

Ransomware Analysis: Rhysida, BlackCat (ALPHV & Sphynx), and LockBit (2.0 / 3.0)

Author: Victor Chinedu Ndukwe

Repository: GitHub — Research Write-up

Date: 23 October 2025

Abstract

This document summarises static and dynamic analyses of several ransomware strains—Rhysida, BlackCat (ALPHV and Sphynx), and LockBit (2.0 and 3.0)—performed on a Windows 10 client within a controlled virtual lab. The goal is to present findings useful for defenders and researchers, including indicators of compromise (IOCs), YARA markers, behaviour summaries, and detection capabilities of IDS tools (Snort, Suricata, OSSEC). Images from the original analysis (PeStudio screenshots, Process Hacker views, ransom notes, and IDS logs) are embedded throughout.

Table of Contents

1. Rhysida
2. BlackCat ALPHV
3. BlackCat Sphynx
4. LockBit 2.0
5. LockBit 3.0
6. Data collection and IDS evaluation
7. Conclusions and recommendations
8. Appendix — Figures and IOCs

1. Rhysida

Rhysida is a ransomware strain notable for high encryption speed, advanced encryption techniques, and evasion methods. It encrypts user files and demands ransom for decryption. The following summarises static and dynamic analysis findings.

1.1 Static Analysis

Entropy and file structure: PeStudio reported an entropy value of 6.645 for the Rhysida sample, indicating packing or encryption. A section flagged with a PDF signature (size ≈ 38,144 bytes) suggests the sample embeds or masquerades as a PDF, possibly as a decoy or payload carrier.

Imports and libraries: Rhysida imports `advapi32.dll`, `kernel32.dll`, `msvcrt.dll`, `user32.dll` and uses functions such as `CryptAcquireContextA`, `CryptGenRandom`, `GetCurrentProcessId`,

VirtualProtect, VirtualQuery, and AddVectoredExceptionHandler. These indicate cryptographic operations, memory manipulation, anti-debugging and process control.

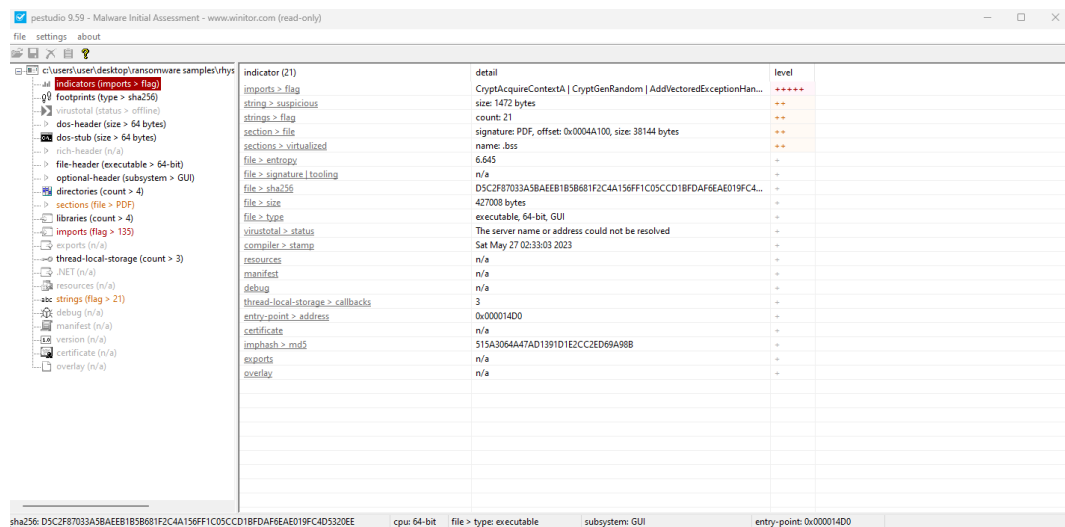


Figure: image1.png

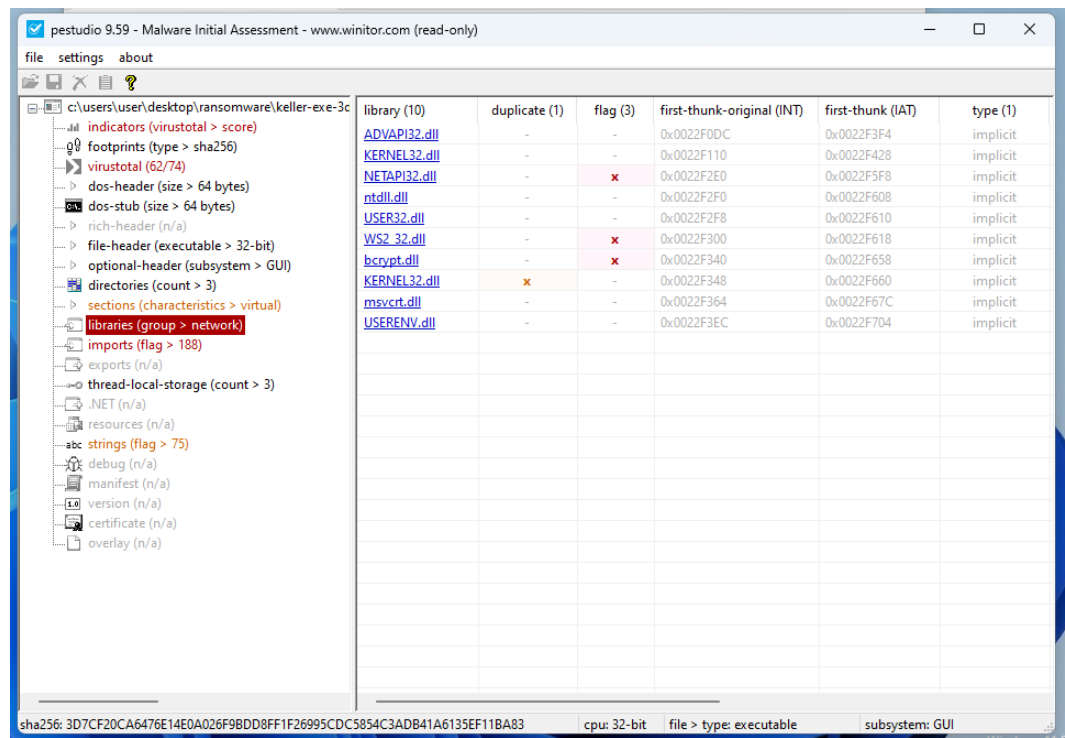


Figure: image10.png

1.2 Dynamic Analysis

Observed behaviours: using Process Hacker, VirusTotal and APIminer, Rhysida created files (notably 'criticalbreachdetected.pdf'), dropped files with a .rhysida extension, modified registry keys (including .pdf associations), and interacted with processes such as cmd.exe, sc.exe,

reg.exe, dllhost.exe and SearchIndexer. No network traffic was observed during the analysis, suggesting the sample can operate offline.

YARA markers and telemetry indicators: powershell, ThreadControl__Context, SEH__vectored, Check_OutputDebugStringA_iat, anti_dbg. Encryption methodology: ChaCha20-based CSPRNG for file encryption, intermittent 1 MB block encryption, AES-256-CTR for file content and RSA-4096 for key wrapping.

2. BlackCat (ALPHV)

BlackCat (ALPHV) is a modular, cross-platform ransomware family. Static analysis shows high entropy (≈ 6.863) and YARA matches indicating network and spreading capabilities.

2.1 Static Analysis

Key libraries: WS2_32.dll, NETAPI32.dll, bcrypt.dll, USERENV.dll, ntdll.dll, msvcrt.dll, USER32.dll, ADVAPI32.dll, KERNEL32.dll. YARA matches included network and spreading indicators, registry manipulation and mutex usage.

2.2 Dynamic Analysis

Behaviour: drops files with .sykffle extension, deletes temporary files and logs, interacts with registry keys to persist and possibly disable security features, injects into processes like wuapihost.exe and wmiprvse.exe, and drops ransom note RECOVER- $\{EXTENSION\}$ -FILES.txt. Some images of infected files and ransom notes are included.

3. BlackCat Sphynx

Sphynx is a stealthy variant of BlackCat. Static entropy observed ≈ 6.805 . The sample demonstrates anti-VM and anti-sandbox techniques and uses a broad set of Windows libraries.

3.1 Static Analysis

Notable libraries and functions: advapi32.dll (AdjustTokenPrivileges), bcrypt.dll (BCryptGenRandom), kernel32.dll (CreateProcessW, VirtualProtect), netapi32.dll (NetShareEnum), mpr.dll (WNetAddConnection2W), ole32/oleaut32, rstrtmgr.dll, secur32.dll and IPHLPAPI.DLL.

3.2 Dynamic Analysis

Behaviour: deletes WER logs, drops files in WER\Temp, modifies registry keys, creates and injects into processes such as wuapihost.exe and wmiadap.exe. API calls observed (APIminer) include NtProtectVirtualMemory, NtClose, LdrGetDllHandle. No network traffic was observed during the execution in the controlled lab.

4. LockBit 2.0

LockBit 2.0 is a fast and efficient ransomware family. Static entropy ≈ 6.781 and contains YARA rules suggesting anti-VM, privilege escalation and spreading capabilities.

4.1 Static Analysis

Key libraries: WS2_32.dll, CRYPT32.dll, gdiplus.dll, SHLWAPI.dll, MPR.dll, ntdll.dll, msvcrt.dll, KERNEL32.dll, USER32.dll, ADVAPI32.dll, SHELL32.dll, ole32.dll.

4.2 Dynamic Analysis

Behaviour: executes system commands to delete shadow copies and backups (vssadmin, wmic, bcdedit, wbadmin), encrypts files with .lockbit extension, modifies registry for persistence, creates mutexes and spawns process trees to disable recovery and cover tracks.

5. LockBit 3.0

LockBit 3.0 improves upon LockBit 2.0 with enhanced evasion techniques (HeavensGate, DebuggerHiding__Thread) and refined file-system manipulation. Entropy ≈ 6.877 .

5.1 Static Analysis

Notable functions: MessageBoxW, LoadResource, WriteFile, CreateFileW, NtClose, RtlAllocateHeap. Uses HeavensGate technique to execute 64-bit code from 32-bit processes.

5.2 Dynamic Analysis

Behaviour: extensive file operations, registry manipulation, process injection (WMIADAP.EXE), and capability to capture screenshots and manipulate tokens for privilege escalation. Ransom note delivery and potential data exfiltration are consistent with modern ransomware tactics.

6. Data collection and IDS evaluation

Methodology: A baseline was captured, each ransomware sample was deployed to a Windows 10 client machine, IDS tools (Snort, Suricata, OSSEC) logged activity, and snapshots restored after each test.

Findings: Snort and Suricata (network-based IDS) generated no significant alerts for the samples in the isolated virtual lab. OSSEC (host-based IDS) detected registry changes, file modifications, ransom note creation and process anomalies for multiple samples, demonstrating host-level detection strengths.

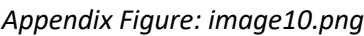
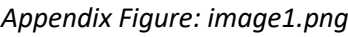
7. Conclusions and recommendations

Summary: Host-based detection (OSSEC) outperformed network-based IDS (Snort/Suricata) in this lab for ransomware that operated offline and primarily modified the host.

Recommendations: Employ layered detection combining host and network telemetry, deploy endpoint detection and response (EDR), ensure regular backups and immutable snapshots, monitor for registry changes and abnormal process creation, and craft YARA rules and Sigma signatures from the observed markers.

8. Appendix — Figures and IOCs

This appendix includes the figures extracted from the original analysis and suggested IOCs derived from the observations.



pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)

file settings about

c:\users\user\desktop\ransomware\keller-exe-3c

- indicators (virustotal > score)
- footprints (type > sha256)
- virustotal (62/74)
 - dos-header (size > 64 bytes)
 - dos-stub (size > 64 bytes)
 - rich-header (n/a)
 - file-header (executable > 32-bit)
 - optional-header (subsystem > GUI)
 - directories (count > 3)
 - sections (characteristics > virtual)
 - libraries (group > network)
 - imports (flag > 188)
 - exports (n/a)
 - thread-local-storage (count > 3)
 - .NET (n/a)
 - resources (n/a)
 - strings (flag > 75)
 - debug (n/a)
 - manifest (n/a)
 - version (n/a)
 - certificate (n/a)
 - overlay (n/a)

imports (188)	flag (47)	first-thunk-original (INT)	first-thunk (IAT)	hint
GetOverlappedResult	x	0x0022FC42	0x0022FC42	539 (0x021B)
Wow64DisableWow64FsRedir	x	0x002300E0	0x002300E0	1251 (0x04E3)
ControlService	x	0x0022F722	0x0022F722	103 (0x0067)
OpenProcessToken	x	0x0022F766	0x0022F766	500 (0x01F4)
FindVolumeClose	x	0x0022FA2E	0x0022FA2E	318 (0x013E)
GetCurrentProcessId	x	0x0022FB0A	0x0022FB0A	421 (0x01A5)
QueryPerformanceFrequency	x	0x0022FE0C	0x0022FE0C	936 (0x03A8)
NetApiBufferFree	x	0x0023012A	0x0023012A	47 (0x002F)
NetServerEnum	x	0x0023013E	0x0023013E	158 (0x009E)
NetShareEnum	x	0x0023014E	0x0023014E	178 (0x00B2)
WSACleanup	x	0x0023018A	0x0023018A	30 (0x001E)
WSAGetLastError	x	0x00230198	0x00230198	47 (0x002F)
WSASocketW	x	0x002301AA	0x002301AA	87 (0x0057)
WSAStartup	x	0x002301B8	0x002301B8	88 (0x0058)
bind	x	0x002301C6	0x002301C6	145 (0x0091)
closesocket	x	0x002301CE	0x002301CE	146 (0x0092)
connect	x	0x002301DC	0x002301DC	147 (0x0093)
freeaddrinfo	x	0x002301F6	0x002301F6	148 (0x0094)
getaddrinfo	x	0x002301F6	0x002301F6	149 (0x0095)
ioctlsocket	x	0x00230204	0x00230204	167 (0x00A7)
recv	x	0x00230212	0x00230212	171 (0x00AB)
recvfrom	x	0x0023021A	0x0023021A	172 (0x00AC)
send	x	0x00230226	0x00230226	174 (0x00AE)
sendto	x	0x0023022E	0x0023022E	175 (0x00AF)
setsockopt	x	0x00230238	0x00230238	176 (0x00B0)
VirtualProtect	x	0x002302B2	0x002302B2	1212 (0x04BC)
VirtualQuery	x	0x002302C4	0x002302C4	1215 (0x04BF)

sha256: 3D7CF20CA6476E14E0A026F98DD8FF1F26995CDC5854C3ADB41A6135EF11BA83 cpu: 32-bit file > type: executable subsystem: GUI

Appendix Figure: image11.png

pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)

file settings about

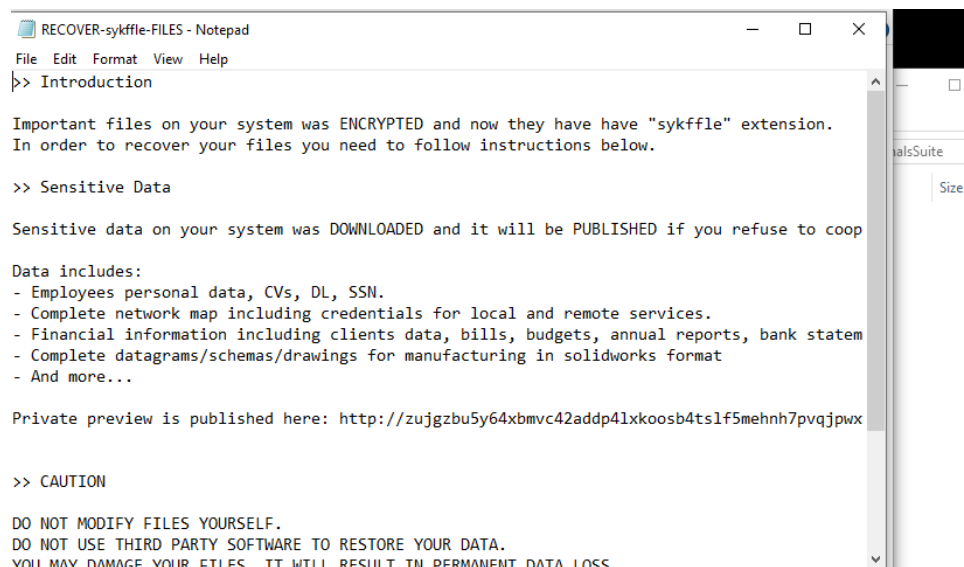
c:\users\user\desktop\ransomware\keller-exe-3c

- indicators (virustotal > score)
- footprints (type > sha256)
- virustotal (62/74)
 - dos-header (size > 64 bytes)
 - dos-stub (size > 64 bytes)
 - rich-header (n/a)
 - file-header (executable > 32-bit)
 - optional-header (subsystem > GUI)
 - directories (count > 3)
 - sections (characteristics > virtual)
 - libraries (group > network)
 - imports (flag > 188)
 - exports (n/a)
 - thread-local-storage (count > 3)
 - .NET (n/a)
 - resources (n/a)
 - strings (flag > 75)
 - debug (n/a)
 - manifest (n/a)
 - version (n/a)
 - certificate (n/a)
 - overlay (n/a)

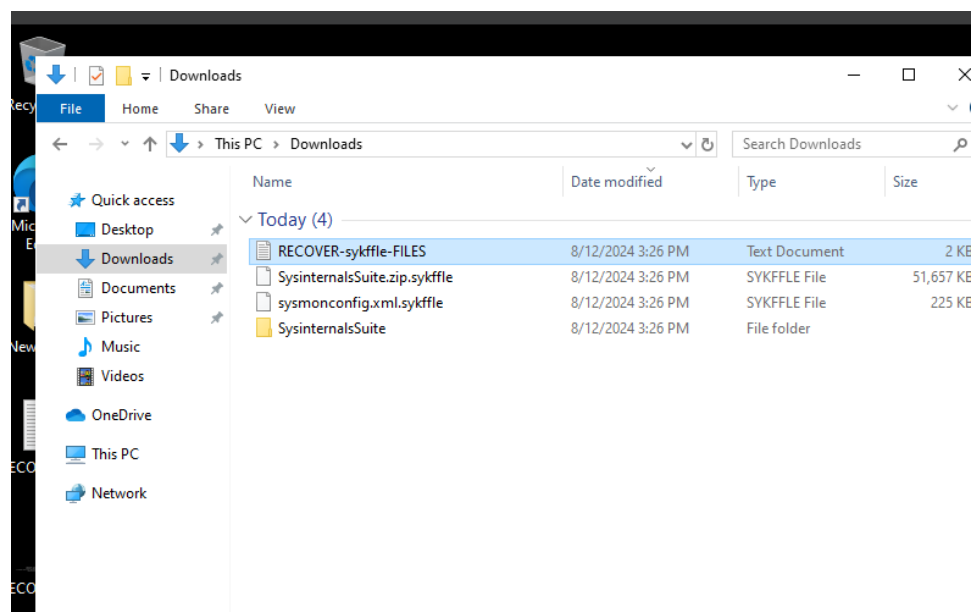
property	value	value	value
section	section[0]	section[1]	section[2]
name	.text	.data	.rdata
footprint > sha256	FC0D75BF51D08118C9F7864...	CAB4B3F458395293102DBB...	DD7C14DADF
entropy	6.395	1.188	7.624
file-ratio (99.96%)	71.77 %	0.02 %	25.36 %
raw-address (begin)	0x00000400	0x00190000	0x00190200
raw-address (end)	0x00190000	0x00190200	0x0021D600
raw-size (2280448 bytes)	0x0018FC00 (1637376 bytes)	0x00000200 (512 bytes)	0x0008D400 (
virtual-address	0x00001000	0x00191000	0x00192000
virtual-size (2280044 bytes)	0x0018FA4C (1636940 bytes)	0x00000108 (264 bytes)	0x0008D384 (
characteristics	0x60500060	0xC0400040	0x40600040
write	-	x	-
execute	x	-	-
share	-	-	-
self-modifying	-	-	-
virtual	-	-	-
items			
directory > import	-	-	-
directory > thread-local-storage	-	-	-
directory > import-address	-	-	-
base-of-code	0x00001000	-	-
base-of-data	-	0x00191000	-
entry-point	0x000014C0	-	-
thread-local-storage	0x0014CFF0	-	-
thread-local-storage	0x0018FC20	-	-

sha256: 3D7CF20CA6476E14E0A026F98DD8FF1F26995CDC5854C3ADB41A6135EF11BA83 cpu: 32-bit file > type: executable subsystem: GUI

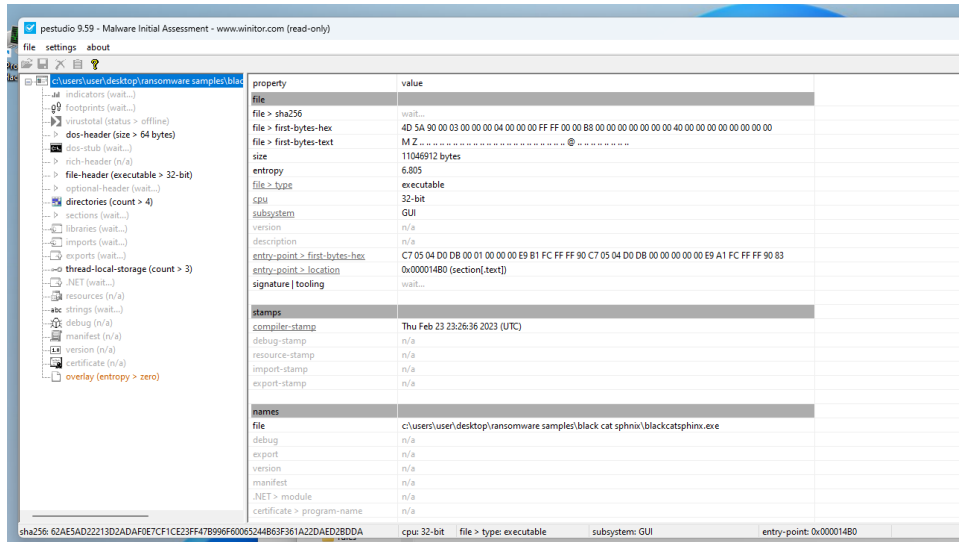
Appendix Figure: image12.png



Appendix Figure: image13.png



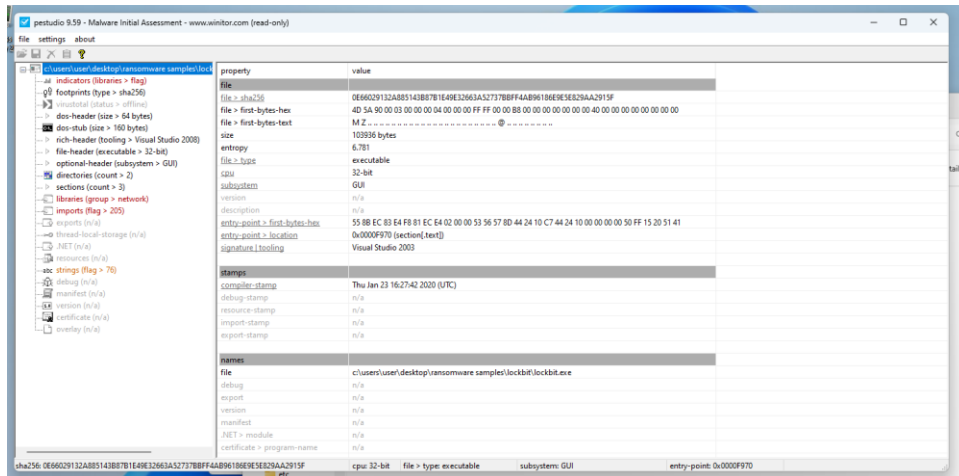
Appendix Figure: image14.png



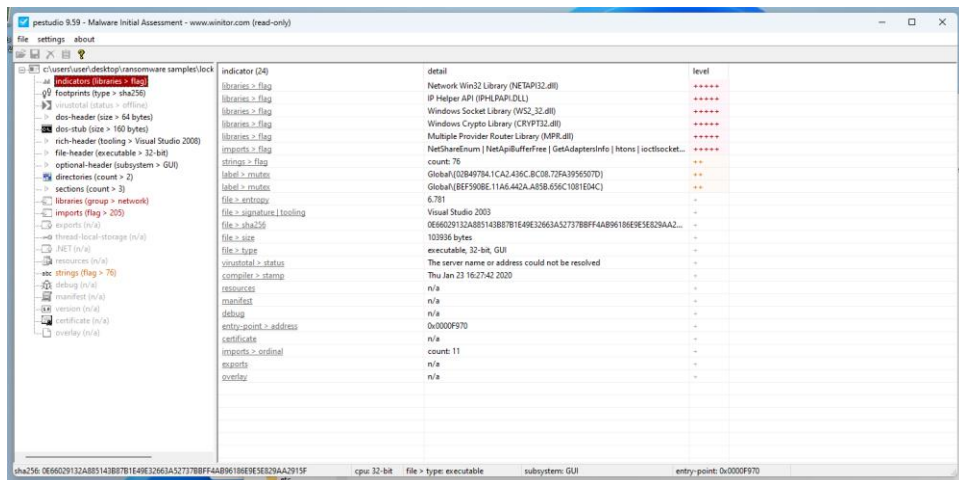
Appendix Figure: image15.png

```
<_notification_>-<0,0x00000000> __action__((action)"gatherer")
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x75351000,
[length]0x00001000, [protection]4, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0,
[process_identifier]8632)
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x75351000,
[length]0x00001000, [protection]2, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0,
[process_identifier]8632)
<system>-<0,0x00000000> NtClose([handle]0x00000240)
<system>-<0,0x00000000> NtClose([handle]0x00000244)
<exception>-<0,0x00000000> SetUnhandledExceptionFilter()
<system>-<-1073741515,0xC0000135> LdrGetDllHandle([module_address]0x00000000, [module_name]"libgcc_s_dw2-1.dll",
[stack_pivoted]0)
<exception>-<32513616,0x01F01E50> RtlAddVectoredExceptionHandler([FirstHandler]0)
<process>-<0,0x00000000> NtAllocateVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x01A38000,
[region_size]0x00006000, [allocation_type]4096, [protection]260, [stack_pivoted]0, [stack_dep_bypass]0,
[heap_dep_bypass]0, [process_identifier]8632)
<system>-<0,0x00000000> LdrGetDllHandle([module_address]0x75D20000, [module_name]"kernel32", [stack_pivoted]0)
<process>-<0,0x00000000> NtTerminateProcess([process_handle]0x00000000, [status_code]0, [process_identifier]0)
<process>-<0,0x00000000> NtTerminateProcess([process_handle]0x00000000, [status_code]0, [process_identifier]0)
<system>-<0,0x00000000> LdrGetDllHandle([module_address]0x75D20000, [module_name]"kernel32.dll", [stack_pivoted]0)
<system>-<0,0x00000000> LdrGetDllHandle([module_address]0x75760000, [module_name]"kernelbase.dll",
[stack_pivoted]0)
<system>-<0,0x00000000> NtClose([handle]0x00000228)
<system>-<0,0x00000000> NtClose([handle]0x0000022C)
<system>-<0,0x00000000> LdrGetDllHandle([module_address]0x77140000, [module_name]"ntdll.dll", [stack_pivoted]0)
<system>-<0,0x00000000> NtClose([handle]0x00000204)
<system>-<0,0x00000000> NtClose([handle]0x00000200)
<system>-<0,0x00000000> NtClose([handle]0x000001F4)
<system>-<0,0x00000000> NtClose([handle]0x000001F8)
<system>-<0,0x00000000> NtClose([handle]0x000001FC)
<system>-<0,0x00000000> NtClose([handle]0x000001F0)
<system>-<0,0x00000000> NtClose([handle]0x000001EC)
<system>-<0,0x00000000> NtClose([handle]0x000001E8)
<system>-<0,0x00000000> NtClose([handle]0x000001E4)
<system>-<0,0x00000000> NtClose([handle]0x000001D8)
<system>-<0,0x00000000> NtClose([handle]0x000001DC)
<system>-<0,0x00000000> NtClose([handle]0x000001E0)
<system>-<0,0x00000000> NtClose([handle]0x000001D0)
<system>-<0,0x00000000> NtClose([handle]0x000001D4)
<system>-<0,0x00000000> NtClose([handle]0x000001C8)
<system>-<0,0x00000000> NtClose([handle]0x000001CC)
<system>-<0,0x00000000> NtClose([handle]0x000001C4)
<system>-<0,0x00000000> LdrGetDllHandle([module_address]0x77140000, [module_name]"ntdll.dll", [stack_pivoted]0)
<system>-<0,0x00000000> LdrUnloadDll([module_address]0x75160000, [library]"IMM32")
<system>-<0,0x00000000> NtClose([handle]0x000001A0)
<system>-<0,0x00000000> NtClose([handle]0x000001A4)
<system>-<0,0x00000000> NtClose([handle]0x000001A8)
<registry>-<0,0x00000000> NtOpenKey([key_handle]0x000001A8, [desired_access]131097, [regkey]"HKEY_LOCAL_MACHINE
\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize")
<registry>-<-1073741772,0xC0000034> NtQueryValueKey([key_handle]0x000001A8, [information_class]2,
[regkey]"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles",
[key_name]<NULL>, [reg_type]0, [value]<NULL>)
<system>-<0,0x00000000> NtClose([handle]0x000001A8)
```

Appendix Figure: image16.png



Appendix Figure: image17.png



Appendix Figure: image18.png

pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)

file settings about

c:\Users\User\Desktop\ransomware sample\lock

indicators (libraries > flag)

footprints (type > sha256)

metadata (status > offline)

dos-header (size > 64 bytes)

dos-stub (size > 160 bytes)

rich-header (tooling > Visual Studio 2008)

file-header (executable > 32-bit)

optional-header (subsystem > GUI)

directories (count > 2)

sections (count > 3)

libraries (group > network)

imports (flag > 205)

exports (n/a)

thread-local-storage (n/a)

.NET (n/a)

resources (n/a)

strings (flag > 76)

debug (n/a)

manifest (n/a)

version (n/a)

certificate (n/a)

overlay (n/a)

imports (205)	flag (81)	first-thunk-original (NT)	first-thunk (IAT)	hint	group (0)	technique (17)	type (6)
GetCurrentProcessId	x	0x0001A6C0	0x0001A6C0	449 (0x17C1)	reconnaissance	T1057 Process Discovery	implicit
FindVolumeName	x	0x0001A732	0x0001A732	339 (0x175B)	reconnaissance	T1058 File System Logical	implicit
NetShareEnum	x	0x00019C79	0x00019C79	239 (0x00F7)	network	-	implicit
NetApiBufferFree	x	0x00019E38	0x00019E38	101 (0x0065)	network	-	implicit
GetAdapterInfo	x	0x00019EAA	0x00019EAA	63 (0x003F)	network	-	implicit
FindHtcm	x	0x00000009	0x00000009	0 (0x0000)	network	-	implicit
10.licetsocket	x	0x0000000A	0x0000000A	0 (0x0000)	network	-	implicit
111.WSASetLastError	x	0x0000000E	0x0000000E	0 (0x0000)	network	-	implicit
4.1connect	x	0x00000004	0x00000004	0 (0x0000)	network	-	implicit
11.inet_addr	x	0x00000008	0x00000008	0 (0x0000)	network	-	implicit
151 (. WSAFDISet)	x	0x00000007	0x00000007	0 (0x0000)	network	-	implicit
1.licetsocket	x	0x00000001	0x00000001	0 (0x0000)	network	-	implicit
18.1set	x	0x00000012	0x00000012	0 (0x0000)	network	-	implicit
116.WSACleanup	x	0x00000014	0x00000014	0 (0x0000)	network	-	implicit
113.WSASocket	x	0x00000013	0x00000013	0 (0x0000)	network	-	implicit
23.1connect	x	0x00000017	0x00000017	0 (0x0000)	network	-	implicit
WinNetUserEnumW	x	0x0001A1A9	0x0001A1A9	6 (0x0006)	network	-	implicit
WinNetUserEnumW	x	0x0001A196	0x0001A196	61 (0x003D)	network	-	implicit
WinNetUserEnumW	x	0x0001A1A2	0x0001A1A2	25 (0x0019)	network	-	implicit
WinNetUserEnumW	x	0x0001A19C	0x0001A19C	36 (0x0024)	network	-	implicit
WinNetUserEnumW	x	0x0001A19C	0x0001A19C	16 (0x0010)	network	-	implicit
DbgLocateVirtualMemory	x	0x0001A1F2	0x0001A1F2	133 (0x0087)	memory	T1055 Process Injection	implicit
WinFile	x	0x0001A7A6	0x0001A7A6	117 (0x0075)	file	-	implicit
SetThreadAffinityMask	x	0x0001A77A	0x0001A77A	1168 (0x0490)	execution	-	implicit
OpenProcess	x	0x0001A382	0x0001A382	896 (0x0380)	execution	T1055 Process Injection	implicit
CreateToolhelp32Snapshot	x	0x0001A3A6	0x0001A3A6	190 (0x00BE)	execution	T1057 Process Discovery	implicit
Process32First	x	0x0001A3A6	0x0001A3A6	917 (0x0395)	execution	T1057 Process Discovery	implicit
TerminateProcess	x	0x0001A360	0x0001A360	1216 (0x04C0)	execution	-	implicit
Process32Next	x	0x0001A3C0	0x0001A3C0	919 (0x0397)	execution	T1057 Process Discovery	implicit
CreateProcessA	x	0x0001A3E8	0x0001A3E8	164 (0x00A4)	execution	T1056 Execution through API	implicit
SetProcessShutdownParams	x	0x0001A67E	0x0001A67E	1193 (0x04B3)	execution	-	implicit
ShellExecuteExA	x	0x0001A264	0x0001A264	288 (0x0120)	execution	T1106 Execution through API	implicit
LoadEnumeratedAssembliesModules	x	0x0001A20C	0x0001A20C	64 (0x0040)	dynamic-library	-	implicit
RegisterSslKey	x	0x0001A996	0x0001A996	988 (0x03F8)	diagnostic	-	implicit
CryptBinaryToStringA	x	0x00019E06	0x00019E06	134 (0x008C)	crypto	T1132 Data Encoding	implicit
CryptReleaseContext	x	0x0001AAB8	0x0001AAB8	203 (0x00CB)	crypto	T1027 Obfuscated Files or Information	implicit
CryptGenRandom	x	0x0001A834	0x0001A834	193 (0x00C1)	crypto	T1027 Obfuscated Files or Information	implicit
SetConsoleCtrlHandler	x	0x0001A606	0x0001A606	1069 (0x042D)	console	-	implicit
SetConsoleTitle	x	0x0001A639	0x0001A639	1065 (0x0425)	console	-	implicit
SetConsoleMode	x	0x0001A66C	0x0001A66C	1063 (0x0423)	console	-	implicit
PostMessageW	-	0x0001A684	0x0001A684	563 (0x0233)	windowing	-	implicit
GetWindowLongA	-	0x0001A8A2	0x0001A8A2	403 (0x0197)	windowing	T1055 Process Injection	implicit
SetWindowLongA	-	0x0001A8C4	0x0001A8C4	707 (0x02C7)	windowing	T1055 Process Injection	implicit
GetCurrentProcess	-	0x0001A6F6	0x0001A6F6	710 (0x029E)	windowing	-	implicit

Appendix Figure: image19.png

pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)

file settings about

c:\Users\User\Desktop\ransomware sample\lock

indicators (imports > flag)

footprints (type > sha256)

metadata (status > offline)

dos-header (size > 64 bytes)

rich-header (n/a)

file-header (executable > 64-bit)

optional-header (subsystem > GUI)

directories (count > 4)

sections (file > PDF)

imports (flag > 135)

exports (n/a)

thread-local-storage (count > 3)

.NET (n/a)

resources (n/a)

strings (flag > 21)

debug (n/a)

manifest (n/a)

version (n/a)

certificate (n/a)

overlay (n/a)

library (4)	duplicate (0)	flag (0)	first-thunk-original (NT)	first-thunk (IAT)	type (1)	imports (135)	group (0)	description
ADVAPI32.dll	-	-	0x00073064	0x0007348C	implicit	2	-	Advanced Windows 32 Base API
USER32.dll	-	-	0x0007307C	0x000734D4	implicit	54	-	Windows NT BASE API Client
USER32.dll	-	-	0x00073234	0x0007368C	implicit	78	-	Microsoft C Runtime Library
USER32.dll	-	-	0x0007344C	0x00073904	implicit	1	-	Multi-User Windows USER API Client Library

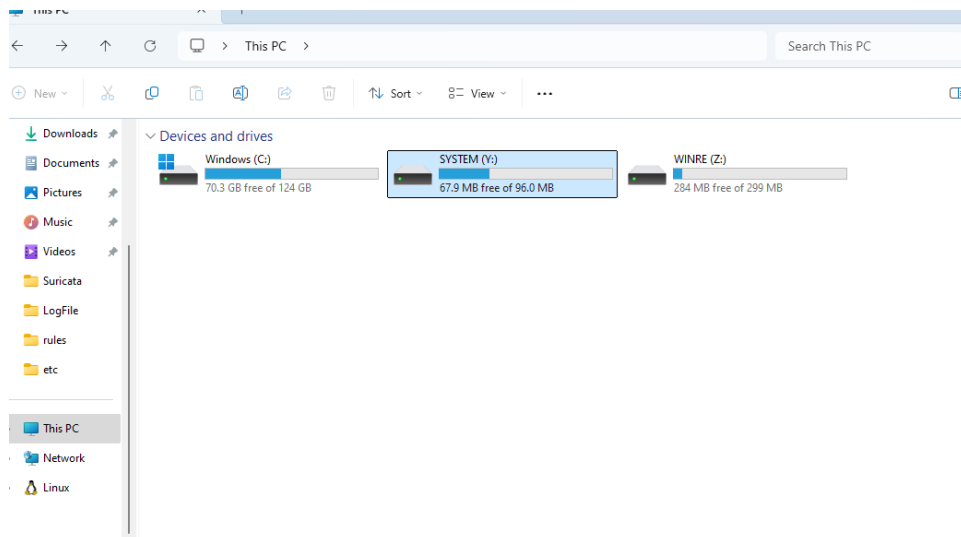
Appendix Figure: image2.png

```

<_notification>-<0,0x00000000> __process_([time_low]-486431023, [time_high]31124091, [pid]3676, [ppid]6264,
[module_path]"C:\Users\User\Desktop\Ransomware\lockbit.exe", [command_line]"C:\Users\User\Desktop\Ransomware
\lockbit.exe" ", [is_64bit]0, [track]11)
<_notification>-<0,0x00000000> __action_([action]"gatherer")
<_notification>-<0,0x00000000> __action_([action]"gatherer")
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x76841000,
[length]0x00001000, [protection]4, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0,
[process_identifier]3676)
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x76841000,
[length]0x00001000, [protection]2, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0,
[process_identifier]3676)
<system>-<0,0x00000000> NtClose([handle]0x00000240)
<system>-<0,0x00000000> NtClose([handle]0x00000244)
<process>-<0,0x00000000> NtOpenSection([section_handle]0x000000E0, [desired_access]13, [section_name]"shcore.dll")
<process>-<0,0x00000000> NtMapViewOfSection([section_handle]0x000000E0, [process_handle]0xFFFFFFFF,
[base_address]0x76500000, [commit_size]0, [section_offset]0, [view_size]0x000C1000, [allocation_type]8388608,
[win32_protect]128, [process_identifier]3676)
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x765B4000,
[length]0x00001000, [protection]2, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0,
[process_identifier]3676)
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x77551000,
[length]0x00003000, [protection]4, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0,
[process_identifier]3676)
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x77551000,
[length]0x00003000, [protection]2, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0,
[process_identifier]3676)
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x765B0000,
[length]0x00001000, [protection]4, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0,
[process_identifier]3676)
<system>-<0,0x00000000> NtClose([handle]0x000000E0)
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x765B0000,
[length]0x00001000, [protection]2, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0,
[process_identifier]3676)
<system>-<0,0x00000000> LdrGetDllHandle([module_address]0x760C0000, [module_name]"api-ms-win-core-synch-
11-2-0.dll", [stack_pivoted]0)
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x77226000,
[length]0x00001000, [protection]4, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0,
[process_identifier]3676)
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x77226000,
[length]0x00001000, [protection]2, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0,
[process_identifier]3676)
<process>-<244,0x000000F4> CreateThread([stack_size]0, [function_address]0x0040FEF0, [parameter]0x00000000,
[flags]0, [thread_identifier]9000)
<file>-<0,0x00000000> NtCreateFile([file_handle]0x00000180, [desired_access]1180063, [file_attributes]0,
[create_disposition]2, [create_options]0, [share_access]7, [filepath]"\\Device\\ConDrv\\Server", [filepath_r]"\\Device
\\ConDrv\\Server", [status_info]0x00000000)
<file>-<0,0x00000000> NtCreateFile([file_handle]0x00000184, [desired_access]1180063, [file_attributes]0,
[create_disposition]2, [create_options]32, [share_access]7, [filepath]"\\Device\\ConDrv\\Reference",
[filepath_r]"\\Reference", [status_info]0x00000000)
<services>-<0,0x00000000> OpenSCManagerA([machine_name]<NULL>, [database_name]<NULL>, [desired_access]983103)
<system>-<0,0x00000000> NtClose([handle]0x00000298)
<system>-<0,0x00000000> NtClose([handle]0x0000029C)

```

Appendix Figure: image20.png

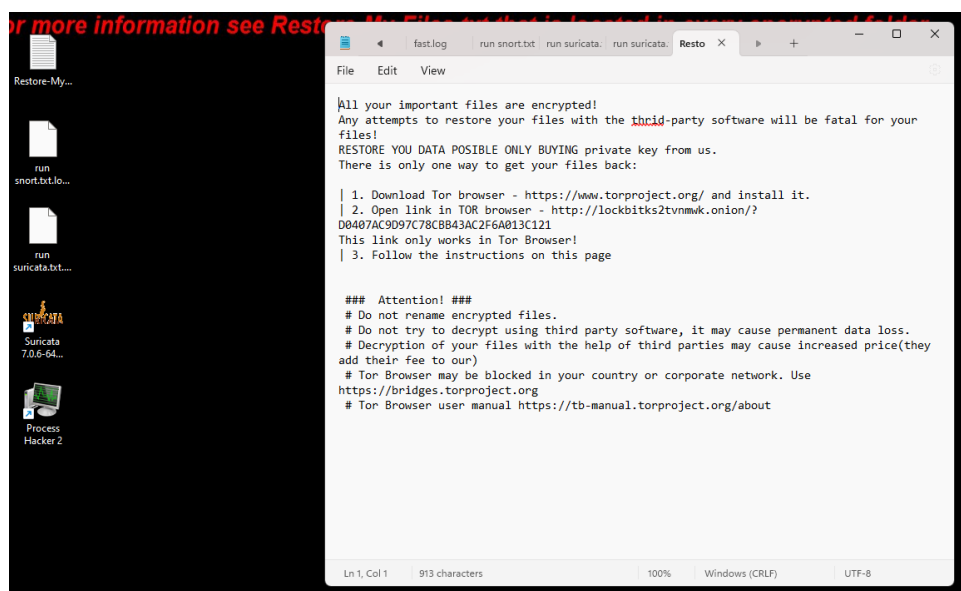


Appendix Figure: image21.png

421 results.

Address	Length	Result
0x5eeb30	11	SimSun-ExtB
0x5f0a2c	56	\\SYSTEM32\\kernel.appcore.dll
0x5f1ce0	38	NT AUTHORITY\\SYSTEM
0x5f1da0	28	LockBit Ransom
0x5f1e30	28	WINDEV2404EVAL
0x5f1e60	28	WINDEV2404EVAL
0x5f1ef0	30	lsapolicylookup
0x5f491e	76	\$****(,22666<<@@@#@#@#@#@#@@FFJJPPPTT
0x5f4e37	11	000
0x5f4e4b	97	0)0,4-4.>/F0F1P2X3X7XEBOfQfRfSfUfVfWfj^jsntzuzw
0x5f5958	20	?@ABCDEFGH
0x5f6fd8	62	C:\\Windows\\SYSTEM32\\clbcatq.dll
0x600fa0	46	oot%\\system32\\msctf.dll
0x600fe0	44	8473 files encrypted
0x6011c0	64	C:\\Windows\\System32\\OLEAUT32.dll
0x601260	44	8473 files encrypted
0x6012b0	58	C:\\Windows\\System32\\msctf.dll
0x6013f0	44	8473 files encrypted
0x601530	44	8473 files encrypted
0x601580	62	%Systemroot%\\System32\\msctf.dll
0x601800	58	C:\\Windows\\System32\\msctf.dll
0x6018a0	58	C:\\Windows\\system32\\msctf.dll

Appendix Figure: image22.png



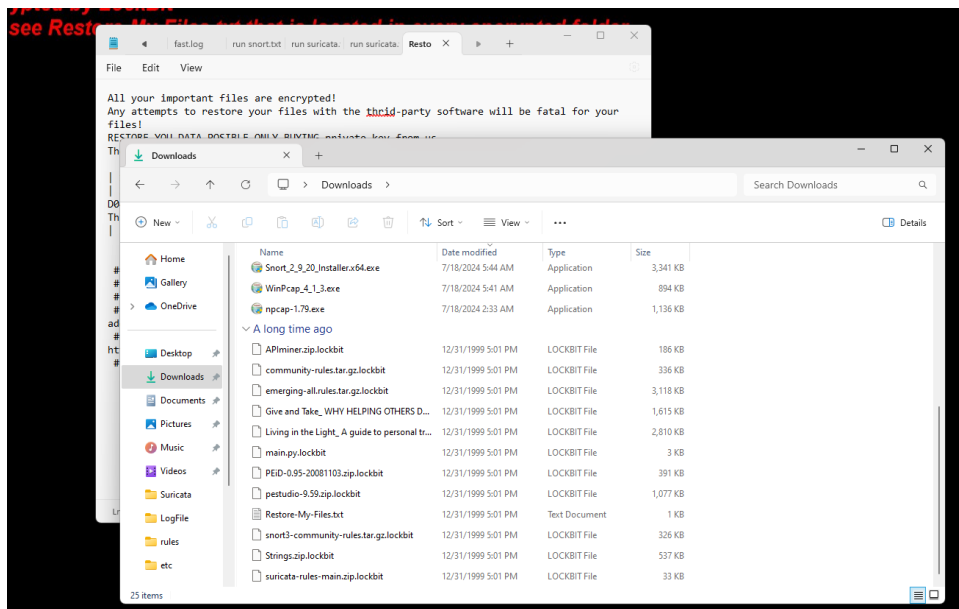
Appendix Figure: image23.png

All your files are encrypted by LockBit
for more information see Restore-My-Files.txt that is located in every encrypted folder

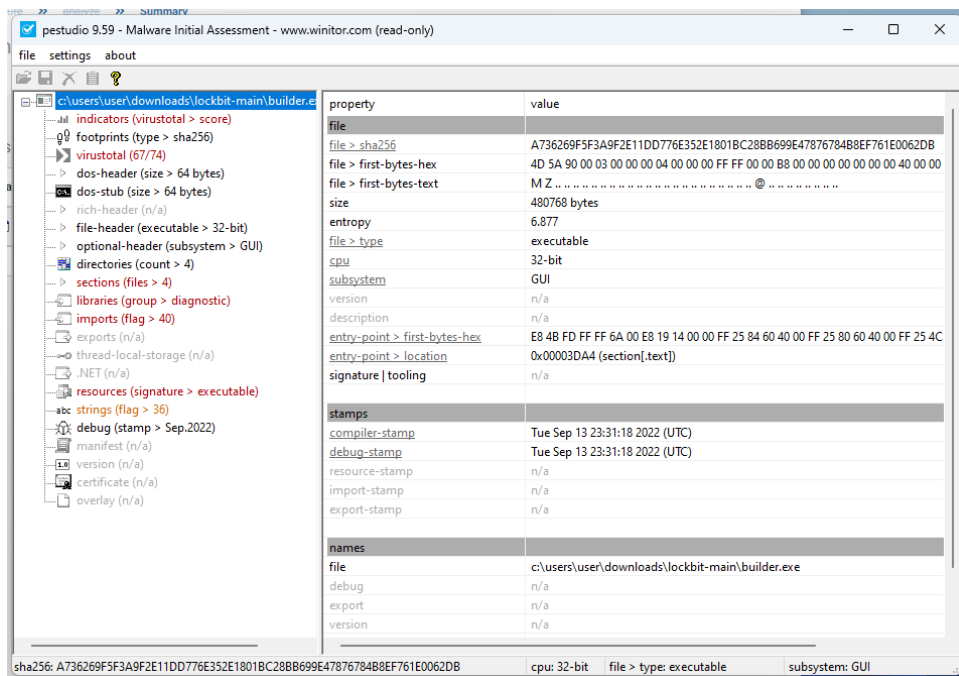
Appendix Figure: image24.png

Results - Lockbit.exe (8748)		
3,009 results.		
Address	Length	Result
0xc416d6	49	DriveData=C:\Windows\System32\Drivers\DriverData
0xc4170f	12	HOMEDRIVE=C:
0xc4171c	20	HOMEPATH=%User%\User
0xc41731	40	LOCALAPPDATA=C:\Users\User\AppData\Local
0xc4175a	28	LOGONSERVERS=\\WINDDEV240\NETAL
0xc41777	79	MOZ_PLUGIN_PATH=C:\Program Files (x86)\Foxit Software\Foxit Reader\plugins\
0xc417c7	22	NUMBER_OF_PROCESSORS=4
0xc417d6	31	OneDrive=C:\Users\User\OneDrive
0xc417e6	13	OS=Windows_NT
0xc4180c	332	Path=C:\Windows\System32\C:\Windows\C:\Windows\System32\Winem\C:\Windows\System32\WindowsPowerShell\1.0\C:\Windows\System32\OpenSSH\C:\Pro...
0xc41899	61	PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
0xc41897	26	PROCESSOR_ARCHITECTURE=x86
0xc41862	28	PROCESSOR_ARCHITECTURE=AMD64
0xc418cf	72	PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 185 Stepping 2, GenuineIntel
0xc41a18	17	PROCESSOR_LEVEL=6
0xc41a2a	23	PROCESSOR_REVISION=a592
0xc41a42	26	ProgramData=C:\ProgramData
0xc41a5d	35	ProgramFiles=C:\Program Files (x86)
0xc41a81	40	ProgramFiles(x86)=C:\Program Files (x86)
0xc41aaa	29	ProgramFiles(x86)=C:\Program Files
0xc41ac8	104	PSModulePath=%ProgramFiles%\WindowsPowerShell\Modules\C:\Windows\System32\WindowsPowerShell\1.0\Modules
0xc41b11	22	PUBLIC=C:\Users\Public
0xc41b4b	14	SystemDrive=C:
0xc41b57	21	SystemRoot=C:\Windows
0xc41b6d	37	TEMP=C:\Users\User\AppData\Local\Temp
0xc41b73	36	TMP=C:\Users\User\AppData\Local\Temp
0xc41b88	25	USERDOMAIN=WINDDEV240\NETAL
0xc41b42	40	USERDOMAIN_ROAMINGPROFILE=WINDDEV240\NETAL
0xc41bfb	13	USERNAME=User
0xc41c09	25	USERPROFILE=C:\Users\User
0xc41c23	17	windir=C:\Windows
0xc42d84	10	A31F8B1C8
0xc42db0	36	Intel(R) PRO(1000) MT Desktop Adapter
0xc42d88	12	192.168.46.1
0xc42d98	15	255.255.255.255
0xc42d0	929	All your important files are encrypted! Any attempts to restore your files with the third-party software will be fatal for your files! RESTORE YOUR DATA POSSIBLE ONLY ...
0xc4e392	50	VirtualBox Shared Folders
0xc4e758	50	VirtualBox Shared Folders
0xc4e660	50	VirtualBox Shared Folders
0xc4e60	28	WINDDEV240\NETAL
0xc23f4778	22	svchost.exe
0xc23f5228	24	winlogon.exe
0xc23f878	24	services.exe
0xc23f6a0	22	svchost.exe
0xc23f6a0	30	fontshost.exe
0xc23f6d8	30	fontshost.exe
0xc23f738	22	svchost.exe
0xc23f760	22	svchost.exe
0xc23f7d8	22	svchost.exe
0xc23f800	77	svchost.exe

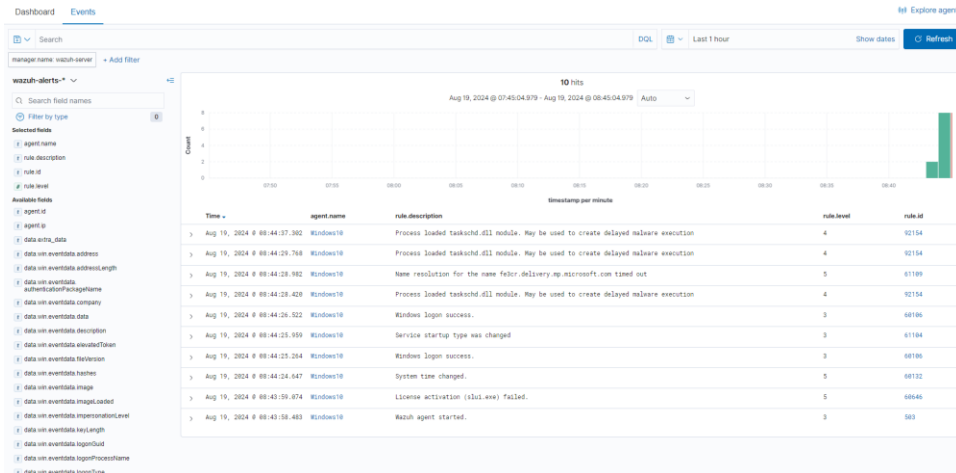
Appendix Figure: image25.png



Appendix Figure: image26.png



Appendix Figure: image27.png



Appendix Figure: image28.png

Time	Agent	Agent name	Technique(s)	Technique	Description	Level	Rule ID
Aug 19, 2024 @ 08:59:26.925	009	Windows10	T1055	Command and Control	Executable file dropped in folder commonly used by malware	15	92213
Aug 19, 2024 @ 08:59:25.338	009	Windows10	T1070.004	Defense Evasion	Powershell was used to delete files or directories	3	92021
Aug 19, 2024 @ 08:59:25.712	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 08:59:24.853	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 08:59:24.886	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 08:59:24.818	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 08:59:24.241	009	Windows10	T1027 T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
Aug 19, 2024 @ 08:59:24.191	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 08:59:24.188	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 08:59:23.887	009	Windows10	T1027 T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
Aug 19, 2024 @ 08:59:23.978	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 08:59:23.928	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052

Appendix Figure: image29.png

file	settings	about
pestudio 3.39 - Malware Initial Assessment - www.wintor.com (read-only)		
imports (135)	flag (21)	first-thunk-original (N/T)
GetCurrentProcessId	x	0x0000000000007264
GetThreadContext	x	0x00000000000024C4
GetThreadPriority	x	0x0000000000003A62
VirtualProtect	x	0x0000000000007042
VirtualQuery	x	0x0000000000007054
GetCurrentProcess	x	0x00000000000079D0
GetCurrentThread	x	0x00000000000028F5
GetCurrentThreadId	x	0x0000000000007A9E
RtlAddFunctionTable	x	0x00000000000078E4
SetProcessAffinityMask	x	0x0000000000007C58
SetThreadContext	x	0x0000000000007C72
SuspendThread	x	0x0000000000007CC0
TerminateProcess	x	0x0000000000007C20
AddVectoredExceptionHandler	x	0x000000000000793E
BaseSetException	x	0x000000000000787E
RemoveVectoredExceptionHandler	x	0x00000000000078A4
OutputDebugStringA	x	0x000000000000784E
CryptAcquireContextA	x	0x0000000000007914
CryptGenRandom	x	0x0000000000007992
rand	x	0x0000000000007804
srand	x	0x0000000000007404
CreateEventA	-	0x000000000000796A
CreateSemaphoreA	-	0x000000000000797A
DeleteCriticalSection	-	0x000000000000799E
EnterCriticalSection	-	0x000000000000798B
InitializeCriticalSection	-	0x0000000000007806
LeaveCriticalSection	-	0x0000000000007836
ReleaseSemaphore	-	0x0000000000007896
ResetEvent	-	0x00000000000078C8

Appendix Figure: image3.png

➤	Aug 19, 2024 @ 08:59:23.308	009	Windows10	T1027 T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
➤	Aug 19, 2024 @ 08:59:23.249	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:23.234	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
➤	Aug 19, 2024 @ 08:59:23.129	009	Windows10	T1027 T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
➤	Aug 19, 2024 @ 08:59:23.123	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:23.074	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
➤	Aug 19, 2024 @ 08:59:22.953	009	Windows10	T1027 T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
➤	Aug 19, 2024 @ 08:59:22.854	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:22.871	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
➤	Aug 19, 2024 @ 08:59:22.086	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:21.963	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
➤	Aug 19, 2024 @ 08:59:21.834	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:21.769	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052

Appendix Figure: image30.png

Security Alerts								
	Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
➤	Aug 19, 2024 @ 08:59:26.825	009	Windows10	T1105	Command and Control	Executable file dropped in folder commonly used by malware	15	92213
➤	Aug 19, 2024 @ 08:59:25.339	009	Windows10	T1070.004	Defense Evasion	Powershell was used to delete files or directories	3	92021
➤	Aug 19, 2024 @ 08:59:25.112	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:24.953	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
➤	Aug 19, 2024 @ 08:59:24.866	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:24.818	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
➤	Aug 19, 2024 @ 08:59:24.241	009	Windows10	T1027 T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
➤	Aug 19, 2024 @ 08:59:24.191	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:24.188	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
➤	Aug 19, 2024 @ 08:59:23.987	009	Windows10	T1027 T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
➤	Aug 19, 2024 @ 08:59:23.879	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:23.830	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052

Appendix Figure: image31.png

➤	Aug 19, 2024 @ 08:59:23.308	009	Windows10	T1027 T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
➤	Aug 19, 2024 @ 08:59:23.249	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:23.234	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
➤	Aug 19, 2024 @ 08:59:23.129	009	Windows10	T1027 T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
➤	Aug 19, 2024 @ 08:59:23.123	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:23.074	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
➤	Aug 19, 2024 @ 08:59:22.953	009	Windows10	T1027 T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
➤	Aug 19, 2024 @ 08:59:22.904	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:22.871	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
➤	Aug 19, 2024 @ 08:59:22.086	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:21.963	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
➤	Aug 19, 2024 @ 08:59:21.834	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
➤	Aug 19, 2024 @ 08:59:21.769	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052

Appendix Figure: image32.png

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 16, 2024 @ 09:20:56.628	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:56.763	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:56.080	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:55.962	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 16, 2024 @ 09:20:55.680	009	Windows10	T1490	Impact	System recovery disabled. Possible ransomware detected.	10	100105
Aug 16, 2024 @ 09:20:55.753	009	Windows10	T1490	Impact	System recovery disabled. Possible ransomware detected.	10	100105
Aug 16, 2024 @ 09:20:55.361	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 16, 2024 @ 09:20:55.106	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:54.736	009	Windows10	T1033.005	Execution, Persistence, Privilege Escalation	Process loaded located at module. May be used to create delayed malware execution	4	92154
Aug 16, 2024 @ 09:20:54.637	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 16, 2024 @ 09:20:53.751	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:53.726	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:53.701	009	Windows10			Software protection service scheduled successfully.	3	60642
Aug 16, 2024 @ 09:20:53.386	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 16, 2024 @ 09:20:52.946	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:52.115	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:48.656	009	Windows10	T1059.001	Execution	C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 09:20:33.581	009	Windows10	T1059 T1059	Command and Control, Execution	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe created a new scripting file under Windows Temp or User data folder	9	92201
Aug 16, 2024 @ 09:20:31.865	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 16, 2024 @ 09:20:30.381	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039

Appendix Figure: image33.png

Aug 16, 2024 @ 09:20:54.736	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:53.726	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:53.701	009	Windows10			Software protection service scheduled successfully.	3	60642
Aug 16, 2024 @ 09:20:53.386	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 16, 2024 @ 09:20:52.946	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:52.115	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:48.656	009	Windows10	T1059.001	Execution	C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 09:20:33.581	009	Windows10	T1059 T1059	Command and Control, Execution	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe created a new scripting file under Windows Temp or User data folder	9	92201
Aug 16, 2024 @ 09:20:31.865	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 16, 2024 @ 09:20:30.381	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039
Aug 16, 2024 @ 09:20:30.359	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039
Aug 16, 2024 @ 09:20:30.290	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039
Aug 16, 2024 @ 09:20:30.346	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039
Aug 16, 2024 @ 09:20:29.251	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 16, 2024 @ 09:20:29.235	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 16, 2024 @ 09:20:29.235	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 16, 2024 @ 09:20:29.220	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031

Appendix Figure: image34.png

Aug 16, 2024 @ 10:16:25.892	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.892	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.897	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.838	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.816	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.816	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.761	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.764	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.745	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.737	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.726	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.708	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:16:25.706	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:15:58.801	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010
Aug 16, 2024 @ 10:15:58.802	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	12	92010

Appendix Figure: image35.png

Time	Agent	Agent name	Technique(s)	Tactic(s)	Observation	Level	Rule ID
Aug 16, 2024 @ 09:20:56.628	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:56.763	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:56.080	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:55.962	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 16, 2024 @ 09:20:55.680	009	Windows10	T1490	Impact	System recovery disabled. Possible ransomware detected.	10	100105
Aug 16, 2024 @ 09:20:55.753	009	Windows10	T1490	Impact	System recovery disabled. Possible ransomware detected.	10	100105
Aug 16, 2024 @ 09:20:55.361	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 16, 2024 @ 09:20:55.106	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:54.736	009	Windows10	T1033.005	Execution, Persistence, Privilege Escalation	Process loaded located at module. May be used to create delayed malware execution	4	92154
Aug 16, 2024 @ 09:20:54.637	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 16, 2024 @ 09:20:53.751	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:53.726	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:53.701	009	Windows10			Software protection service scheduled successfully.	3	60642
Aug 16, 2024 @ 09:20:53.386	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 16, 2024 @ 09:20:52.946	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:52.115	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:48.656	009	Windows10	T1059.001	Execution	C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 09:20:33.581	009	Windows10	T1059 T1059	Command and Control, Execution	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe created a new scripting file under Windows Temp or User data folder	9	92201
Aug 16, 2024 @ 09:20:31.865	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 16, 2024 @ 09:20:30.381	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039

Appendix Figure: image36.png

Aug 16, 2024 @ 09:20:30.750	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:53.726	009	Windows10	T1076	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows login success.	3	60106
Aug 16, 2024 @ 09:20:53.701	009	Windows10			Software protection service scheduled successfully.	3	60642
Aug 16, 2024 @ 09:20:53.386	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 16, 2024 @ 09:20:52.946	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:52.115	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92032
Aug 16, 2024 @ 09:20:48.656	009	Windows10	T1059.001	Execution	C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 09:20:33.581	009	Windows10	T1059 T1059	Command and Control, Execution	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe created a new scripting file under Windows Temp or User data folder	9	92201
Aug 16, 2024 @ 09:20:31.868	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 16, 2024 @ 09:20:30.381	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039
Aug 16, 2024 @ 09:20:30.359	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039
Aug 16, 2024 @ 09:20:30.290	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039
Aug 16, 2024 @ 09:20:30.346	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039
Aug 16, 2024 @ 09:20:29.251	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 16, 2024 @ 09:20:29.235	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 16, 2024 @ 09:20:29.235	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 16, 2024 @ 09:20:29.220	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031

Appendix Figure: image37.png

Aug 16, 2024 @ 10:16:25.892	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.892	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.897	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.838	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.816	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.816	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.761	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.764	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.745	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.737	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.726	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.708	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:16:25.706	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:15:58.861	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066
Aug 16, 2024 @ 10:15:58.852	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Exploiter process was accessed by C:\Windows\System32\cmd.exe binary in a suspicious location launched by C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	4	92066

Appendix Figure: image38.png

Time	Agent	Agent name	Technique(s)	Tactics	Description	Level	Rule ID
Aug 19, 2024 @ 10:18:36.380	009	Windows10	T1003	Command and Control	Executable file imported in UserShellcode folder	12	92207
Aug 19, 2024 @ 10:17:45.137	009	Windows10	T1034	Defense Evasion, Privilege Escalation	LotusBot 3.0 Remoteview launched	16	100013
Aug 19, 2024 @ 10:18:21.146	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:21.155	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:21.110	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:21.110	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:21.075	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:21.089	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:21.040	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:21.040	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:21.004	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:20.993	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:20.961	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:20.961	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:18:20.927	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\Users\user\AppData\Local\Microsoft\Windows\SelfHost\SelfHost.exe, possible process injection	12	92910

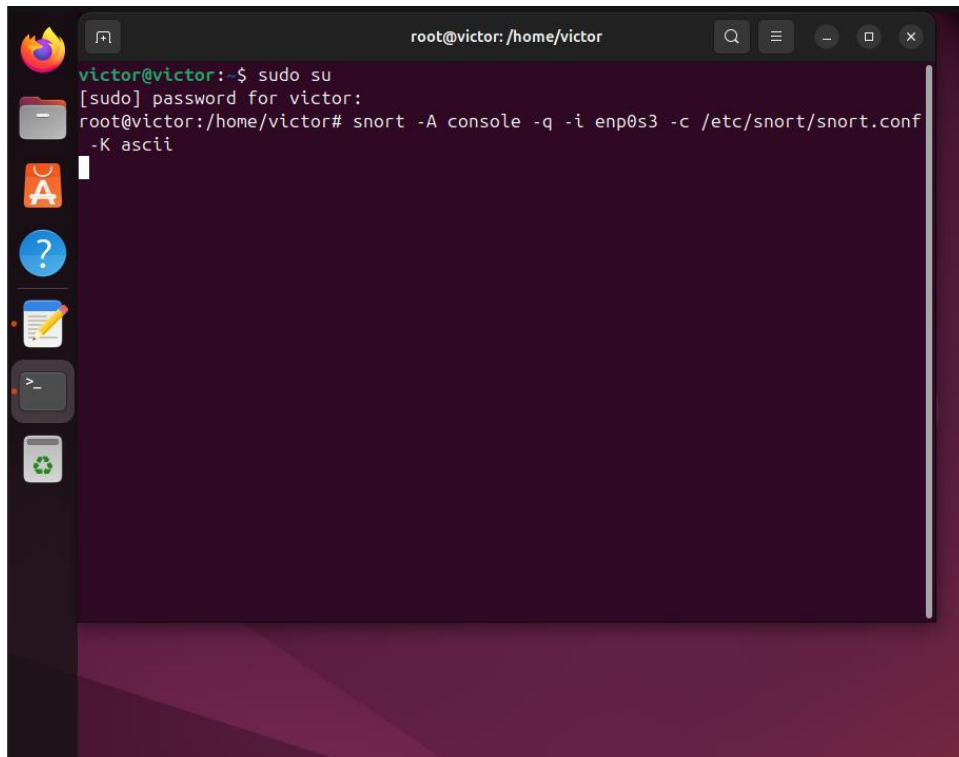
Appendix Figure: image39.png

pestid 9.59 - Malware Initial Assessment - www.winitox.com (read-only)						
file settings about						
encoding (2)	size (bytes)	location	flag (21)	label (191)	group (11)	value (934)
ASCII	19	sections.data	*	import	reconnaissance	GetCurrentProcessId
ASCII	16	sections.data	*	import	reconnaissance	GetThreadContext
ASCII	17	sections.data	*	import	reconnaissance	GetThreadPriority
ASCII	14	sections.data	*	import	memory	VirtualProtect
ASCII	12	sections.data	*	import	memory	VirtualQuery
ASCII	17	sections.data	*	import	execution	GetCurrentProcess
ASCII	16	sections.data	*	import	execution	GetCurrentThread
ASCII	18	sections.data	*	import	execution	GetCurrentThreadId
ASCII	19	sections.data	*	import	execution	RtlAddFunctionTable
ASCII	22	sections.data	*	import	execution	SetProcessAffinityMask
ASCII	16	sections.data	*	import	execution	SetThreadContext
ASCII	13	sections.data	*	import	execution	SuspendThread
ASCII	16	sections.data	*	import	execution	TerminateProcess
ASCII	27	sections.data	*	import	exception	AddVectoredExceptionHandler
ASCII	14	sections.data	*	import	exception	RaiseException
ASCII	30	sections.data	*	import	exception	RemoveVectoredExceptionHandler
ASCII	17	sections.data	*	import	diagnostic	OutputDebugString
ASCII	14	sections.data	*	import	crypto	CryptGenRandom
ASCII	19	sections.data	*	import	crypto	CryptAcquireContext
ASCII	4	sections.data	*	import	crypto	rand
ASCII	5	sections.data	*	import	crypto	rand
ASCII	21	sections.data	*	import	synchro	DeleteCriticalSection
ASCII	20	sections.data	*	import	synchro	EnterCriticalSection
ASCII	25	sections.data	*	import	synchro	InitializeCriticalSection
ASCII	20	sections.data	*	import	synchro	LeaveCriticalSection
ASCII	16	sections.data	*	import	synchro	ReleaseSemaphore
ASCII	10	sections.data	*	import	synchro	ResetEvent
ASCII	8	sections.data	*	import	synchro	SetEvent
ASCII	23	sections.data	*	import	synchro	TryEnterCriticalSection

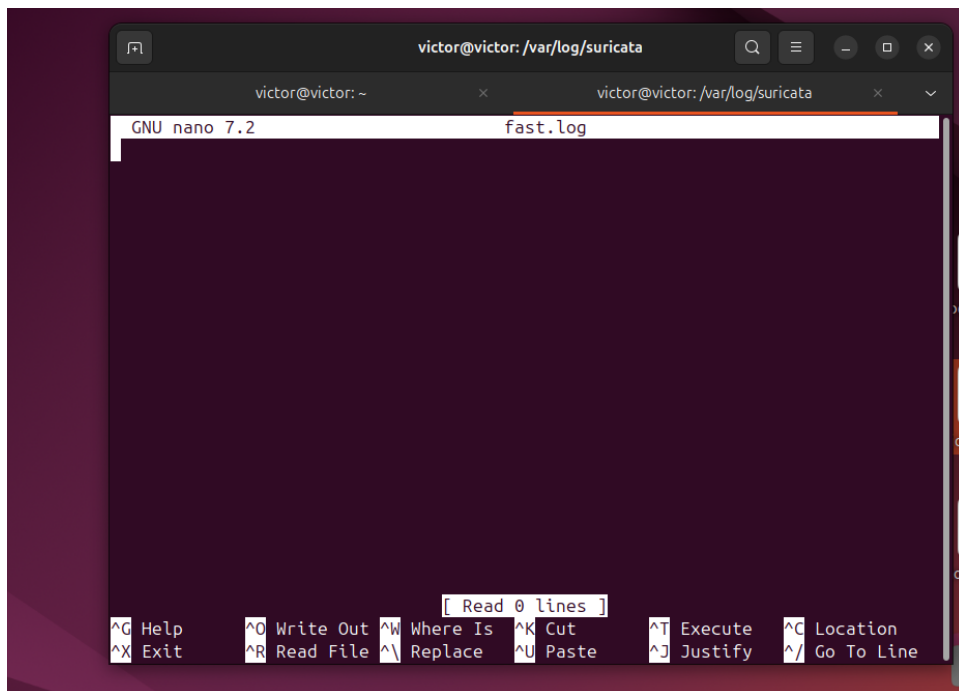
Appendix Figure: image4.png

Aug 19, 2024 @ 09:18:20.303	009	Windows10	T1087	T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:18:20.189	009	Windows10	T1486		Impact	The file C:\Users\user\Desktop\New folder\RECOVER-syFile-FILES.txt has been created in multiple directories. Possible BlackCat ransomware detected.	12	100107
Aug 19, 2024 @ 09:18:25.638	009	Windows10	T1486		Impact	The file C:\Users\user\Desktop\New folder\RECOVER-syFile-FILES.txt has been created in multiple directories. Possible BlackCat ransomware detected.	12	100107
Aug 19, 2024 @ 09:18:25.590	009	Windows10	T1486		Impact	The file C:\Users\user\Desktop\RECOVER-syFile-FILES.txt has been created in multiple directories. Possible BlackCat ransomware detected.	12	100107
Aug 19, 2024 @ 09:18:25.575	009	Windows10	T1059.003		Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:18:25.460	009	Windows10	T1087	T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:18:25.434	009	Windows10	T1027	T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
Aug 19, 2024 @ 09:18:25.434	009	Windows10	T1059.003		Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:18:25.387	009	Windows10	T1059.003		Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:18:25.321	009	Windows10	T1087	T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:18:25.280	009	Windows10	T1059.003		Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:18:25.249	009	Windows10	T1087	T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:18:24.640	009	Windows10				Windows application error event.	9	80602
Aug 19, 2024 @ 09:18:24.363	009	Windows10	T1059.003		Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:18:24.216	009	Windows10	T1087	T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032

Appendix Figure: image40.png



Appendix Figure: image41.png



Appendix Figure: image42.png

pestudio 9.59 - Malware Initial Assessment - www.wintr.com (read-only)

file settings about

c:\users\user\desktop\ransomware\samples\rhys

indicators (imports > flag)

footprints (type > sha256)

unrelated (status > affine)

dos-header (size > 64 bytes)

dos-stub (size > 64 bytes)

rich-header (n/a)

file-header (executable > 64-bit)

optional-header (subsystem > GUI)

directories (count > 4)

resources (count > 4)

imports (flag > 135)

exports (n/a)

thread-local-storage (count > 3)

dll (n/a)

resources (n/a)

strings (flag > 21)

debug (n/a)

manifest (n/a)

version (n/a)

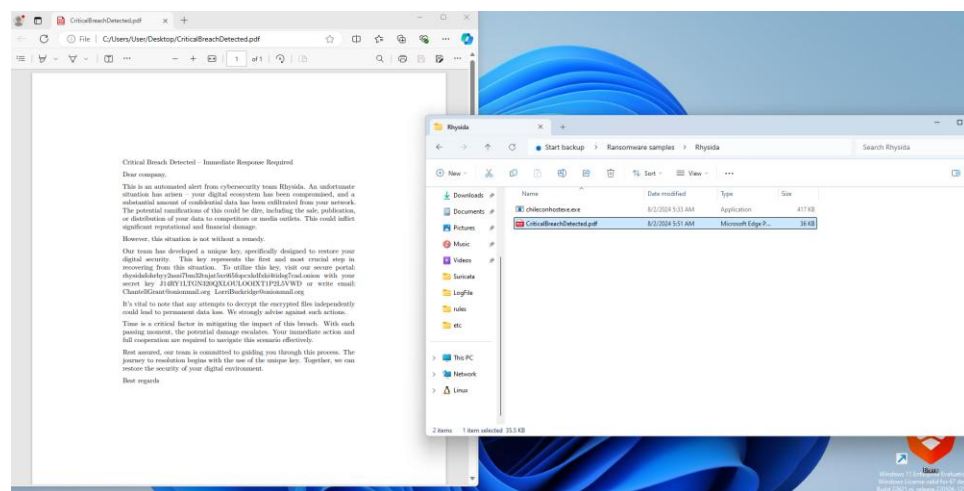
certificate (n/a)

overlay (n/a)

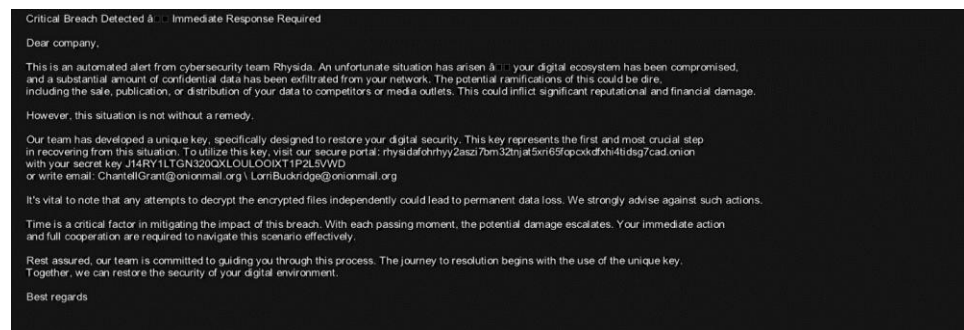
property	value	value	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]	section[4]	section[5]
name	.text	.data	.rdata	.pdata	.xdata	.bss
location	D36958F33B84E1930CD83...	939CB34502675A36CC487...	3F7D14E771A7D7E46E7346...	6F440D8736B4D1907627E...	ED66337F6CF7456D242637B...	n/a
entropy	6.371	7.951	5.741	5.509	4.378	n/a
file-ratio (99.76%)	70.26 %	9.47 %	14.39 %	2.16 %	2.04 %	n/a
raw-address (begin)	0x00004000	0x00048000	0x00053600	0x00062600	0x00064A00	0x00000000
raw-address (end)	0x00049800	0x00053600	0x00062600	0x00064A00	0x00066C00	0x00000000
raw-size (425584 bytes)	0x00049400 (300032 bytes)	0x00009500 (40448 bytes)	0x00009000 (61440 bytes)	0x00002400 (9216 bytes)	0x00002200 (8704 bytes)	0x00000000
virtual-address	0x00001000	0x00048000	0x00055000	0x00064000	0x00067000	0x0006A000
virtual-size (457844 bytes)	0x000493C8 (299976 bytes)	0x00009D80 (40320 bytes)	0x0000E900 (61072 bytes)	0x00002274 (8832 bytes)	0x000021E0 (8672 bytes)	0x00008400
characteristics	0x00000000	0xC0000040	0x40000040	0x40300040	0x40300040	0xC0000000
write	-	x	-	-	-	x
execute	x	-	-	-	-	-
share	-	-	-	-	-	-
self-modifying	-	-	-	-	-	-
virtual	-	-	-	-	-	x
items	-	-	-	-	-	-
directory > import	-	-	-	-	-	-
directory > exception	-	-	-	0x00064000	-	-
directory > thread-local-storage	-	-	-	-	-	-
directory > import-address	-	-	-	-	-	-
base-of-code	0x00001000	-	-	-	-	-
entry-point	0x00001400	-	-	-	-	-
file signature PDF, size 38144 bytes	-	file signature PDF, size 181...	-	-	-	-
thread-local-storage	0x00046D40	-	-	-	-	-
thread-local-storage	0x00046D70	-	-	-	-	-
thread-local-storage	0x00043050	-	-	-	-	-

0x76A736781A4B8E81B0B6F7A7446E771A7D7E46E7346... File is base executable

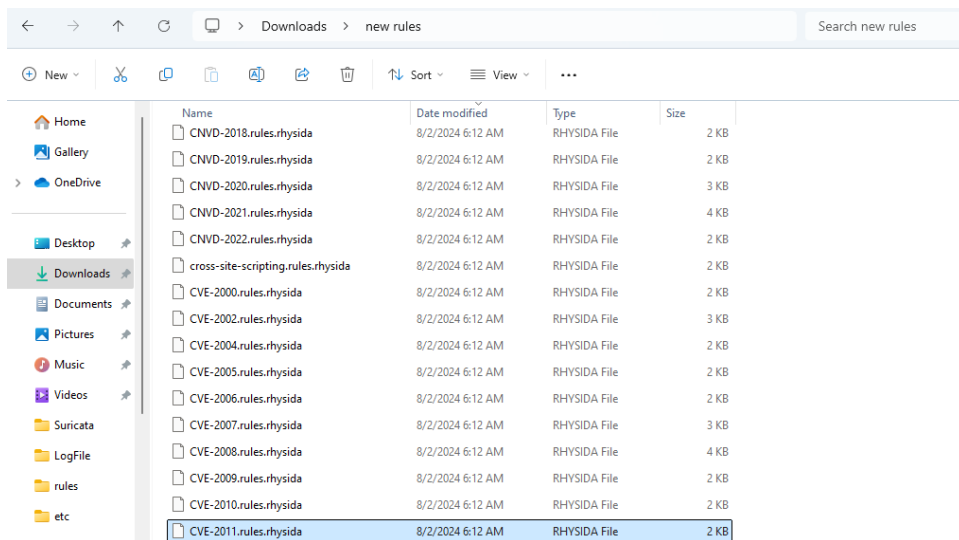
Appendix Figure: image5.png



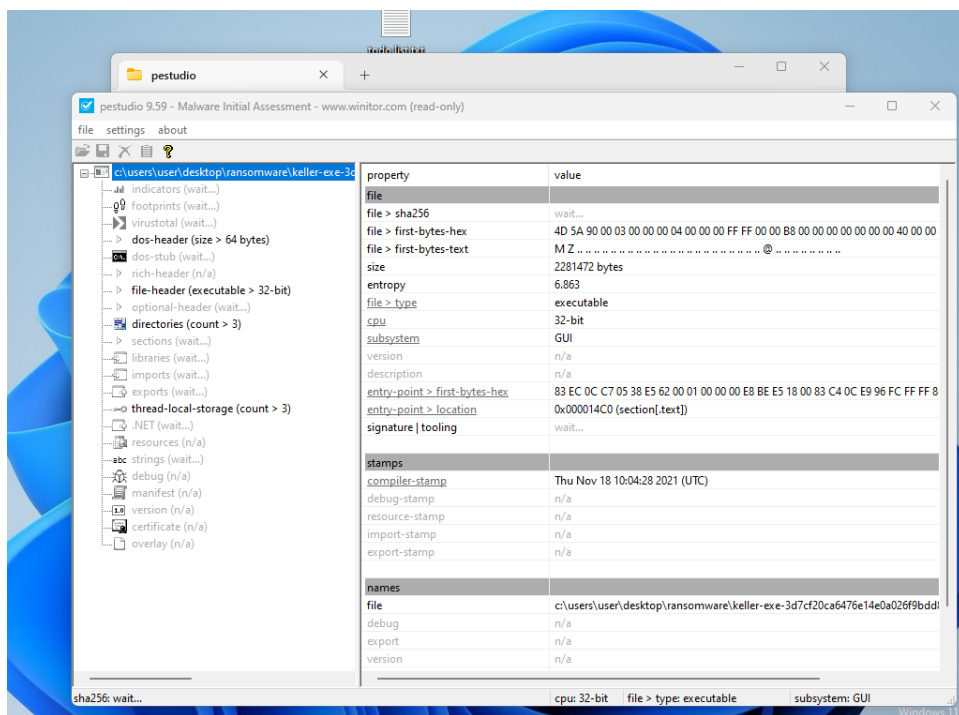
Appendix Figure: image6.png



Appendix Figure: image7.png



Appendix Figure: image8.png



Appendix Figure: image9.png