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

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.

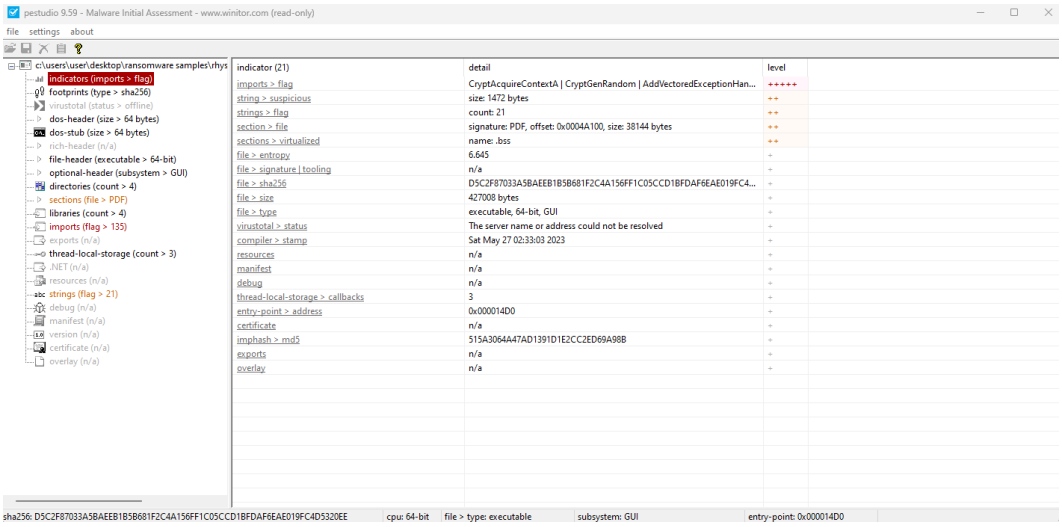


Figure: image1.png

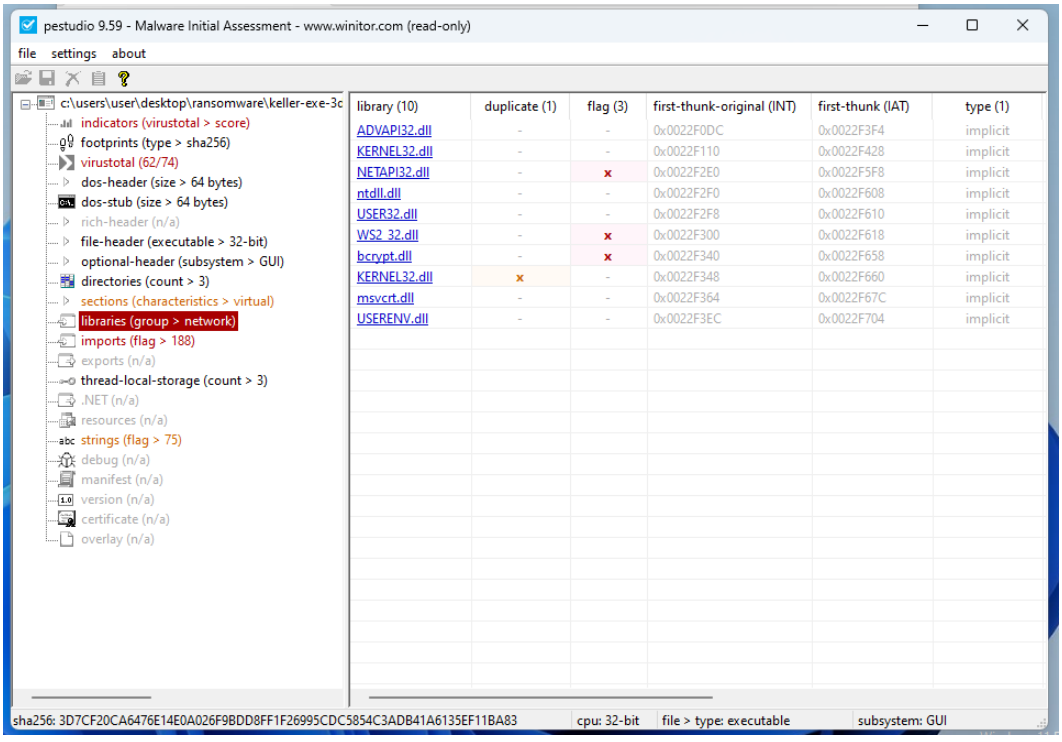


Figure: image10.png

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.

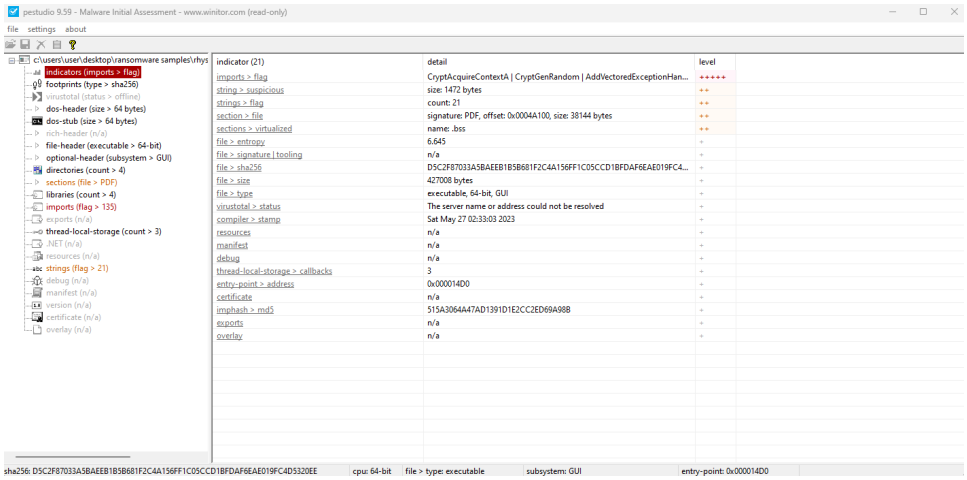
Findings: Snort and Suricata (network-based IDS) generated no significant alerts for the samples in the isolated virtual lab. OSSEC (host-based IDS) detected registry changes, file modifications, ransom note creation and process anomalies for multiple samples, demonstrating host-level detection strengths.

7. Conclusions and recommendations

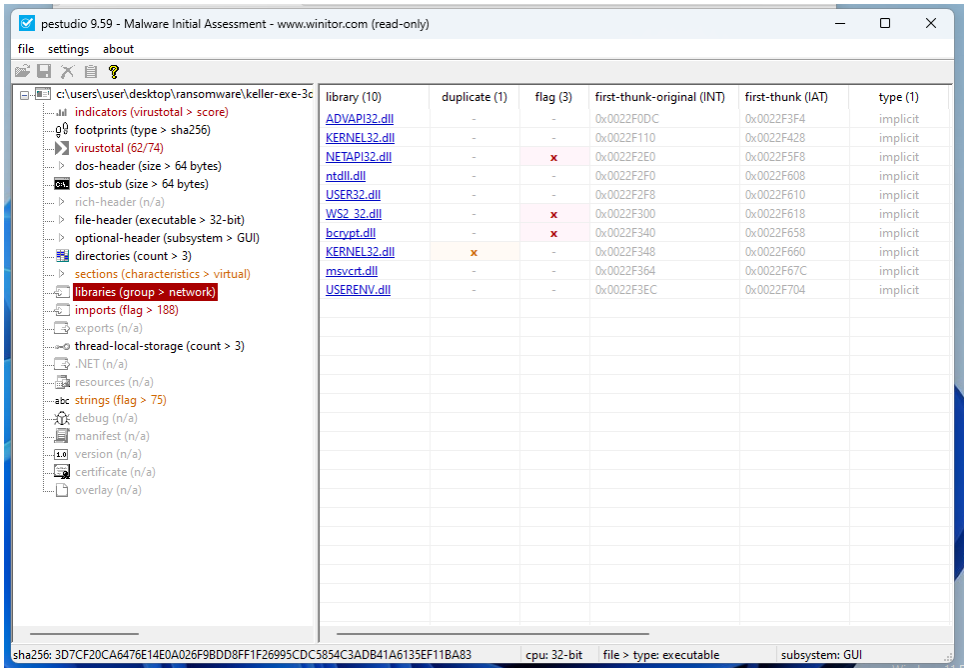
Summary: Host-based detection (OSSEC) outperformed network-based IDS (Snort/Suricata) in this lab for ransomware that operated offline and primarily modified the host.
Recommendations: Employ layered detection combining host and network telemetry, deploy endpoint detection and response (EDR), ensure 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

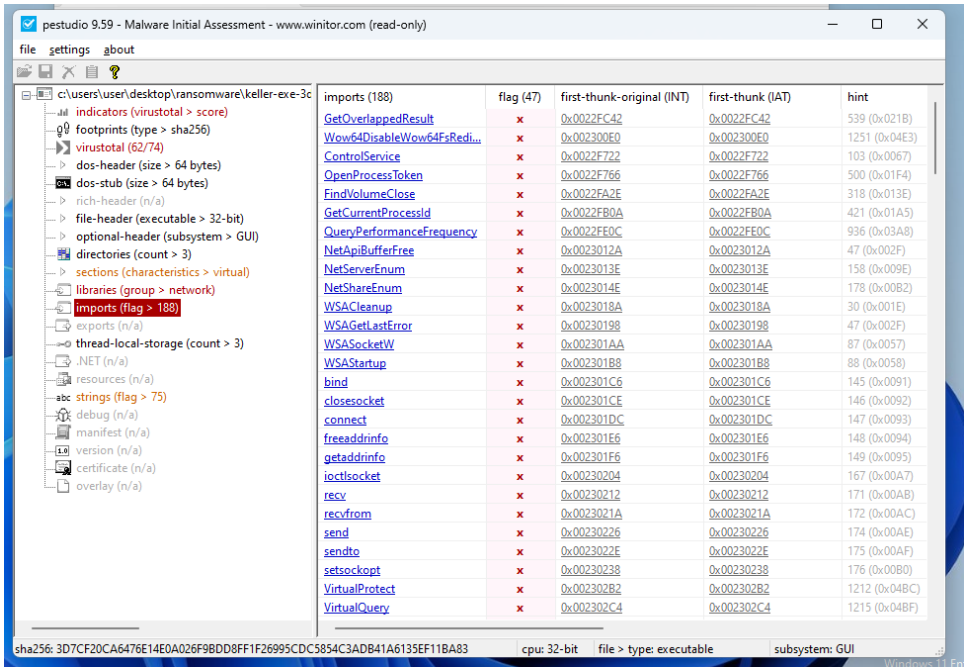
This appendix includes the figures extracted from the original analysis and suggested IOCs derived from the observations.



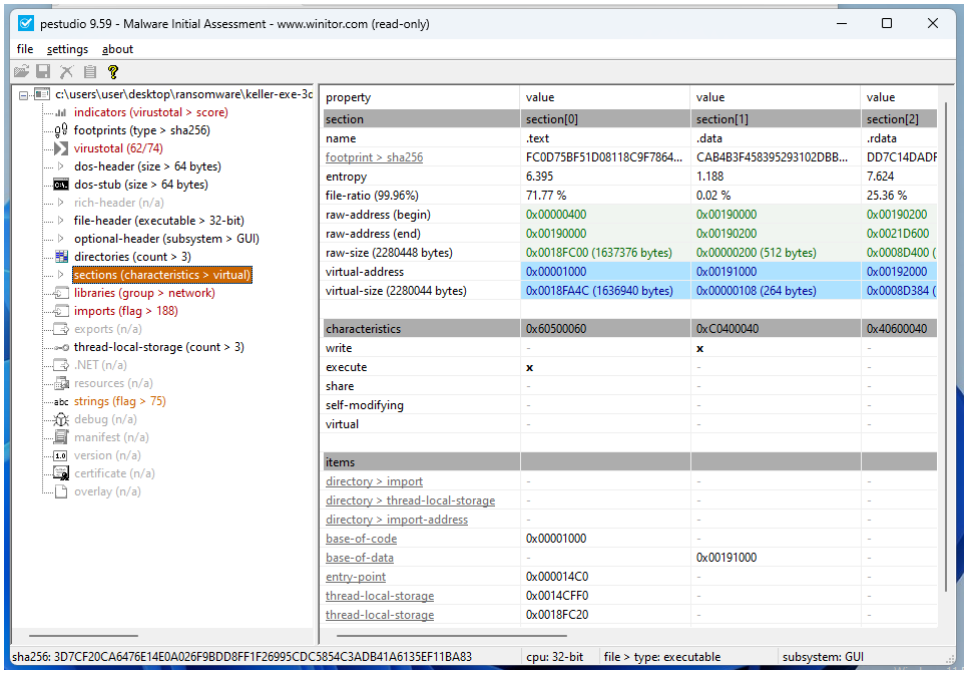
Appendix Figure: image1.png



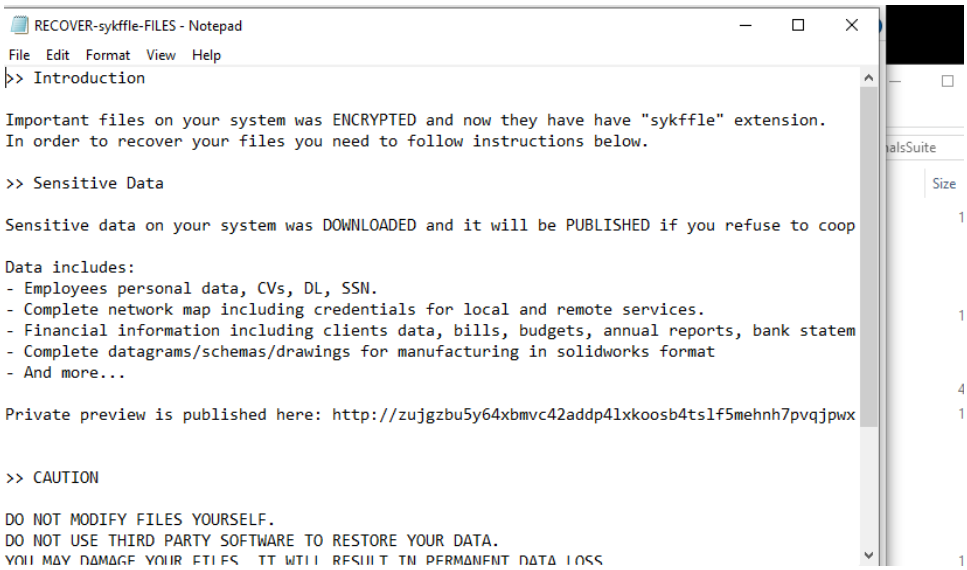
Appendix Figure: image10.png



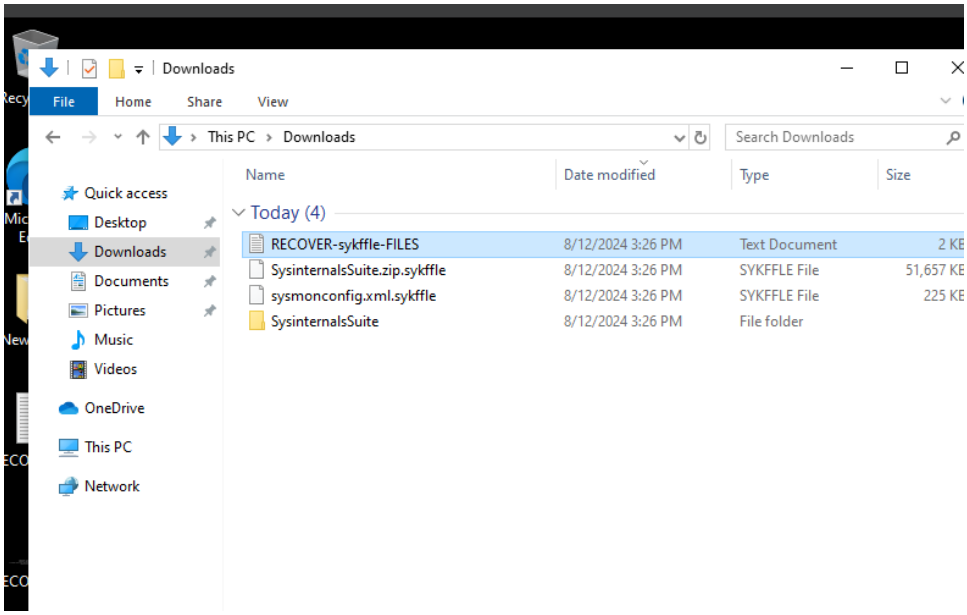
Appendix Figure: image11.png



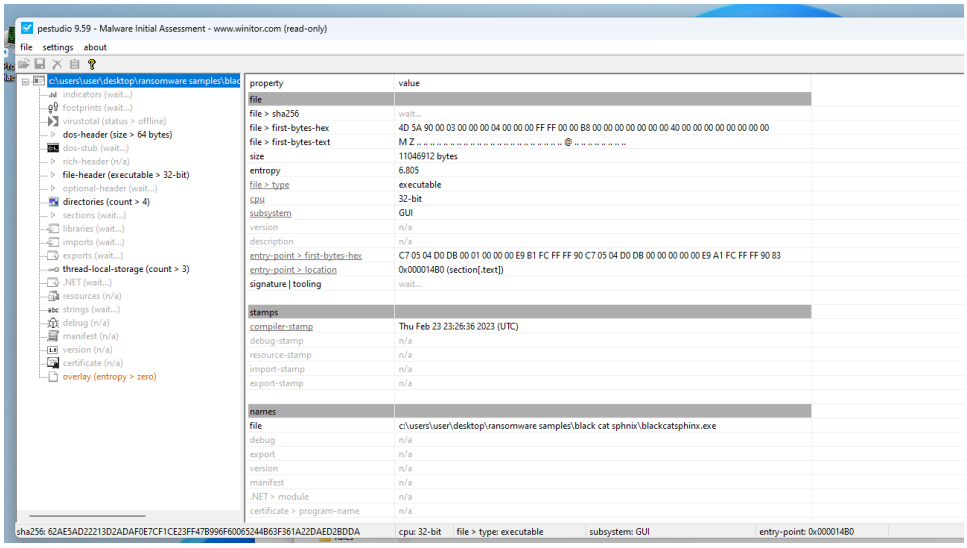
Appendix Figure: image12.png



Appendix Figure: image13.png



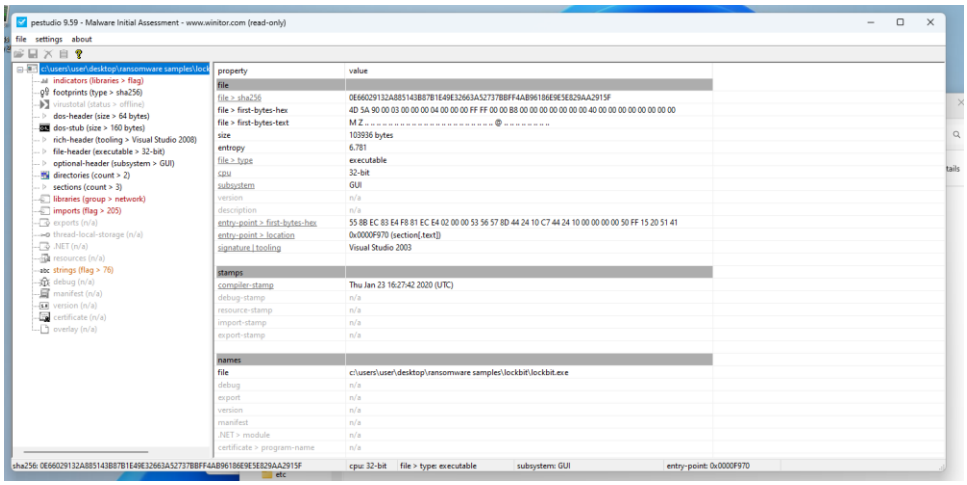
Appendix Figure: image14.png



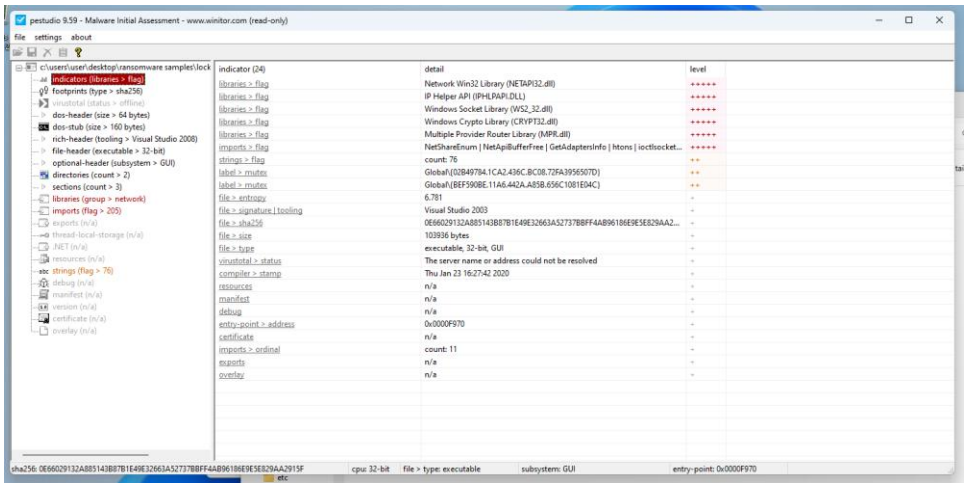
Appendix Figure: image15.png

```
<__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> SetUnhandledExceptionFilte)
<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)
```

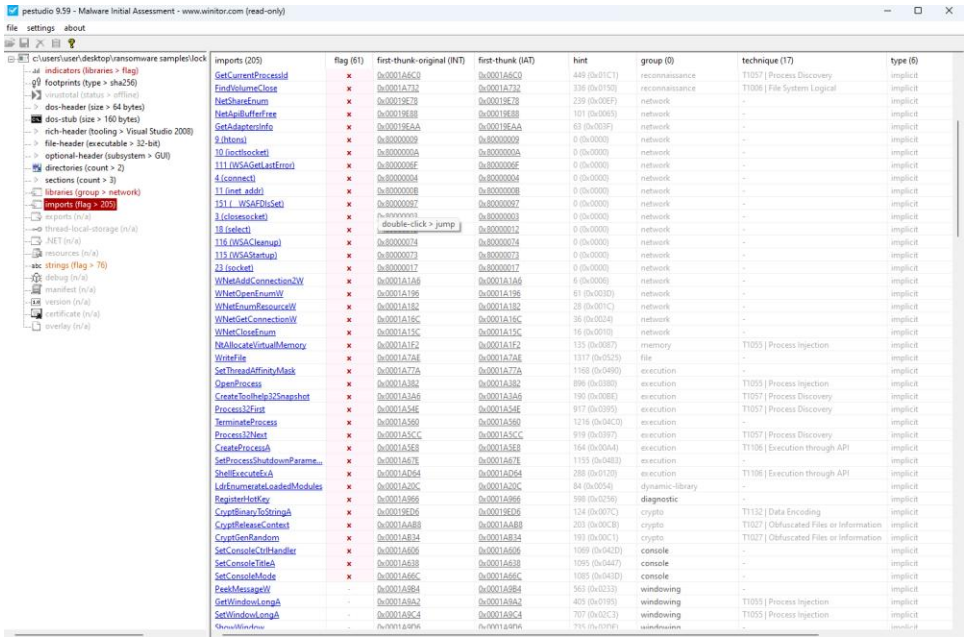
Appendix Figure: image16.png



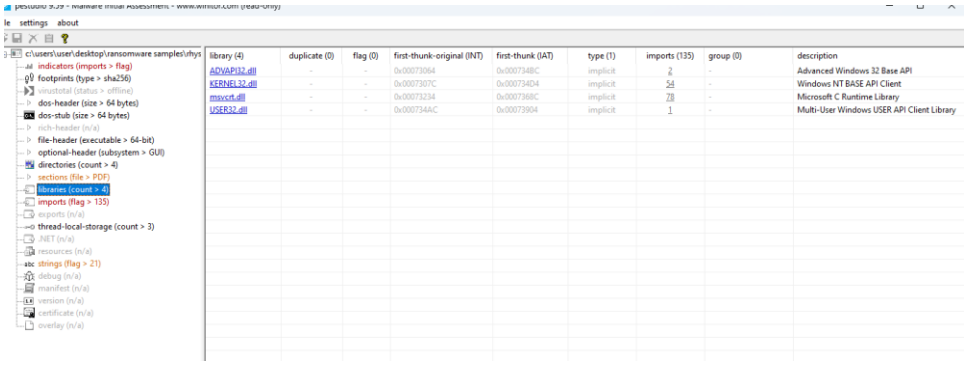
Appendix Figure: image17.png



Appendix Figure: image18.png



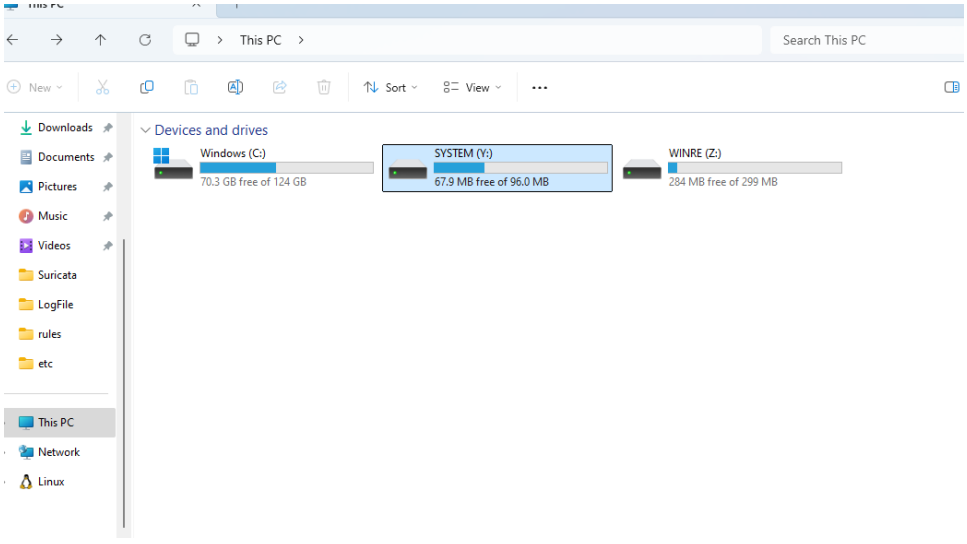
Appendix Figure: image19.png



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]1)
<__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-
l1-2-0.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

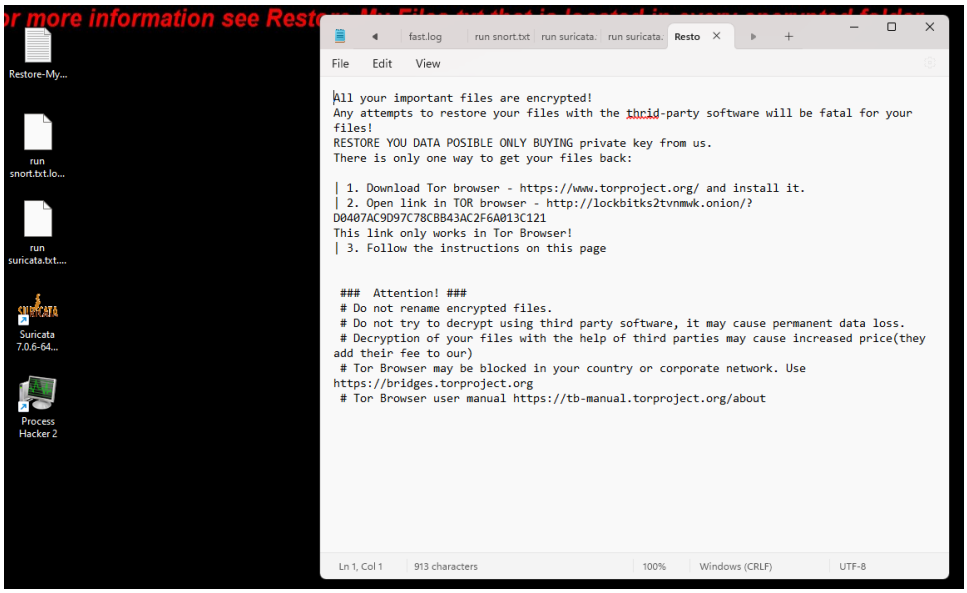


Appendix Figure: image21.png

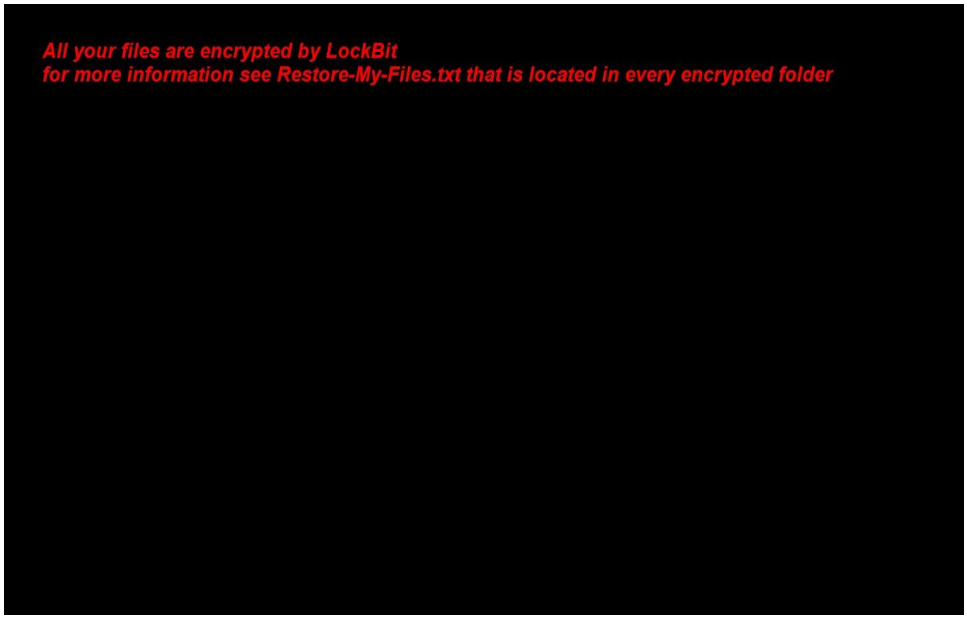
421 results.

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<<@@@@@@@@@@@@@FFFFJJJPPTT
0x5f4e37	11	000
0x5f4e4b	97	0)0,4-4.>/F0F1P2X3X7XEbOfQfRfSfUfVfWf]j^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

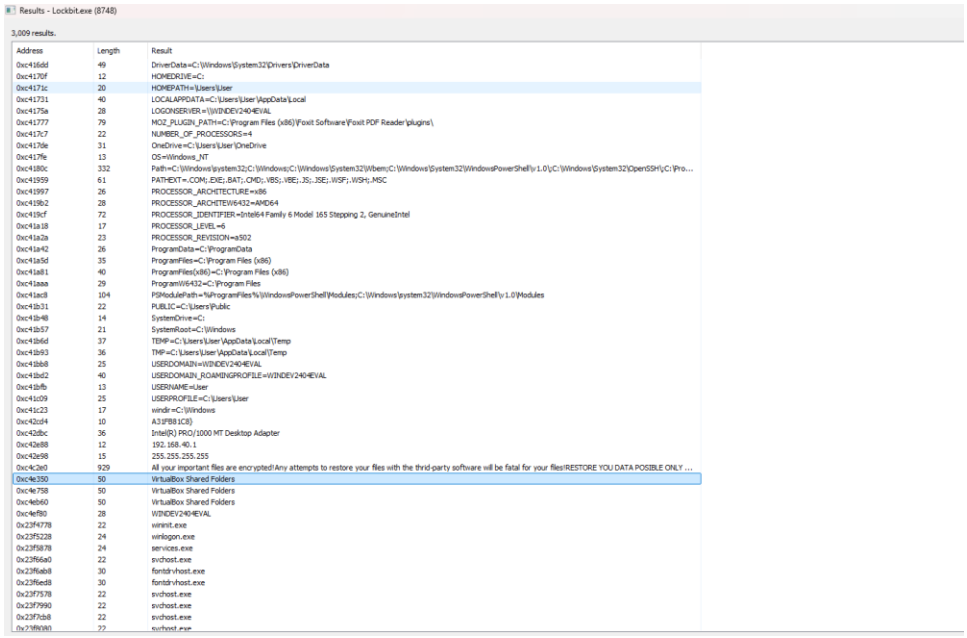
Appendix Figure: image22.png



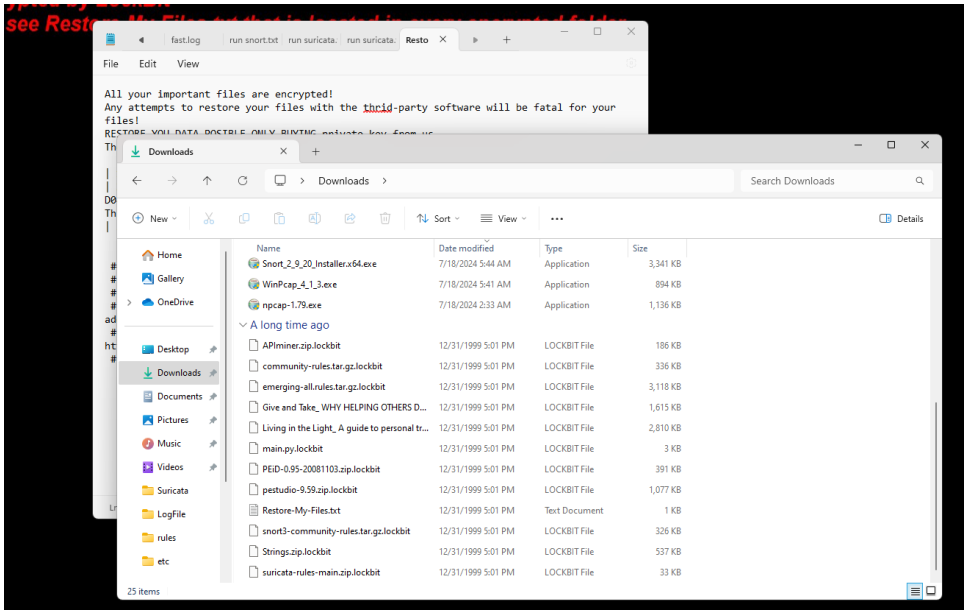
Appendix Figure: image23.png



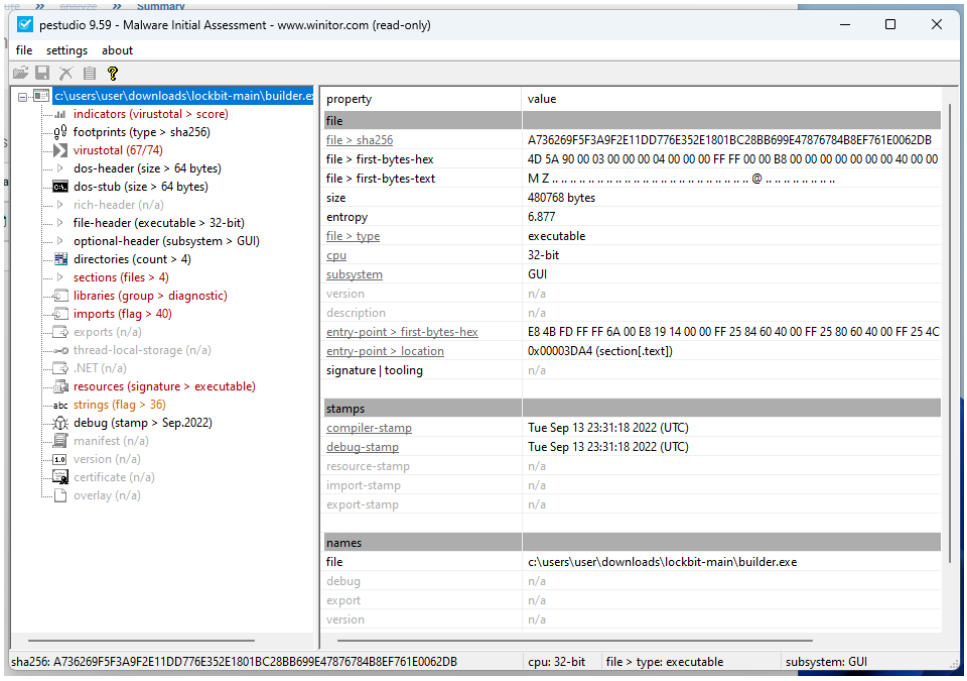
Appendix Figure: image24.png



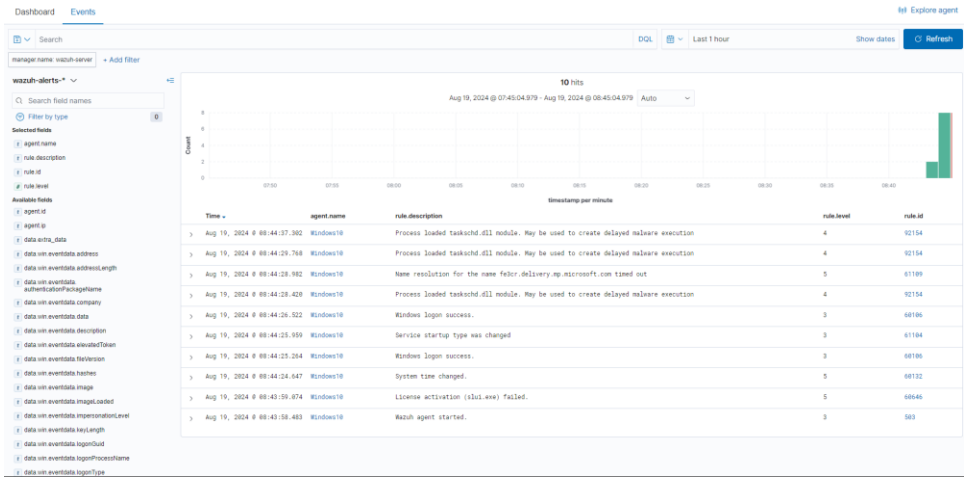
Appendix Figure: image25.png



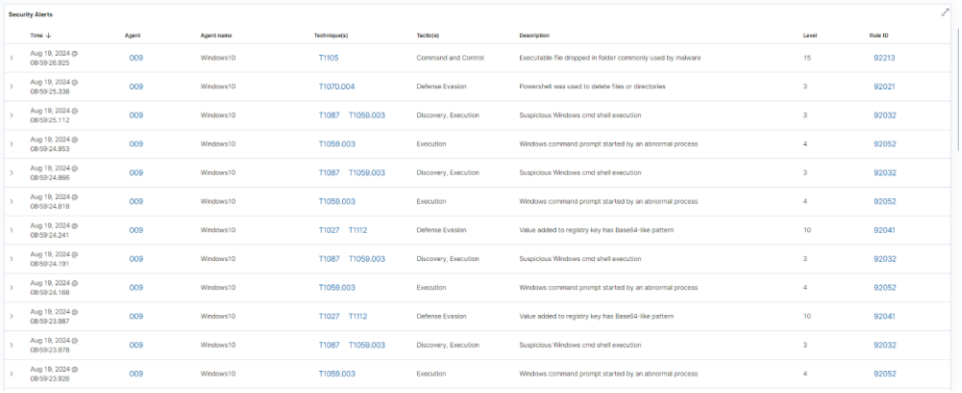
Appendix Figure: image26.png



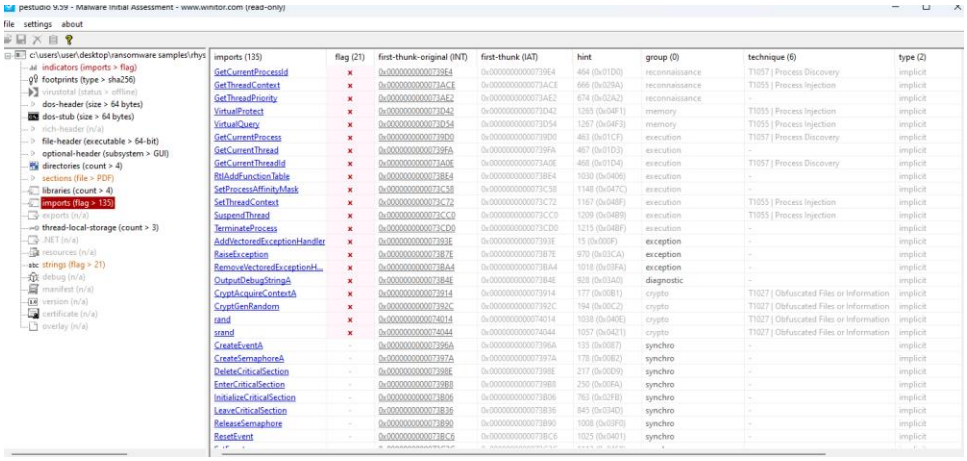
Appendix Figure: image27.png



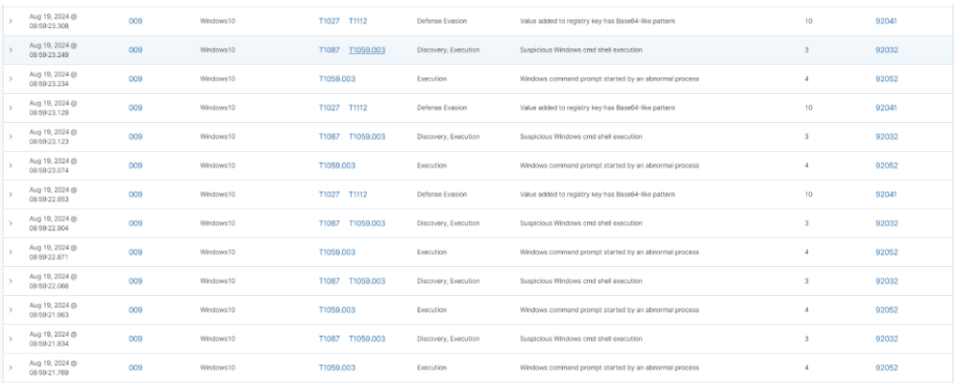
Appendix Figure: image28.png



Appendix Figure: image29.png

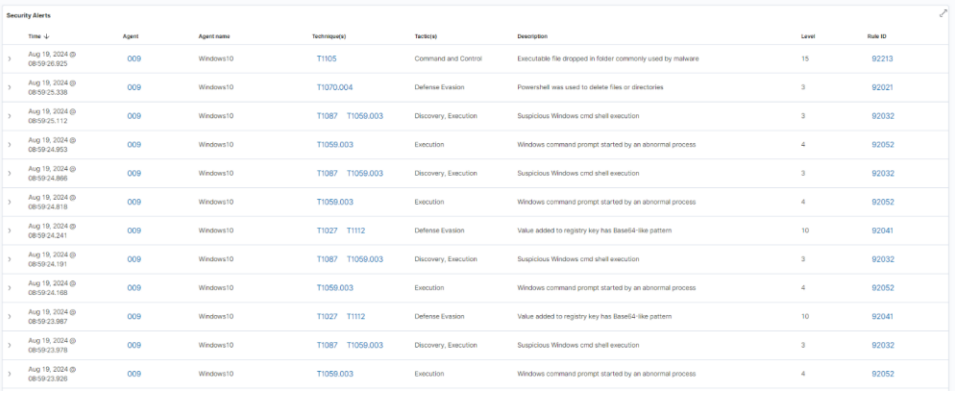


Appendix Figure: image3.png



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 @ 08:59:22.904	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 @ 08:59:22.066	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



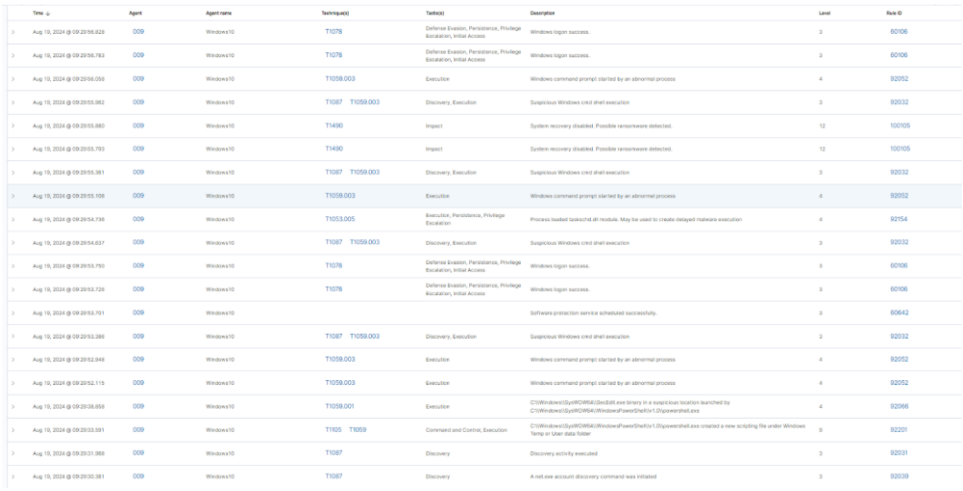
Security Alerts

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 19, 2024 @ 08:59:26.925	009	Windows10	T1105	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 @ 08:59:25.112	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 @ 08:59:24.168	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 @ 08:59:23.978	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 08:59:23.926	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052

Appendix Figure: image31.png

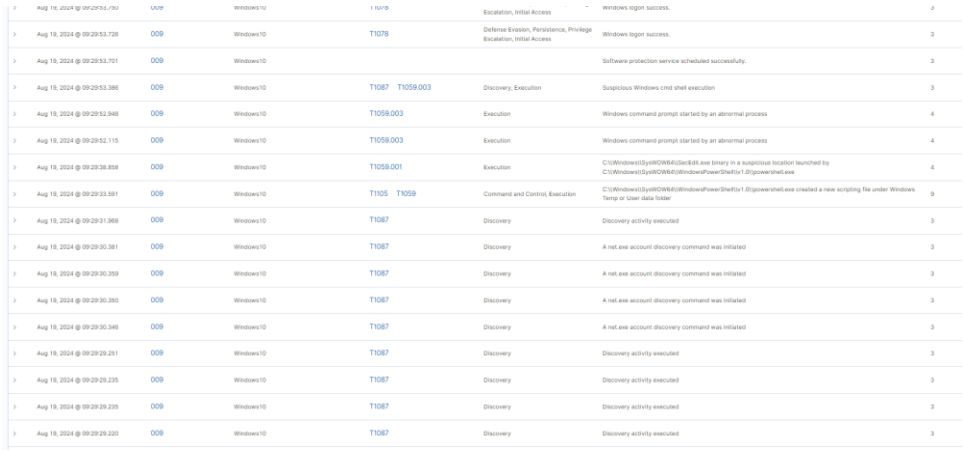
Aug 19, 2024 @ 08:59:23.308	009	Windows10	T1027 T1112	Defense Evasion	Value added to registry key has Base64-like pattern	10	92041
Aug 19, 2024 @ 08:59:23.249	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 08:59:23.234	009	Windows10	T1059.003	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 @ 08:59:22.066	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



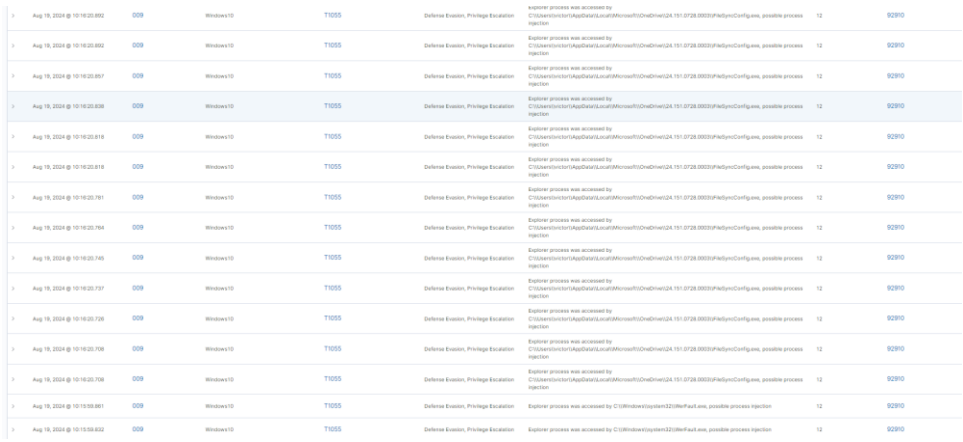
Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 19, 2024 @ 09:29:56.828	009	Windows10	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Aug 19, 2024 @ 09:29:56.783	009	Windows10	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Aug 19, 2024 @ 09:29:56.058	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:29:55.962	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:29:55.880	009	Windows10	T1490	Impact	System recovery disabled. Possible ransomware detected.	12	100105
Aug 19, 2024 @ 09:29:55.793	009	Windows10	T1490	Impact	System recovery disabled. Possible ransomware detected.	12	100105
Aug 19, 2024 @ 09:29:55.361	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:29:55.108	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:29:54.736	009	Windows10	T1053.005	Execution, Persistence, Privilege Escalation	Process loaded taskschd.dll module. May be used to create delayed malware execution	4	92154
Aug 19, 2024 @ 09:29:54.637	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:29:53.750	009	Windows10	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Aug 19, 2024 @ 09:29:53.726	009	Windows10	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Aug 19, 2024 @ 09:29:53.701	009	Windows10			Software protection service scheduled successfully.	3	60642
Aug 19, 2024 @ 09:29:53.386	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:29:52.948	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:29:52.115	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:29:38.858	009	Windows10	T1059.001	Execution	C:\\Windows\\SysWOW64\\SecEdit.exe binary in a suspicious location launched by C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe	4	92066
Aug 19, 2024 @ 09:29:33.591	009	Windows10	T1105 T1059	Command and Control, Execution	C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe created a new scripting file under Windows Temp or User data folder	9	92201
Aug 19, 2024 @ 09:29:31.968	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 19, 2024 @ 09:29:30.381	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039

Appendix Figure: image33.png



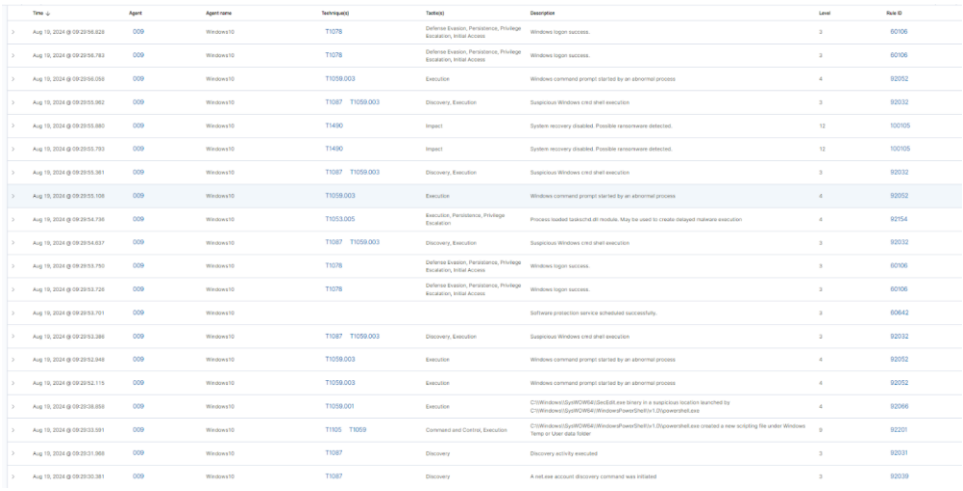
Aug 19, 2024 @ 09:29:53.726	009	Windows10	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3
Aug 19, 2024 @ 09:29:53.701	009	Windows10			Software protection service scheduled successfully.	3
Aug 19, 2024 @ 09:29:53.386	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3
Aug 19, 2024 @ 09:29:52.948	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4
Aug 19, 2024 @ 09:29:52.115	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4
Aug 19, 2024 @ 09:29:38.858	009	Windows10	T1059.001	Execution	C:\\Windows\\SysWOW64\\SecEdit.exe binary in a suspicious location launched by C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe	4
Aug 19, 2024 @ 09:29:33.591	009	Windows10	T1105 T1059	Command and Control, Execution	C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe created a new scripting file under Windows Temp or User data folder	9
Aug 19, 2024 @ 09:29:31.968	009	Windows10	T1087	Discovery	Discovery activity executed	3
Aug 19, 2024 @ 09:29:30.381	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3
Aug 19, 2024 @ 09:29:30.359	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3
Aug 19, 2024 @ 09:29:30.350	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3
Aug 19, 2024 @ 09:29:30.346	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3
Aug 19, 2024 @ 09:29:29.251	009	Windows10	T1087	Discovery	Discovery activity executed	3
Aug 19, 2024 @ 09:29:29.235	009	Windows10	T1087	Discovery	Discovery activity executed	3
Aug 19, 2024 @ 09:29:29.235	009	Windows10	T1087	Discovery	Discovery activity executed	3
Aug 19, 2024 @ 09:29:29.220	009	Windows10	T1087	Discovery	Discovery activity executed	3

Appendix Figure: image34.png



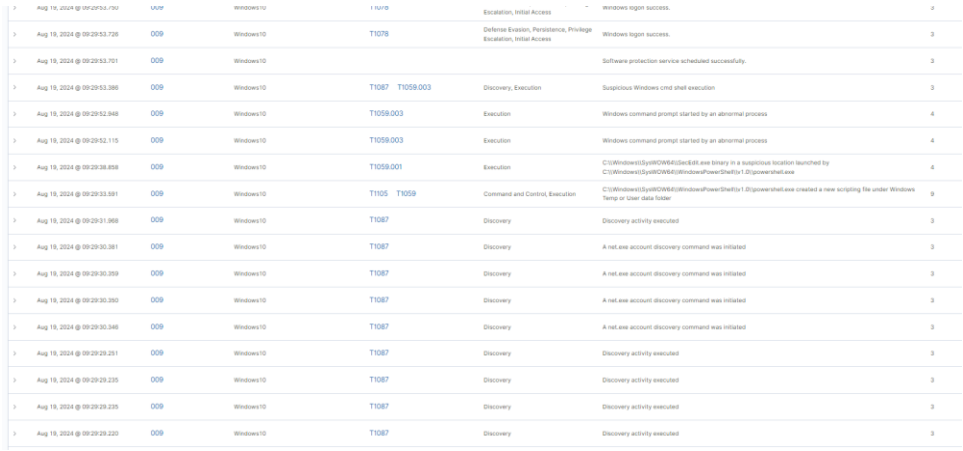
Aug 19, 2024 @ 10:16:20.892	009	Windows10	T1055	Defense Evasion, Privilege Escalation	explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.892	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.857	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.838	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.818	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.818	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.781	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.764	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.745	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.737	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.726	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.708	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.708	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:15:59.861	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Windows\\system32\\WerFault.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:15:59.832	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Windows\\system32\\WerFault.exe, possible process injection	12	92910

Appendix Figure: image35.png



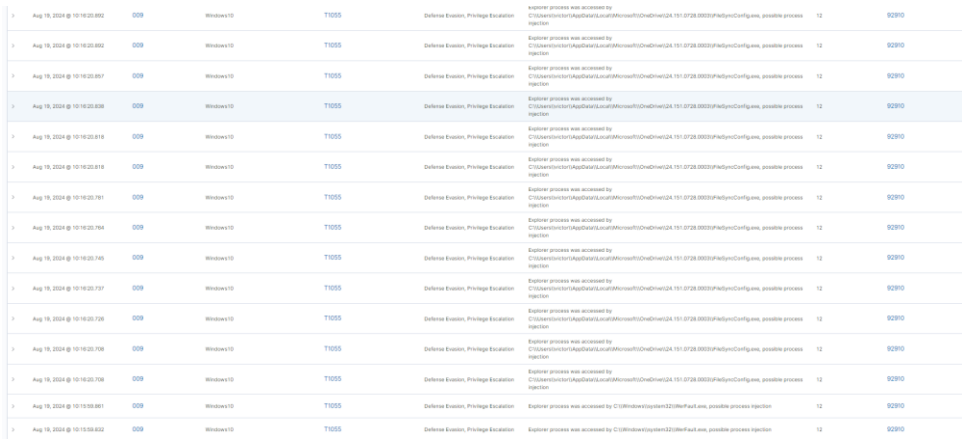
Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 19, 2024 @ 09:29:56.828	009	Windows10	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Aug 19, 2024 @ 09:29:56.783	009	Windows10	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Aug 19, 2024 @ 09:29:56.058	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:29:55.962	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:29:55.880	009	Windows10	T1490	Impact	System recovery disabled. Possible ransomware detected.	12	100105
Aug 19, 2024 @ 09:29:55.793	009	Windows10	T1490	Impact	System recovery disabled. Possible ransomware detected.	12	100105
Aug 19, 2024 @ 09:29:55.361	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:29:55.108	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:29:54.736	009	Windows10	T1053.005	Execution, Persistence, Privilege Escalation	Process loaded taskschd.dll module. May be used to create delayed malware execution	4	92154
Aug 19, 2024 @ 09:29:54.637	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:29:53.750	009	Windows10	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Aug 19, 2024 @ 09:29:53.726	009	Windows10	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Aug 19, 2024 @ 09:29:53.701	009	Windows10			Software protection service scheduled successfully.	3	60642
Aug 19, 2024 @ 09:29:53.386	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
Aug 19, 2024 @ 09:29:52.948	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:29:52.115	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4	92052
Aug 19, 2024 @ 09:29:38.858	009	Windows10	T1059.001	Execution	C:\\Windows\\SysWOW64\\SecEdit.exe binary in a suspicious location launched by C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe	4	92066
Aug 19, 2024 @ 09:29:33.591	009	Windows10	T1105 T1059	Command and Control, Execution	C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe created a new scripting file under Windows Temp or User data folder	9	92201
Aug 19, 2024 @ 09:29:31.968	009	Windows10	T1087	Discovery	Discovery activity executed	3	92031
Aug 19, 2024 @ 09:29:30.381	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3	92039

Appendix Figure: image36.png



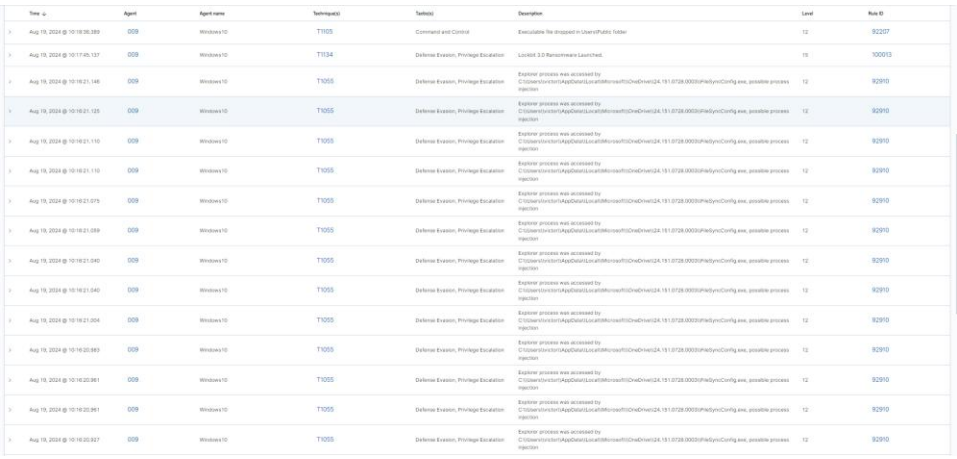
Aug 19, 2024 @ 09:29:53.750	009	Windows10	T1078	Escalation, Initial Access	Windows logon success.	3
Aug 19, 2024 @ 09:29:53.726	009	Windows10	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3
Aug 19, 2024 @ 09:29:53.701	009	Windows10			Software protection service scheduled successfully.	3
Aug 19, 2024 @ 09:29:53.386	009	Windows10	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3
Aug 19, 2024 @ 09:29:52.948	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4
Aug 19, 2024 @ 09:29:52.115	009	Windows10	T1059.003	Execution	Windows command prompt started by an abnormal process	4
Aug 19, 2024 @ 09:29:38.858	009	Windows10	T1059.001	Execution	C:\\Windows\\SysWOW64\\SecEdit.exe binary in a suspicious location launched by C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe	4
Aug 19, 2024 @ 09:29:33.591	009	Windows10	T1105 T1059	Command and Control, Execution	C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe created a new scripting file under Windows Temp or User data folder	9
Aug 19, 2024 @ 09:29:31.968	009	Windows10	T1087	Discovery	Discovery activity executed	3
Aug 19, 2024 @ 09:29:30.381	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3
Aug 19, 2024 @ 09:29:30.359	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3
Aug 19, 2024 @ 09:29:30.350	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3
Aug 19, 2024 @ 09:29:30.346	009	Windows10	T1087	Discovery	A net.exe account discovery command was initiated	3
Aug 19, 2024 @ 09:29:29.251	009	Windows10	T1087	Discovery	Discovery activity executed	3
Aug 19, 2024 @ 09:29:29.235	009	Windows10	T1087	Discovery	Discovery activity executed	3
Aug 19, 2024 @ 09:29:29.235	009	Windows10	T1087	Discovery	Discovery activity executed	3
Aug 19, 2024 @ 09:29:29.220	009	Windows10	T1087	Discovery	Discovery activity executed	3

Appendix Figure: image37.png

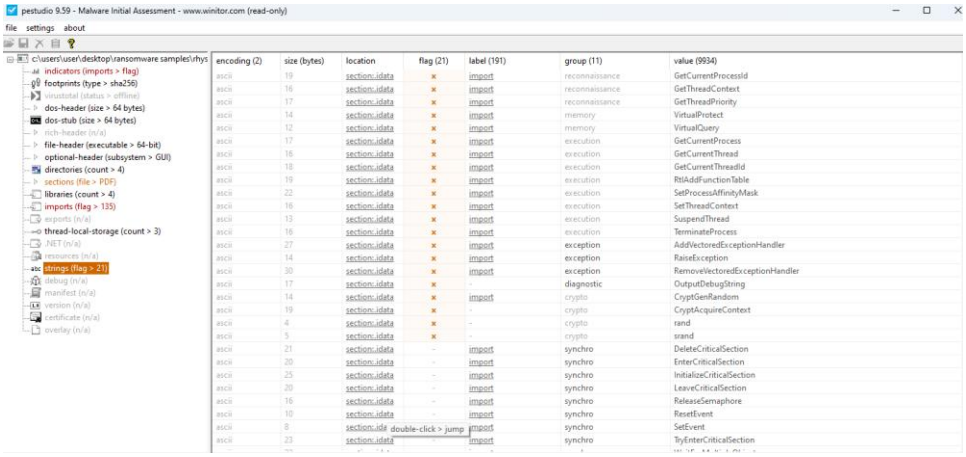


Aug 19, 2024 @ 10:16:20.892	009	Windows10	T1055	Defense Evasion, Privilege Escalation	explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.892	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.857	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.838	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.818	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.818	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.781	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.764	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.745	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.737	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.726	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.708	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:16:20.708	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Users\\victor\\AppData\\Local\\Microsoft\\OneDrive\\24.151.0728.0003\\FileSyncConfig.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:15:59.861	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Windows\\system32\\WerFault.exe, possible process injection	12	92910
Aug 19, 2024 @ 10:15:59.832	009	Windows10	T1055	Defense Evasion, Privilege Escalation	Explorer process was accessed by C:\\Windows\\system32\\WerFault.exe, possible process injection	12	92910

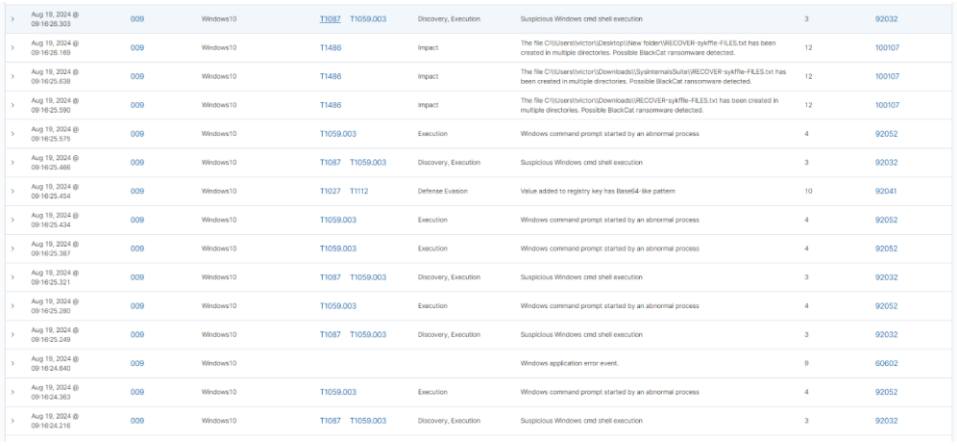
Appendix Figure: image38.png



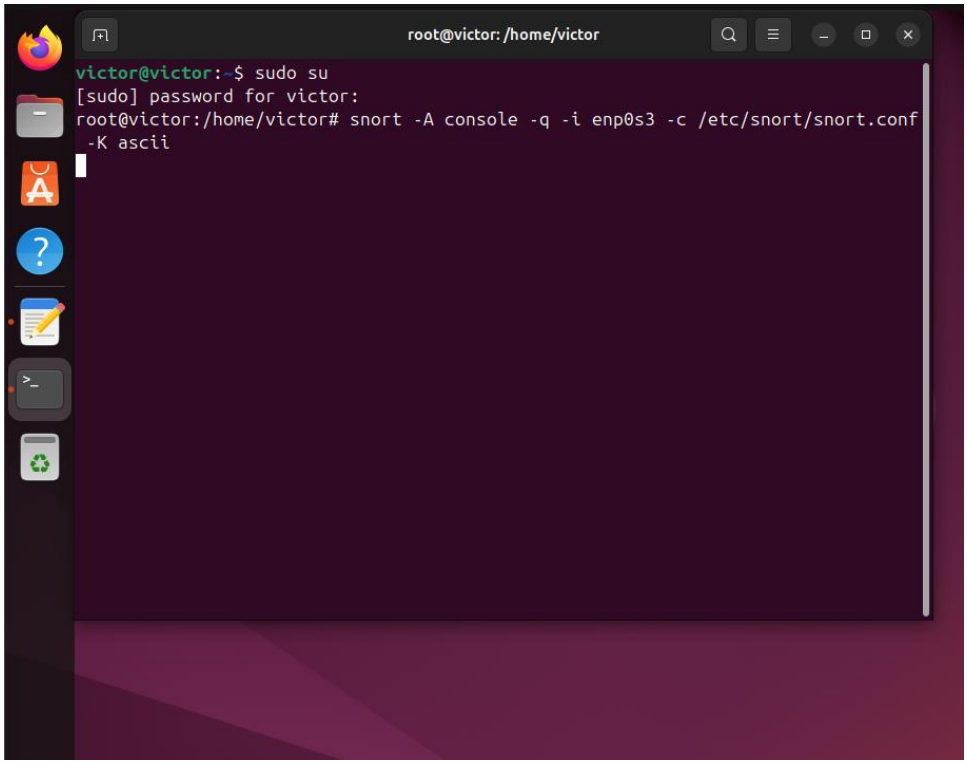
Appendix Figure: image39.png



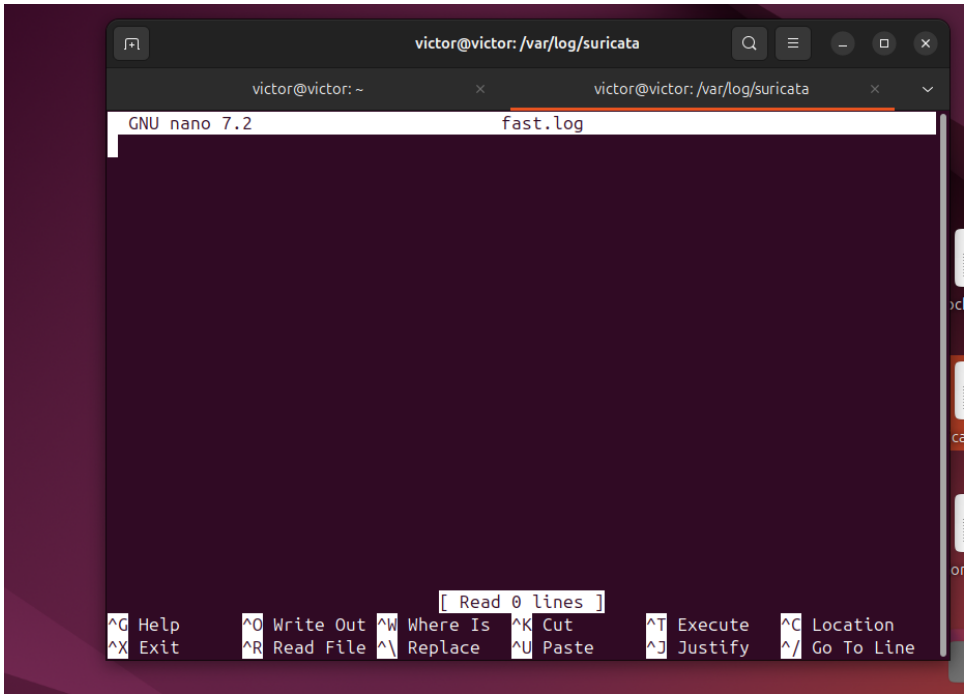
Appendix Figure: image4.png



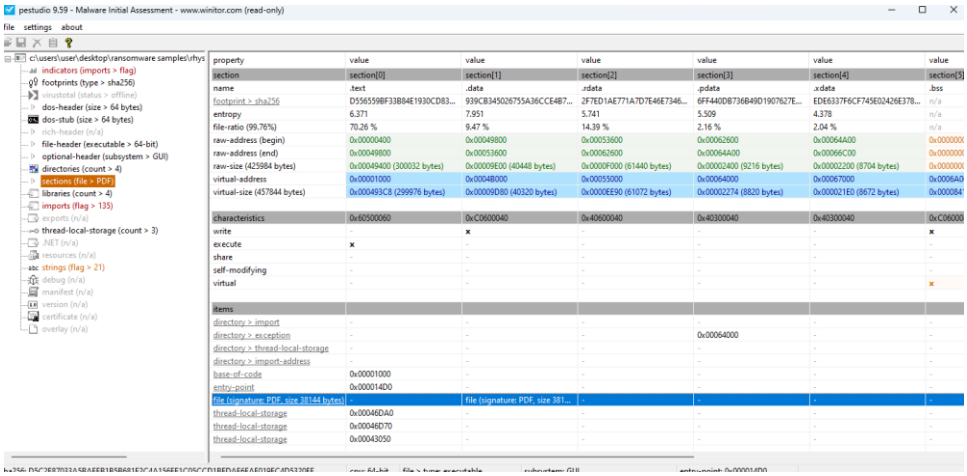
Appendix Figure: image40.png



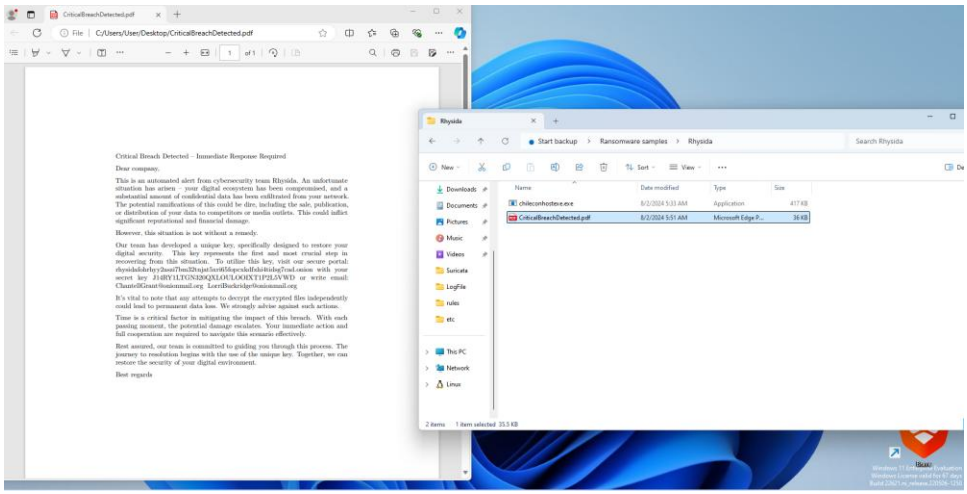
Appendix Figure: image41.png



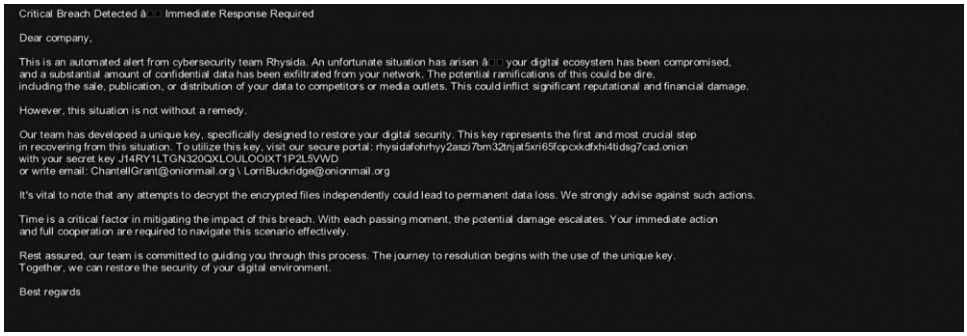
Appendix Figure: image42.png



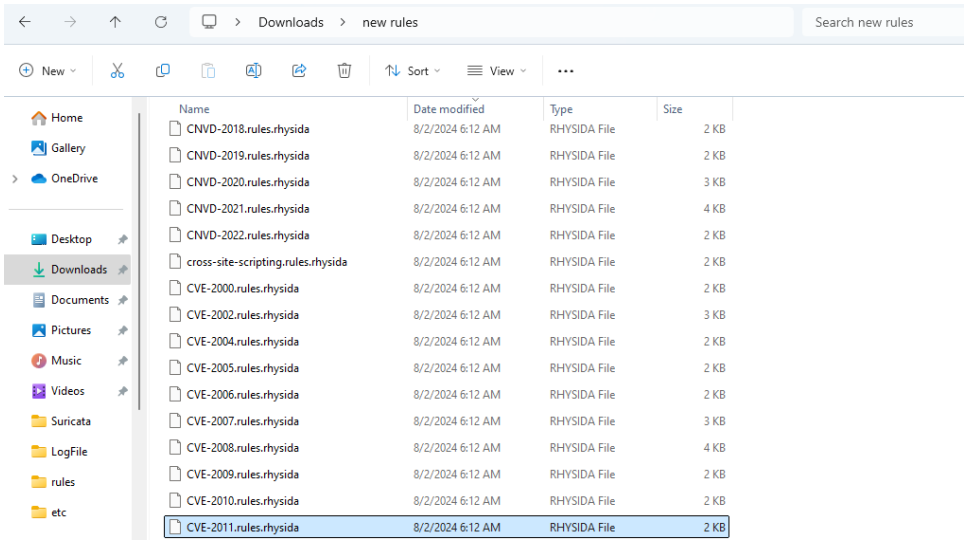
Appendix Figure: image5.png



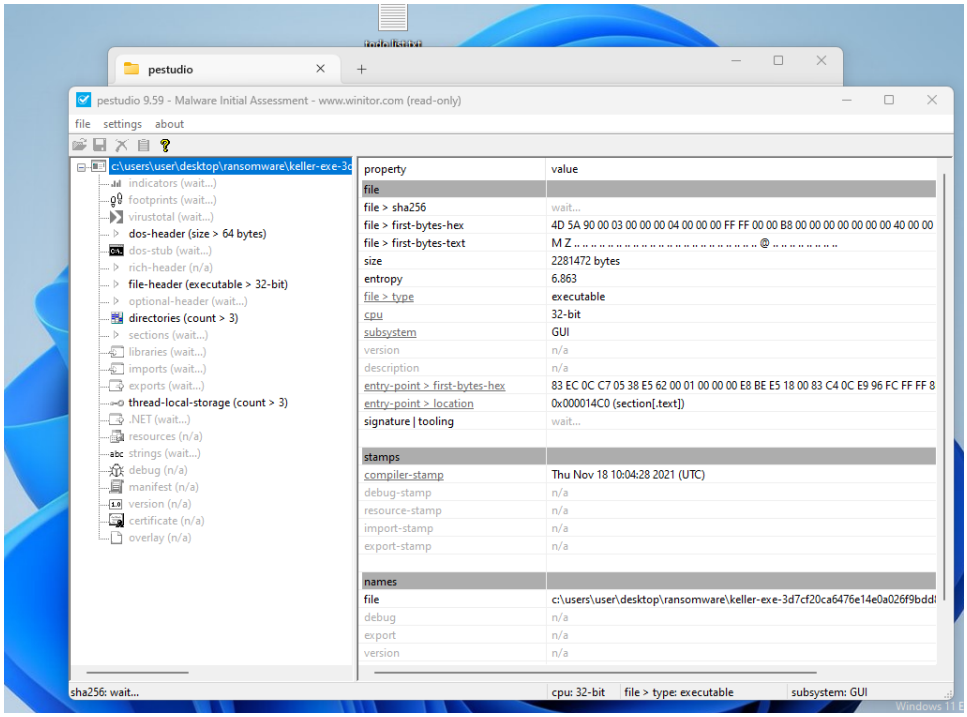
Appendix Figure: image6.png



Appendix Figure: image7.png



Appendix Figure: image8.png



Appendix Figure: image9.png