

SHA256
c597c75c6b6b283e3b5c8caeee095d60902e739653644...

Score
10/10

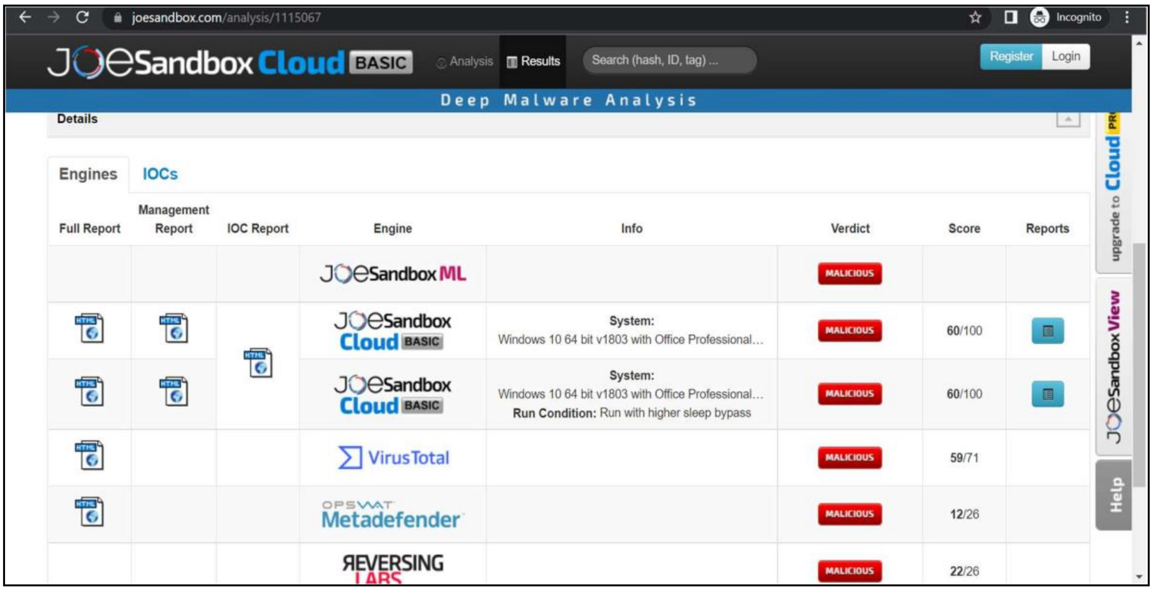
lockbit ransomware

Analysis
max time kernel
73s

Figure 15. Triage

3.3.4 JoeSandBox:

Joe Sandbox is an advanced malware analysis system that provides dynamic analysis capabilities allowing users to run suspicious files or URLs in a controlled environment to monitors their behavior, network communications, and system changes in order to detect malicious activities. It also provides detailed reports. The analysis details can be found at https://www.joesandbox.com/analysis/1115067 as shown in Figure 16.



joesandbox.com/analysis/1115067

JoeSandbox Cloud BASIC — Analysis · Results · Search (hash, ID, tag) ... · Register · Login

Deep Malware Analysis

Details

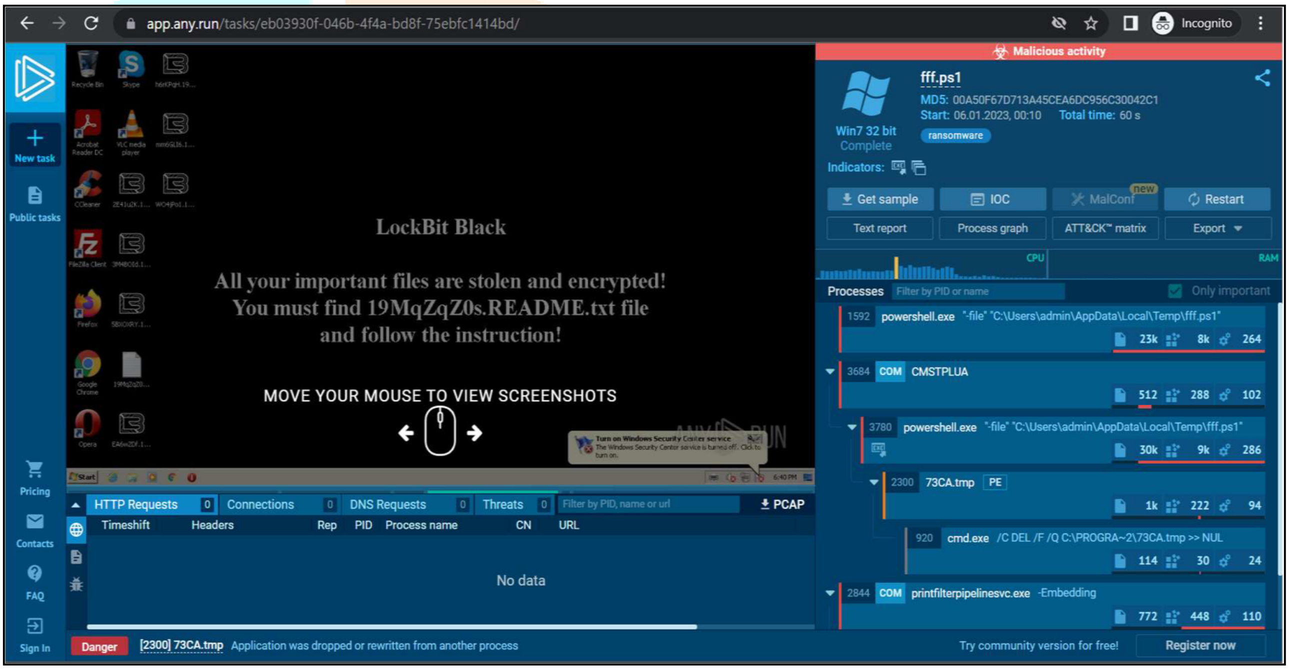
Engines · IOCs

Full Report	Management Report	IOC Report	Engine	Info	Verdict	Score	Reports
			JoeSandbox ML		MALICIOUS		
HTML	HTML	HTML	JoeSandbox Cloud BASIC	System: Windows 10 64 bit v1803 with Office Professional...	MALICIOUS	60/100	▦
HTML	HTML		JoeSandbox Cloud BASIC	System: Windows 10 64 bit v1803 with Office Professional... Run Condition: Run with higher sleep bypass	MALICIOUS	60/100	▦
HTML			VirusTotal		MALICIOUS	59/71	
HTML			OPSWAT Metadefender		MALICIOUS	12/26	
			REVERSING LABS		MALICIOUS	22/26	

Figure 16. JoeSandBox

3.3.5 Any Run:

As shown in Figure 17 Any.Run is an interactive malware analysis platform that enables users to execute and monitor files in a secure sandbox environment and it also provides real-time visibility into the behavior and actions of malware. The complete analysis details and reports can be found at https://app.any.run/tasks/eb03930f046b-4f4a-bd8f-75ebfc1414bd. And the sample can also be downloaded from the same URL.



app.any.run/tasks/eb03930f-046b-4f4a-bd8f-75ebfc1414bd/

LockBit Black

All your important files are stolen and encrypted!
You must find 19MqZqZ0s.README.txt file
and follow the instruction!

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

Turn on Windows Security Center service
The Windows Security Center service is turned off. Click to turn on.

HTTP Requests 0	Connections 0	DNS Requests 0	Threats 0

Timeshift	Headers	Rep	PID	Process name	CN	URL

No data

Danger [2300] 73CA.tmp Application was dropped or rewritten from another process

Malicious activity

fff.ps1
MD5: 00A50F67D713A45CEA6DC956C30042C1
Start: 06.01.2023, 00:10 Total time: 60 s
ransomware
Win7 32 bit
Complete
Indicators:

Processes

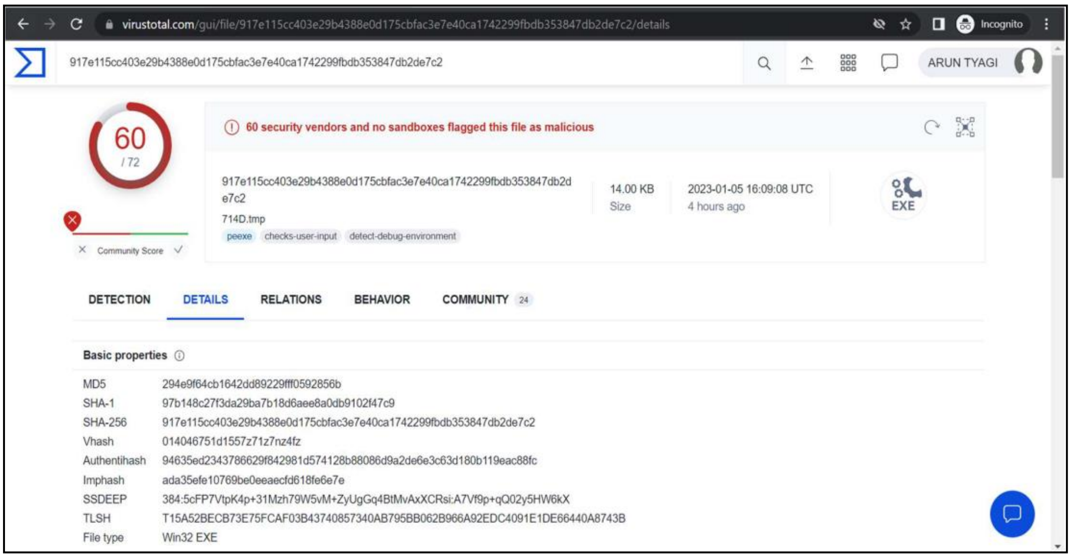
```
1592 powershell.exe "-file" "C:\Users\admin\AppData\Local\Temp\fff.ps1"      23k  8k  264
3684 COM CMSTPLUA                                                            512  288  102
  3780 powershell.exe "-file" "C:\Users\admin\AppData\Local\Temp\fff.ps1"    30k  9k  286
    2300 73CA.tmp PE                                                         1k  222  94
      920 cmd.exe /C DEL /F /Q C:\PROGRA~2\73CA.tmp >> NUL                   114  30  24
2844 COM printfilterpipelinesvc.exe -Embedding                               772  448  110
```

Try community version for free! Register now

Figure 17. Any Run

3.3.6 Virustotal:

One of the mandatory step in analyzing any malware is to scan it on various antivirus engines. VirusTotal is a widely-known online service that provides a platform for analyzing suspicious files and URLs. VirusTotal aggregates multiple antivirus engines and other analysis tools to scan and detect potential malware and is also extensively used in study [16]. The results can be seen at https://www.virustotal.com/gui/file/917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2/details as shown in Figure 18.


virustotal.com/gui/file/917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2/details
Incognito
917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
ARUN TYAGI
60
/ 72
Community Score
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 24

60 security vendors and no sandboxes flagged this file as malicious

917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
714D.tmp
peexe checks-user-input detect-debug-environment

14.00 KB
Size

2023-01-05 16:09:08 UTC
4 hours ago

Basic properties

MD5	294e9f64cb1642dd89229fff0592856b
SHA-1	97b148c27f3da29ba7b18d6aee8a0db9102f47c9
SHA-256	917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
Vhash	014046751d1557z71z7nz4fz
Authentihash	94635ed2343786629f842981d574128b88086d9a2de6e3c63d180b119eac88fc
Imphash	ada35efe10769be0eeaecfd618fe6e7e
SSDEEP	384:5cFP7VtpK4p+31Mzh79W5vM+ZyUgGq4BtMvAxXCRsi:A7Vf9p+qQ02y5HW6kX
TLSH	T15A52BECB73E75FCAF03B43740857340AB795BB062B966A92EDC4091E1DE66440A8743B
File type	Win32 EXE

Figure 18. VirusTotal

Furthermore, the comprehensive analysis yielded a collection of Indicators of Compromise (IoCs) that emerged from the aggregated results. These IoCs should also be taken into consideration when creating rules or signatures for diverse detection platforms, including antivirus software, intrusion detection systems (IDS), intrusion prevention systems (IPS), security information and event management (SIEM) systems, and others. The IoCs are listed in Table 7 & Table 8.

Table 7 Identified IOC -1

IoC Head	**Results**
File Name	c690148b6baec765c65fe91ea9f282d6a411ae90c08d74d600515b3e075e21b2.exe
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	a8e0d56f8c67f1f7b6e592c12d87acab
SHA 1	ed555f0162ea6ec5b8b8bada743cfc628d376274
SHA 256	c690148b6baec765c65fe91ea9f282d6a411ae90c08d74d600515b3e075e21b2
SHA 384	4c1eb3948df7b359851c491b8f268ddd7c18c605d1a2531342488b781e04239f8631d1081ff7ecc0261eda819aa38c32
TLSH	T1A3F38E22A111D077F4271DF12B3672B1B3EB8E2C15A7A417EAE40F58ACA7D632F14517
Ssdeep	3072:wrQnZg2Bvu2K8/PzRanIzrQSsKQj+zXzCGRG2:wrf2Bm3cLRanKr5zRG
Imphash	8365ac85490d89776a96737b801cde2b

Table 8 Identified IOC -2

IoC Head	**Results**
File Name	Powershell: fff.ps1 Dropped file: AE08.exe
MD5	00A50F67D713A45CEA6DC956C30042C1
SHA 1	BF02EF3DB484122B551DA73CE83C2AAC79BBD2FC
SHA 256	PS file: C597C75C6B6B283E3B5C8CAEEE095D60902E7396536444B59513677A94667FF8 Dropped file: 917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
Ssdeep	PS file: 12288:SVv5LDfyZi0CT/KWqZecjqM0aUnbqvmwn+bPQhZUYk7eua4lvp:SVhLt/5cjqM0aUnbqvmwwPpYkx Dropped file: 384:5cFP7VtpK4p+31Mzh79W5vM+ZyUgGq4BtMvAxXCRsi:A7Vf9p+qQ02y5HW6kX

IV. Conclusion

As a self-piloted cyberattack, LockBit ransomware poses critical issues to organizations globally by threatening to disrupt their operations with essential functions coming to a sudden halt, using extortion for the hacker's financial gain, and blackmailing victims for data theft and illegal publication on noncompliance to their demands. To proactively identify and mitigate the lockbit ransomware infection, it is crucial to leverage the findings & IoCs presented in section 3 for the development of effective rules or signatures. Researchers working to create such rules or signatures for efficient malware detection, identification, and contamination prevention can benefit greatly from these findings. By leveraging these findings, researchers can enhance the capabilities of detection systems, including antivirus software, intrusion detection & prevention systems (IDPS), and other security solutions.

V. ACKNOWLEDGMENT

Thanks to the Rashtra Raksha University for the support and facilitation of this research. I would like to express my deepest gratitude to my supervisor Mr. Vivek Joshi, for his invaluable guidance, support, and encouragement throughout my research.

REFERENCES

[1] A. K. Maurya, N. Kumar, A. Agrawal, and R. A. Khan, “Ransomware Evolution, Target and Safety Measures,” International Journal of Computer Sciences and Engineering, vol. 6, no. 1, pp. 80–85, Jan. 2018, doi: 10.26438/ijcse/v6i1.8085.

[2] I. Kara, “Read the digital fingerprints: log analysis for digital forensics and security,” Computer Fraud and Security, vol. 2021, no. 7, pp. 11–16, Jul. 2021, doi: 10.1016/S1361-3723(21)00074-9.

[3] S. Biswas, “Forensic Analysis of Ransomware Infected Windows Hard Disk: A Case Study,” 2022. [Online]. Available: www.ijisrt.com206

[4] Monnappa. K. A, Learning Malware Analysis : Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware. Packt Publishing Ltd, 2018.

[5] A. O. Almashhadani, M. Kaiiali, S. Sezer, and P. O’Kane, “A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware,” IEEE Access, vol. 7, pp. 47053–47067, 2019, doi: 10.1109/ACCESS.2019.2907485.

[6] S. Salehi, H. Shahriari, M. M. Ahmadian, and L. Tazik, “A Novel Approach for Detecting DGA-based Ransomwares,” in 2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), IEEE, Aug. 2018, pp. 1–7. doi: 10.1109/ISCISC.2018.8546941.

[7] S. Talukder, “Tools and Techniques for Malware Detection and Analysis,” Feb. 2020.

[8] S. Talukder and Z. Talukder, “A Survey on Malware Detection and Analysis Tools,” International Journal of Network Security & Its Applications, vol. 12, no. 2, pp. 37–57, Mar. 2020, doi: 10.5121/ijnsa.2020.12203.

[9] N. Naik, P. Jenkins, and N. Savage, “A Ransomware Detection Method Using Fuzzy Hashing for Mitigating the Risk of Occlusion of Information Systems,” in 2019 International Symposium on Systems Engineering (ISSE), IEEE, Oct. 2019, pp. 1–6. doi: 10.1109/ISSE46696.2019.8984540.

[10] A. Amiruddin, C. Kurniawan, E. H. Ramadhani, and J. Rinaldi, “Learning the Basic Strcuture of Several Ransomwares Using Static Analysis Tecgnique,” IOP Conf Ser Mater Sci Eng, vol. 1007, no. 1, p. 012072, Dec. 2020, doi: 10.1088/1757-899X/1007/1/012072.

[11] U. Urooj, B. A. S. Al-rimy, A. Zainal, F. A. Ghaleb, and M. A. Rassam, “Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions,” Applied Sciences, vol. 12, no. 1, p. 172, Dec. 2021, doi: 10.3390/app12010172.

[12] Y. Lemmou, J.-L. Lanet, and E. M. Souidi, “In-Depth Analysis of Ransom Note Files,” Computers, vol. 10, no. 11, p. 145, Nov. 2021, doi: 10.3390/computers10110145.

[13] T. M. Liu, D. Y. Kao, and Y. Y. Chen, “Loocipher ransomware detection using lightweight packet characteristics,” in Procedia Computer Science, Elsevier B.V., 2020, pp. 1677–1683. doi: 10.1016/j.procs.2020.09.192.

[14] D. Serpanos, P. Michalopoulos, G. Xenos, and V. Ieronymakis, “Sisyfos: A Modular and Extendable Open Malware Analysis Platform,” Applied Sciences, vol. 11, no. 7, p. 2980, Mar. 2021, doi: 10.3390/app11072980.

[15] Preeti and A. K. Agrawal, “A Comparative Analysis of Open Source Automated Malware Tools,” in 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, Mar. 2022, pp. 226–230. doi: 10.23919/INDIACom54597.2022.9763227.

[16] S. SECHEL, “A Comparative Assessment of Obfuscated Ransomware Detection Methods,” Informatica Economica, vol. 23, no. 2/2019, pp. 45–62, Jun. 2019, doi: 10.12948/issn14531305/23.2.2019.05.