Malware Analysis Report

LOCKBIT 3.0 Ransomware

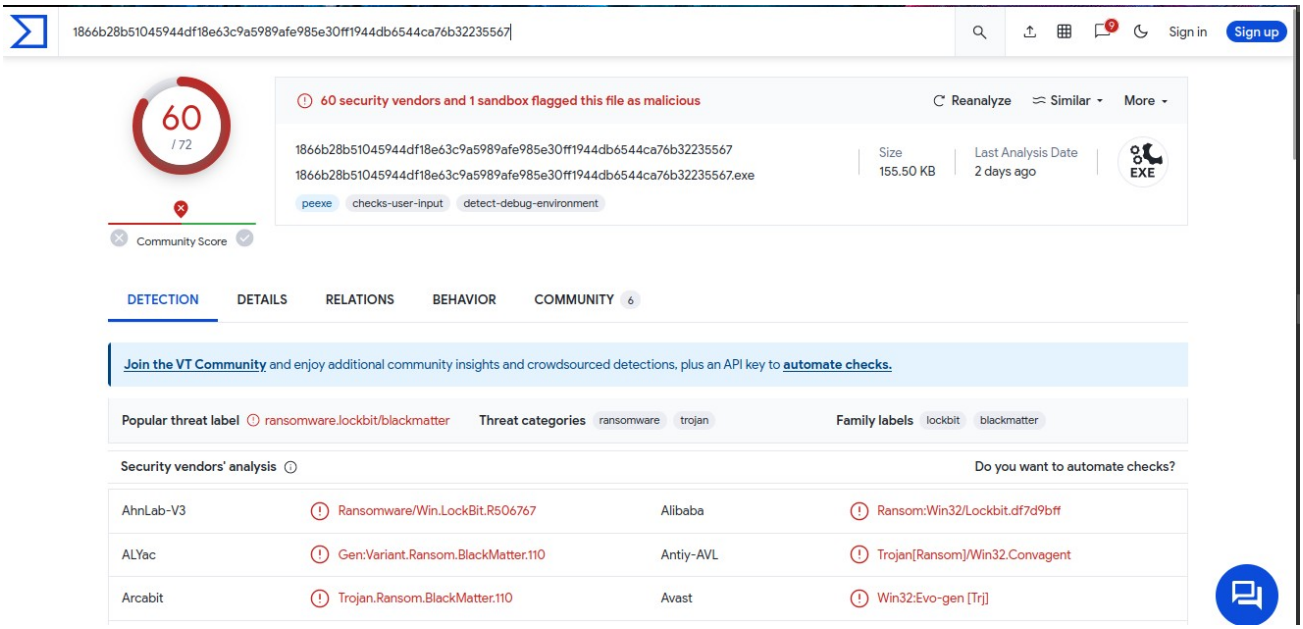
By: Yusuf Amr

Table of Content

Executive Summar

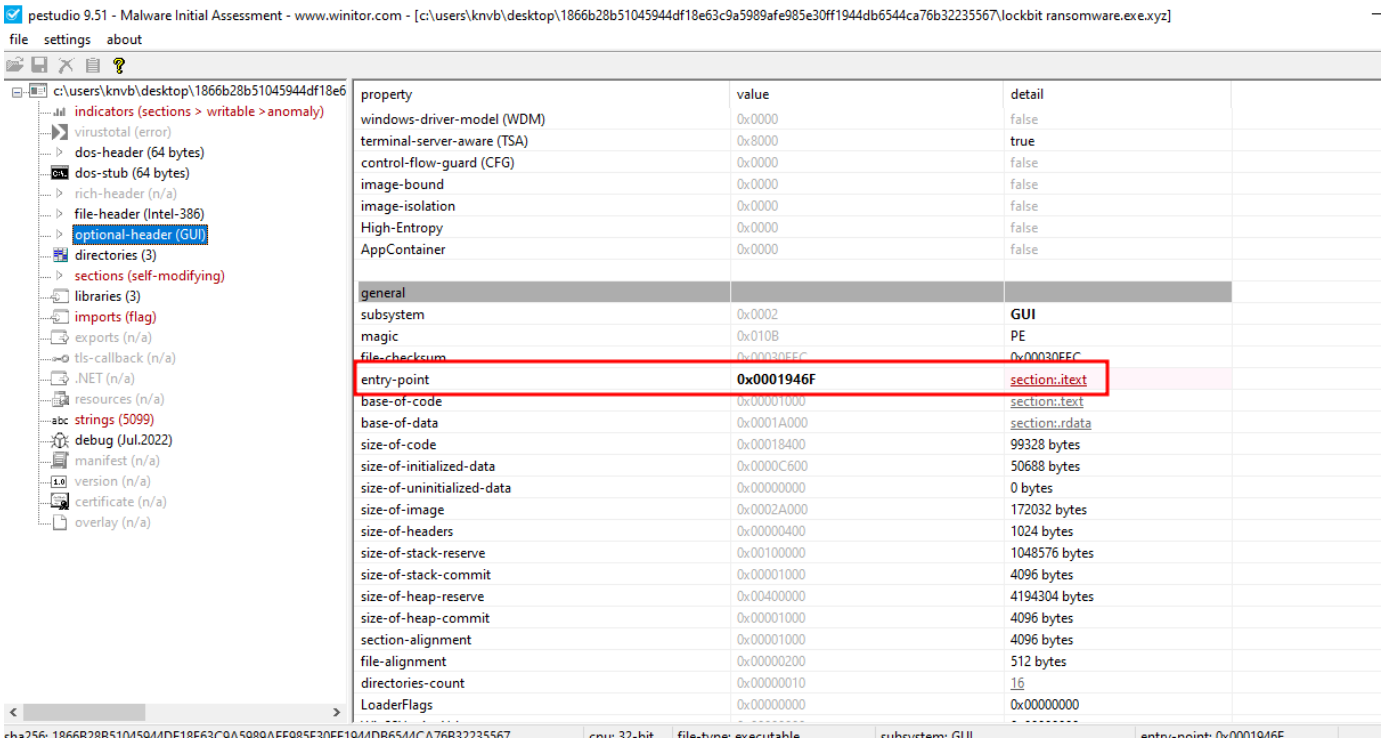
MD5 Hash	7f58f9289043b2a83499feccfb99d540
SHA1 Hash	E56759E391B3C03D2EF739CF3CF12B9B694AEADE
SHA256 Hash	1866B28B51045944DF18E63C9A5989AFE985E30FF1944DB6544CA76B32235567

LockBit 3.0 is a sophisticated ransomware that has been identified as a significant threat to organizations worldwide. This ransomware variant is designed to encrypt files on infected systems, rendering them inaccessible until a ransom is paid. LockBit 3.0 is known for its advanced encryption techniques, which make it difficult to decrypt files without the decryption key. The ransomware is typically distributed through phishing emails or malicious websites, and once it infects a system, it spreads rapidly through the network, encrypting files on all connected devices. LockBit 3.0 is also capable of evading detection by traditional antivirus software, making it a particularly dangerous threat.

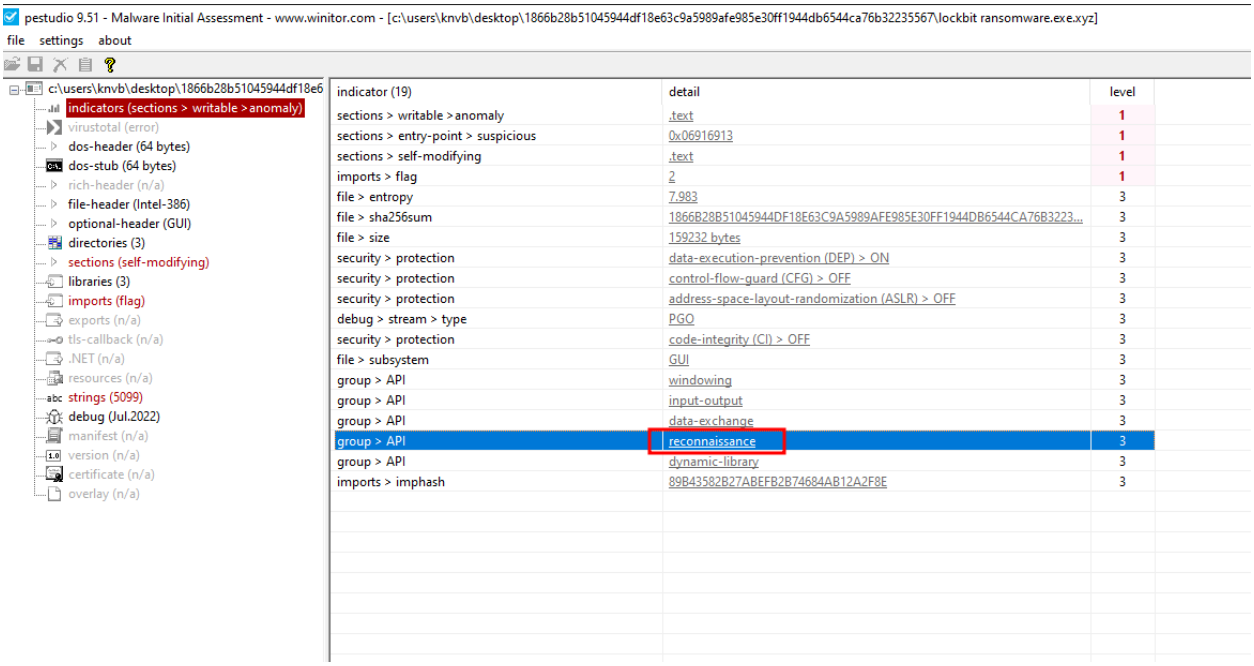


Technical Analysis

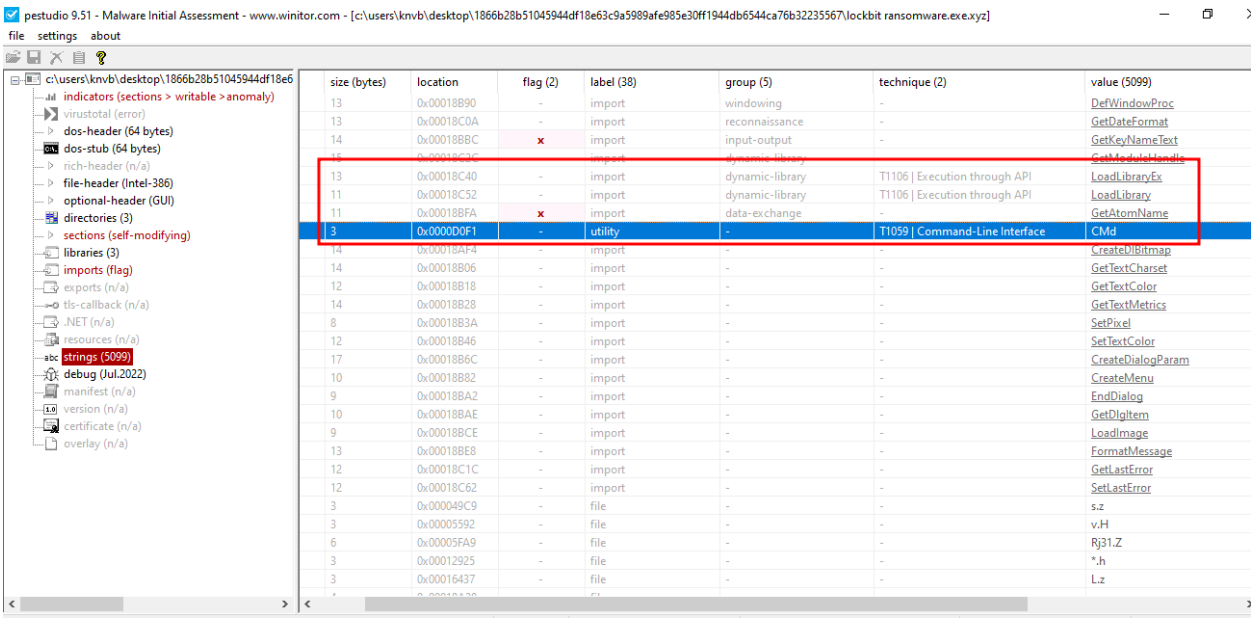
By performing intial inspection of the sample shows signs of malicious activity. the entry point is found within the '.itext' section, which is highly suspicious.



utilizing a set of APIs for reconnaissance purposes.

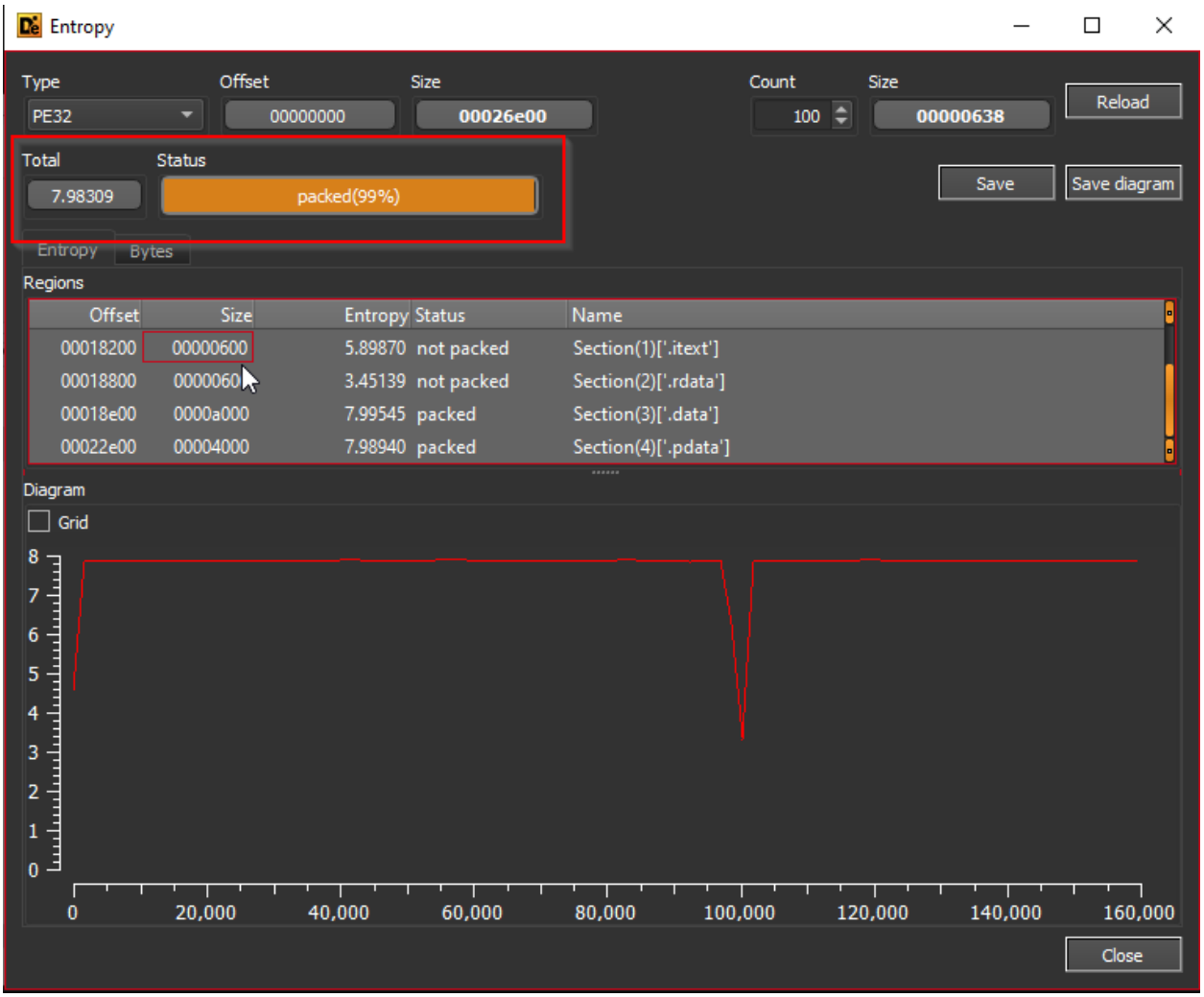


Several library imports and strings appear to be suspicious.



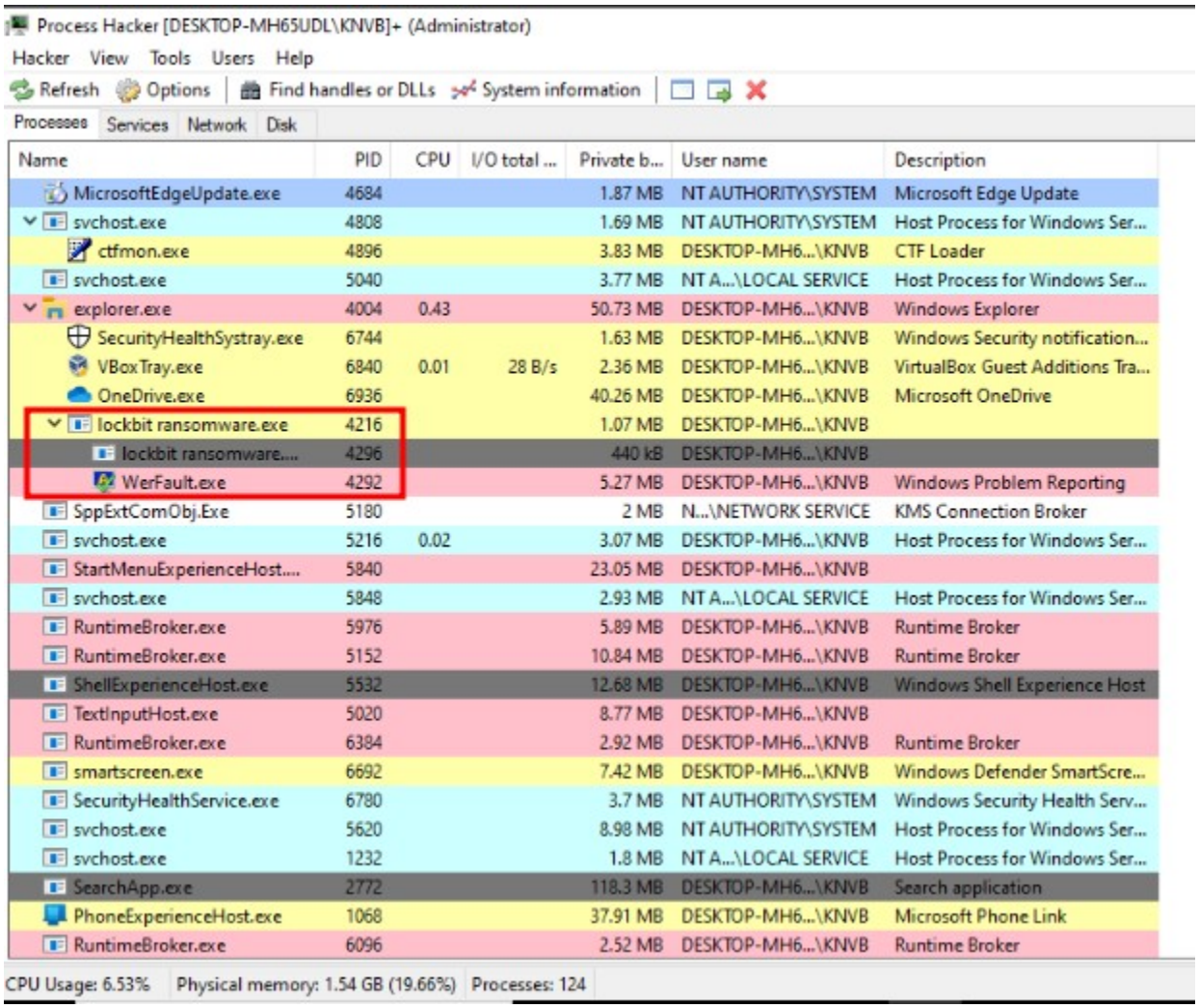
Technical Analysis

Sample is packed as shown below:



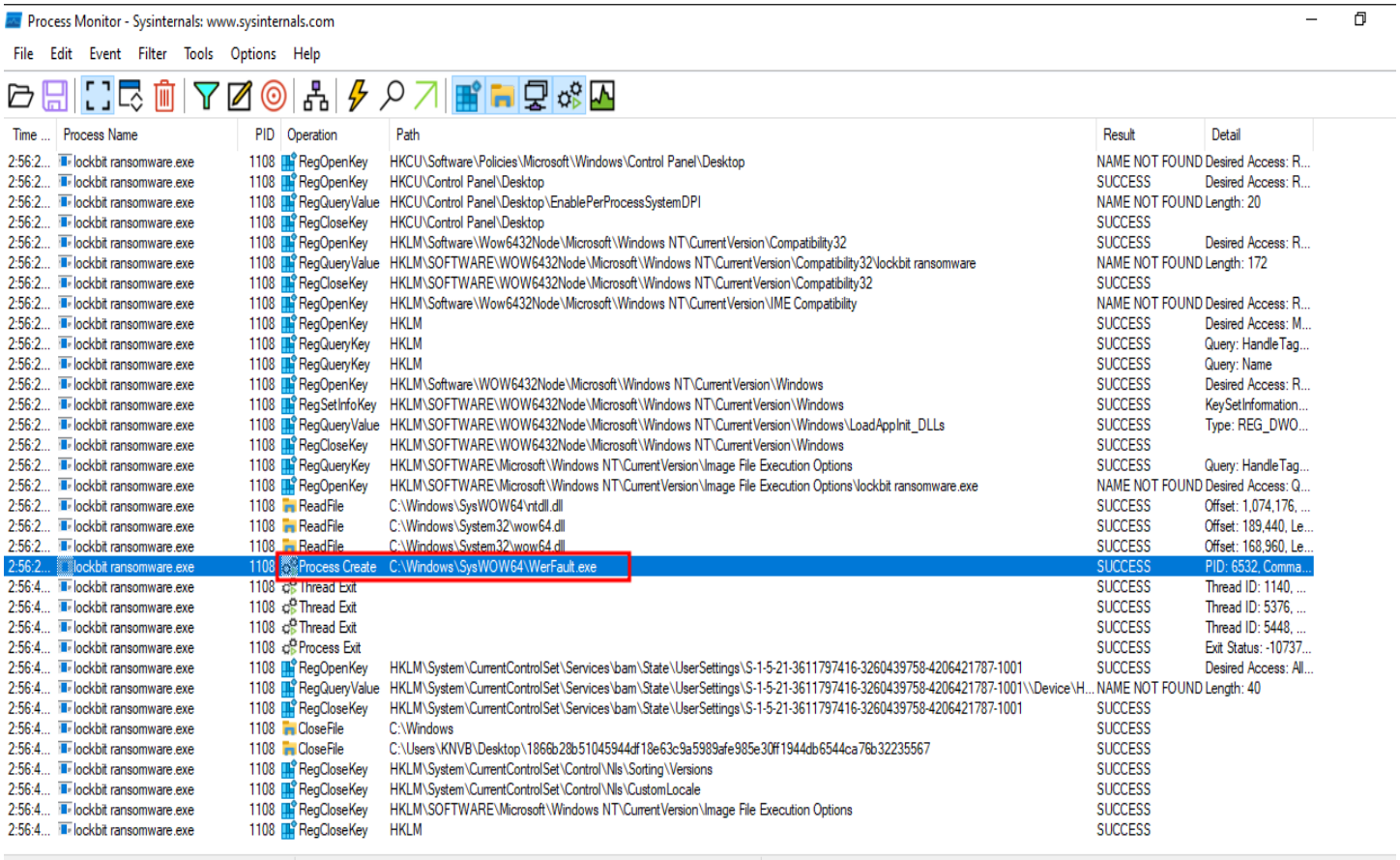
Technical Analysis

After the detonation of the malware sample, a 'WerFault.exe' process briefly appears under the ransomware process for a few seconds before disappearing.



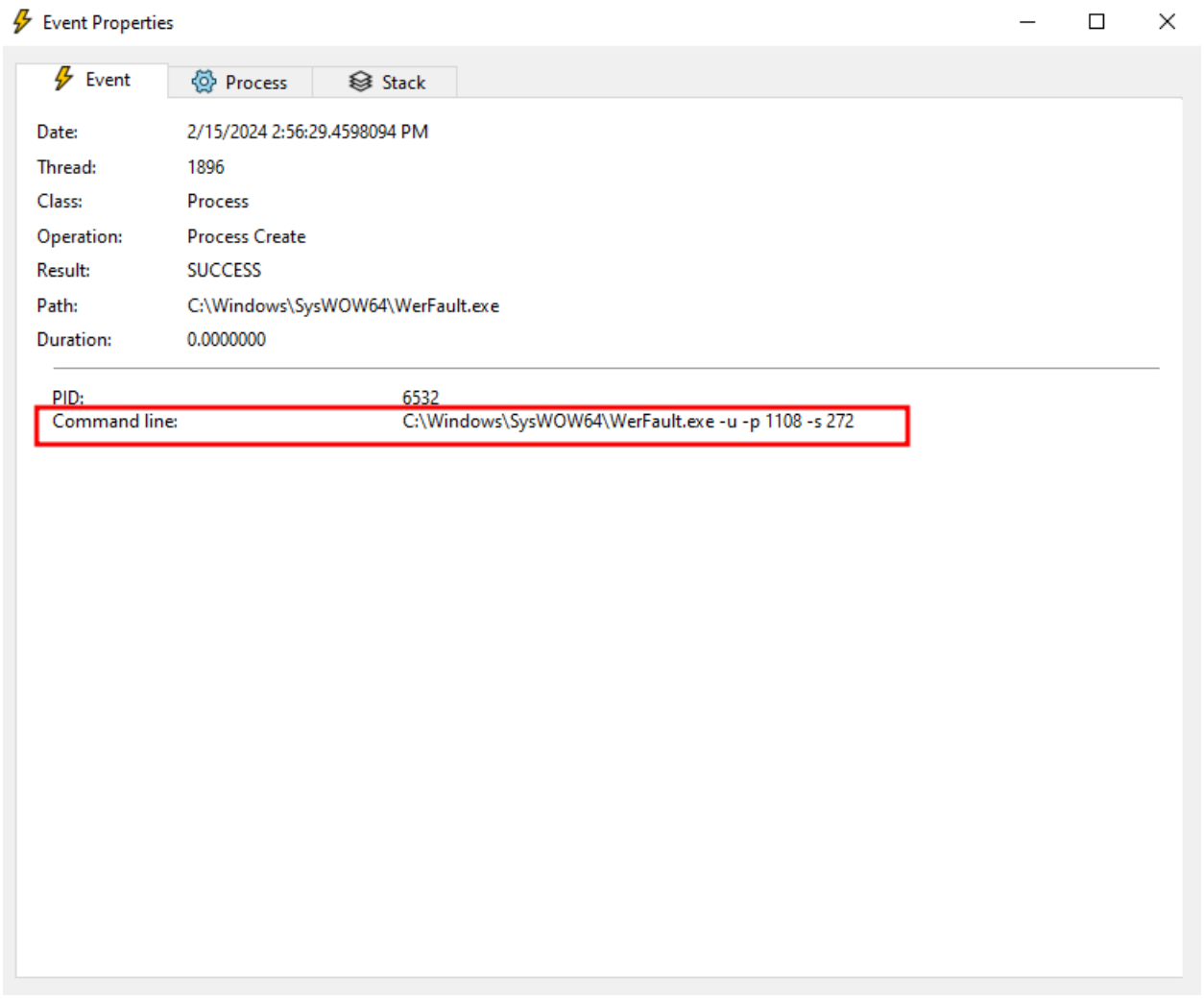
Technical Analysis

By abusing the Windows Problem Reporting (WerFault.exe) error reporting tool, the ransomware is able to stealthily infect devices without raising any alarms on the breached system. This is achieved by launching the malware through a legitimate Windows executable.



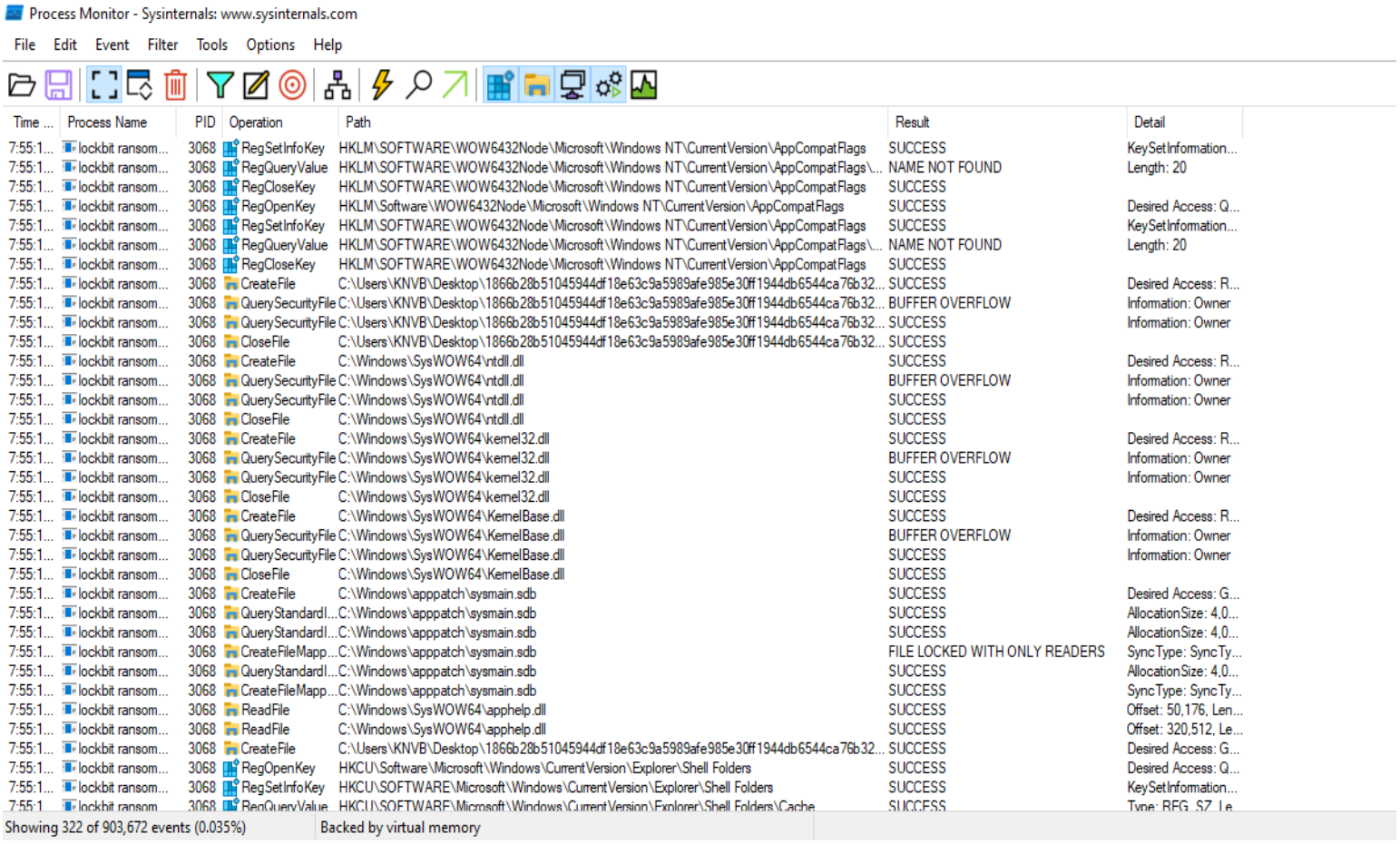
Time ...	Process Name	PID	Operation	Path	Result	Detail
2:56:2...	lockbit ransomware.exe	1108	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: R...
2:56:2...	lockbit ransomware.exe	1108	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: R...
2:56:2...	lockbit ransomware.exe	1108	RegQueryValue	HKCU\Control Panel\Desktop\EnablePerProcessSystemDPI	NAME NOT FOUND	Length: 20
2:56:2...	lockbit ransomware.exe	1108	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
2:56:2...	lockbit ransomware.exe	1108	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS	Desired Access: R...
2:56:2...	lockbit ransomware.exe	1108	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32\lockbit ransomware	NAME NOT FOUND	Length: 172
2:56:2...	lockbit ransomware.exe	1108	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS	
2:56:2...	lockbit ransomware.exe	1108	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\IME Compatibility	NAME NOT FOUND	Desired Access: R...
2:56:2...	lockbit ransomware.exe	1108	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
2:56:2...	lockbit ransomware.exe	1108	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:56:2...	lockbit ransomware.exe	1108	RegQueryKey	HKLM	SUCCESS	Query: Name
2:56:2...	lockbit ransomware.exe	1108	RegOpenKey	HKLM\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS	Desired Access: R...
2:56:2...	lockbit ransomware.exe	1108	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS	KeySetInformation...
2:56:2...	lockbit ransomware.exe	1108	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs	SUCCESS	Type: REG_DWO...
2:56:2...	lockbit ransomware.exe	1108	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS	
2:56:2...	lockbit ransomware.exe	1108	RegQueryKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	Query: HandleTag...
2:56:2...	lockbit ransomware.exe	1108	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\lockbit ransomware.exe	NAME NOT FOUND	Desired Access: Q...
2:56:2...	lockbit ransomware.exe	1108	ReadFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Offset: 1,074,176, ...
2:56:2...	lockbit ransomware.exe	1108	ReadFile	C:\Windows\System32\wow64.dll	SUCCESS	Offset: 189,440, Le...
2:56:2...	lockbit ransomware.exe	1108	ReadFile	C:\Windows\System32\wow64.dll	SUCCESS	Offset: 168,960, Le...
2:56:2...	lockbit ransomware.exe	1108	Process Create	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	PID: 6532, Comma...
2:56:4...	lockbit ransomware.exe	1108	Thread Exit		SUCCESS	Thread ID: 1140, ...
2:56:4...	lockbit ransomware.exe	1108	Thread Exit		SUCCESS	Thread ID: 5376, ...
2:56:4...	lockbit ransomware.exe	1108	Thread Exit		SUCCESS	Thread ID: 5448, ...
2:56:4...	lockbit ransomware.exe	1108	Process Exit		SUCCESS	Exit Status: -10737...
2:56:4...	lockbit ransomware.exe	1108	RegOpenKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3611797416-3260439758-4206421787-1001	SUCCESS	Desired Access: All...
2:56:4...	lockbit ransomware.exe	1108	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3611797416-3260439758-4206421787-1001\\Device\H...	NAME NOT FOUND	Length: 40
2:56:4...	lockbit ransomware.exe	1108	RegCloseKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3611797416-3260439758-4206421787-1001	SUCCESS	
2:56:4...	lockbit ransomware.exe	1108	CloseFile	C:\Windows	SUCCESS	
2:56:4...	lockbit ransomware.exe	1108	CloseFile	C:\Users\KNVB\Desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32235567	SUCCESS	
2:56:4...	lockbit ransomware.exe	1108	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	
2:56:4...	lockbit ransomware.exe	1108	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\CustomLocale	SUCCESS	
2:56:4...	lockbit ransomware.exe	1108	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	
2:56:4...	lockbit ransomware.exe	1108	RegCloseKey	HKLM	SUCCESS	

Technical Analysis



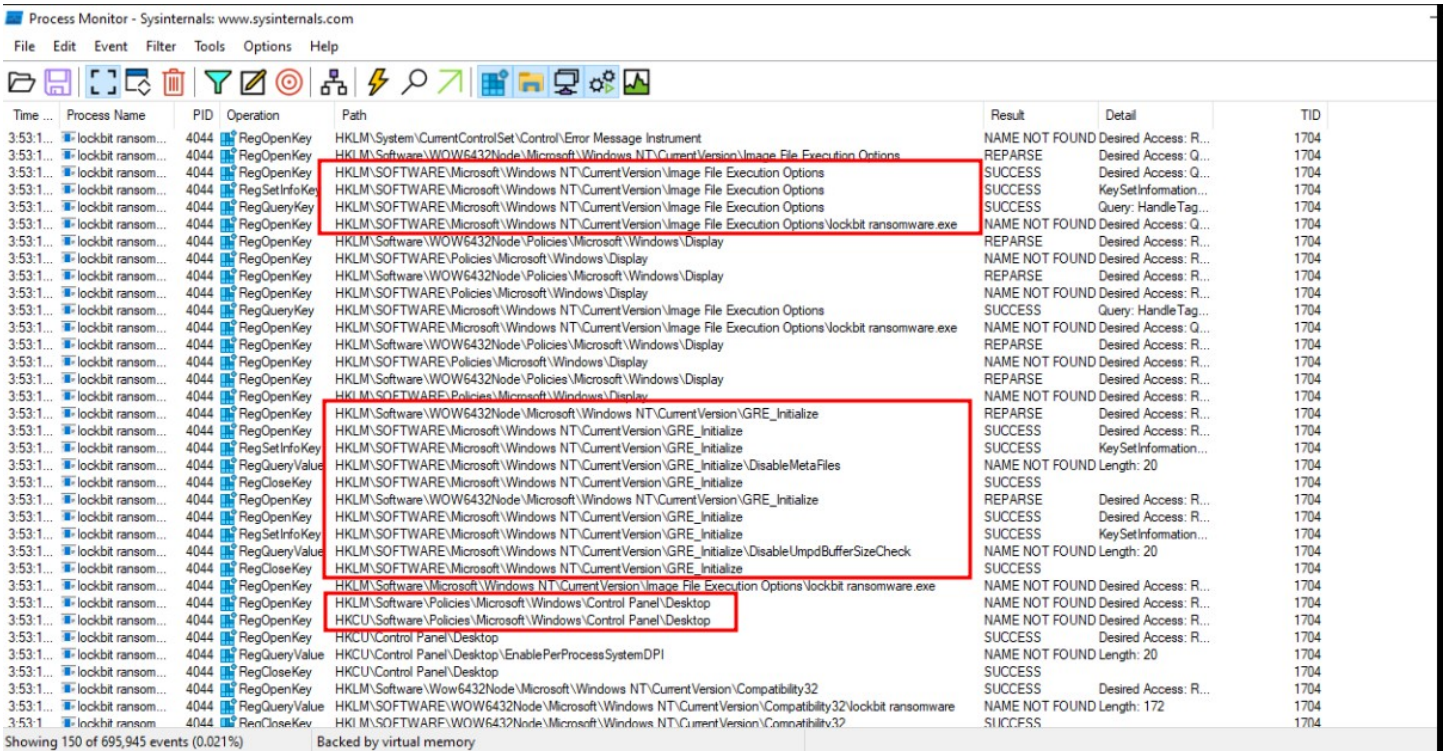
Technical Analysis

buffer overflow exceptions were encountered during the process of reading file attributes:



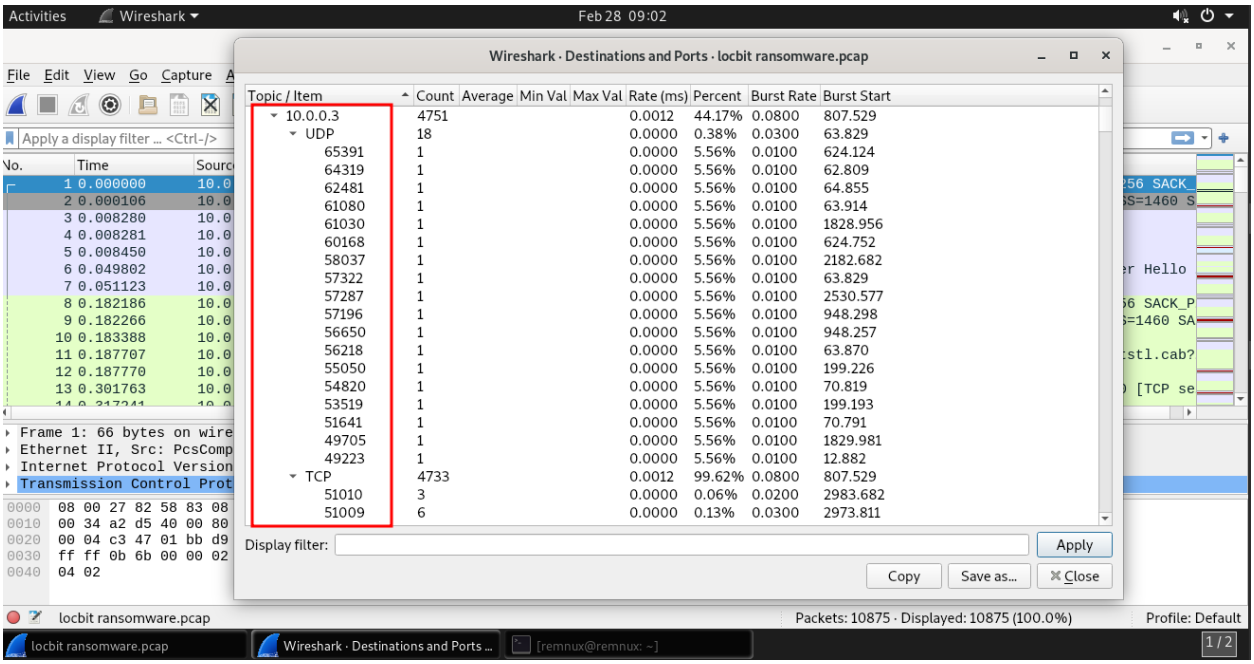
Technical Analysis

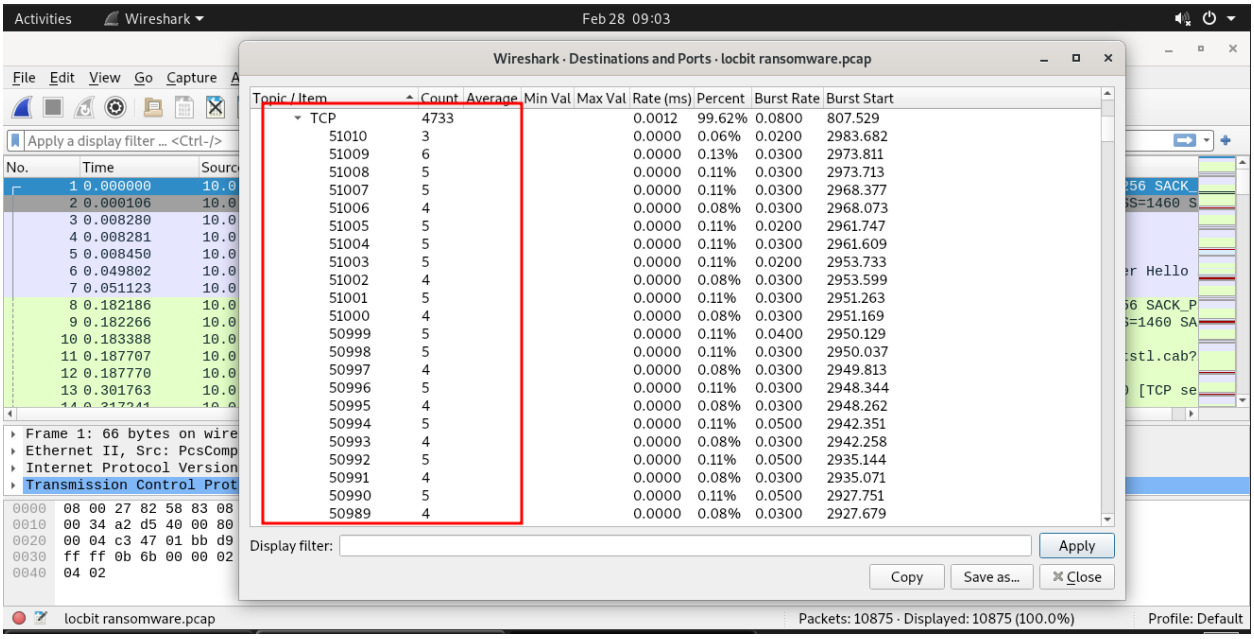
Typical ransomware behavior includes accessing system registers, such as those related to Desktop settings and shell folders.



Technical Analysis

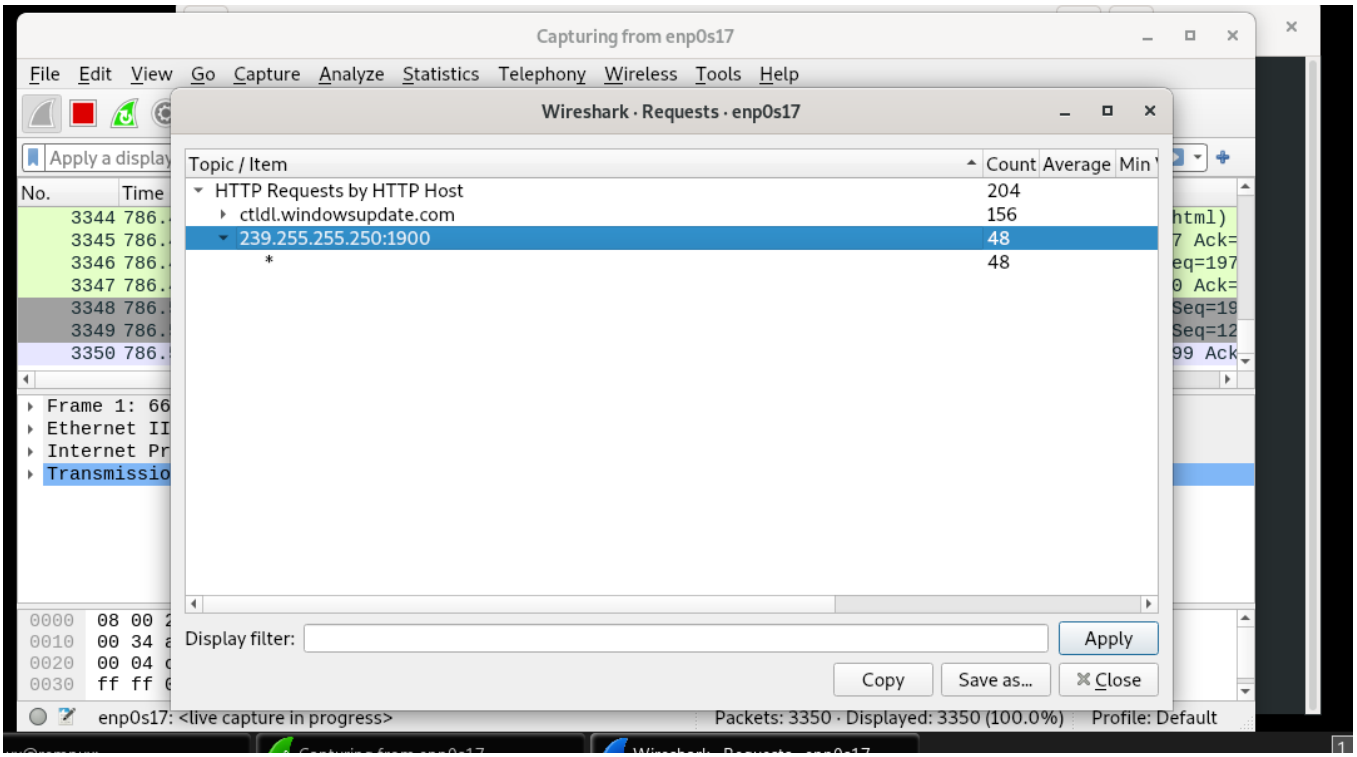
After analyzing the network traffic using Wireshark, it shows that the ransomware sample initiated a port scanning activity on the infected host

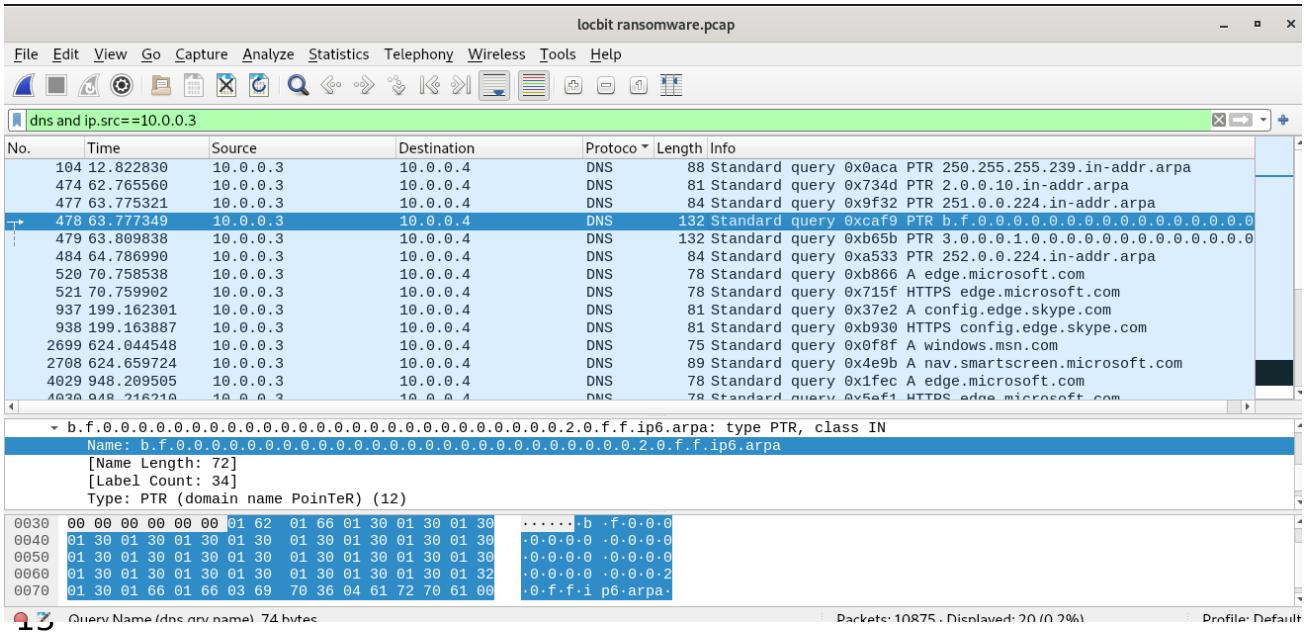




Technical Analysis

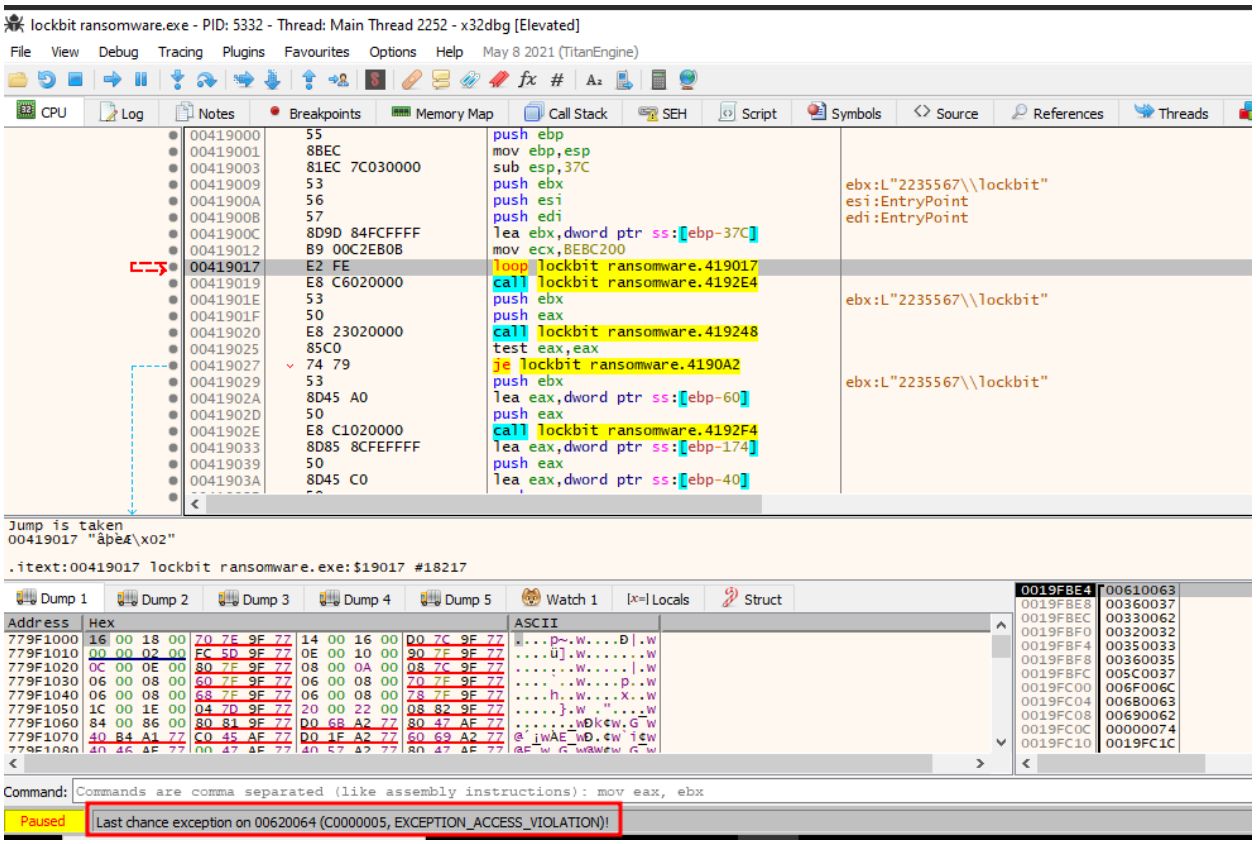
Additionally, there are no external connections to any public IP addresses or DNS queries to a command-and-control (C2C) server, which confirms the static analysis we conducted earlier, indicating that the first stage of the malware is focused on reconnaissance.





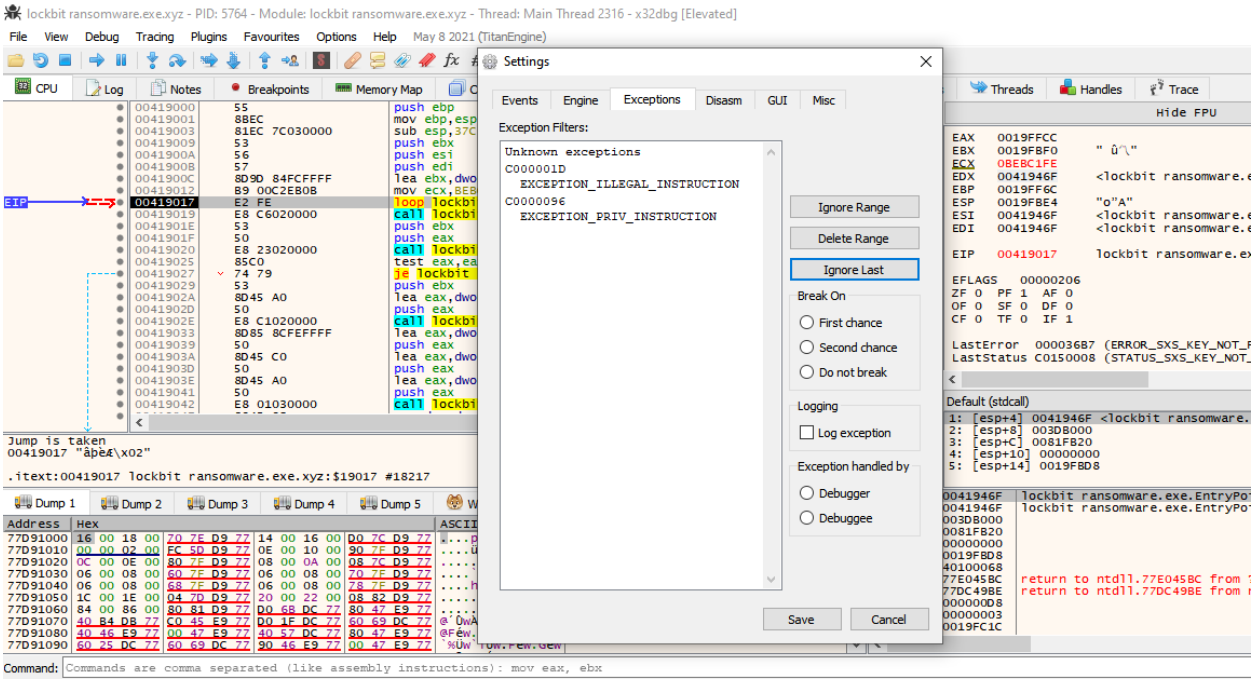
Technical Analysis

The malware employs a debugger evasion technique known as 'Exception Flooding.' The sample contains a significant number of function calls designed to cause a denial of service (DoS) on a debugger



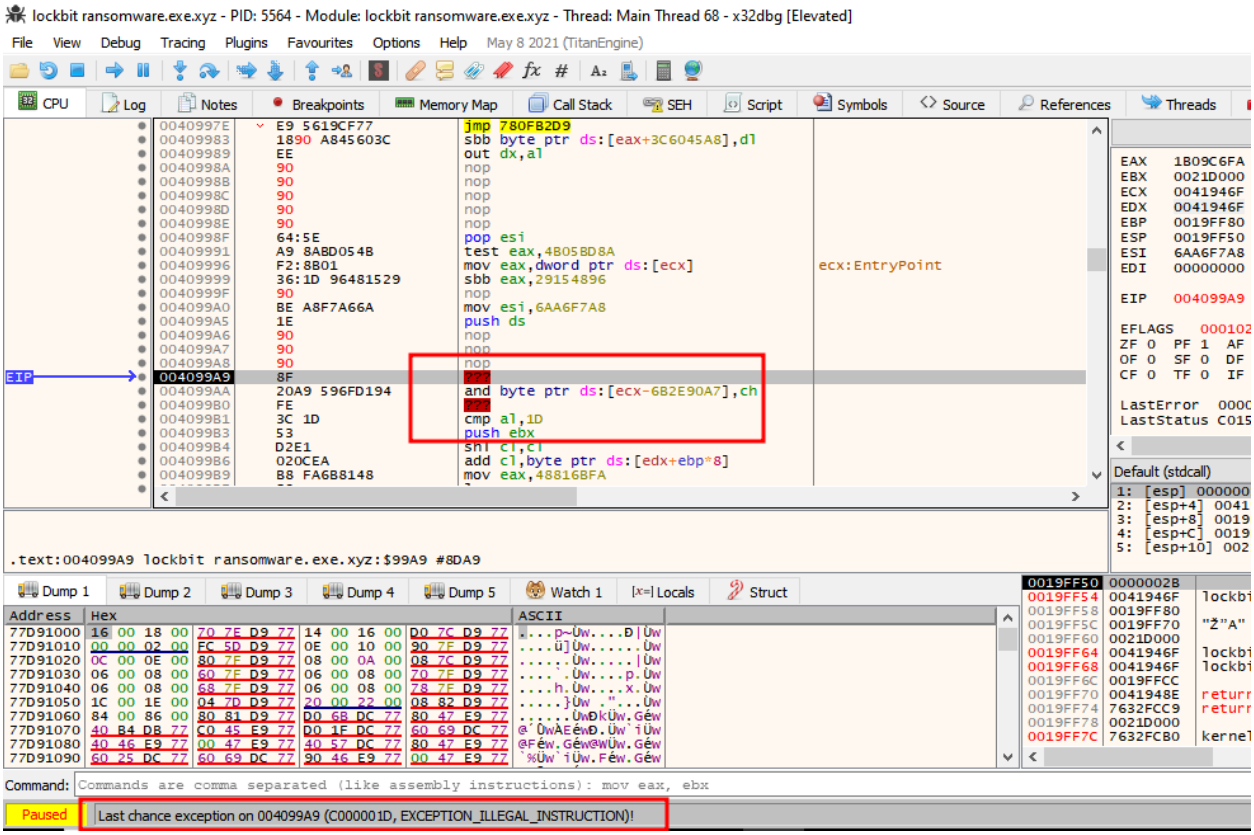
Technical Analysis

This issue can be mitigated by setting the exception code C0000005 in the debugger's exception filter. For x64dbg specifically, if the exception code is not known in advance, the 'Ignore Last' feature can be utilized to automatically add the most recent exception to the filter.



Technical Analysis

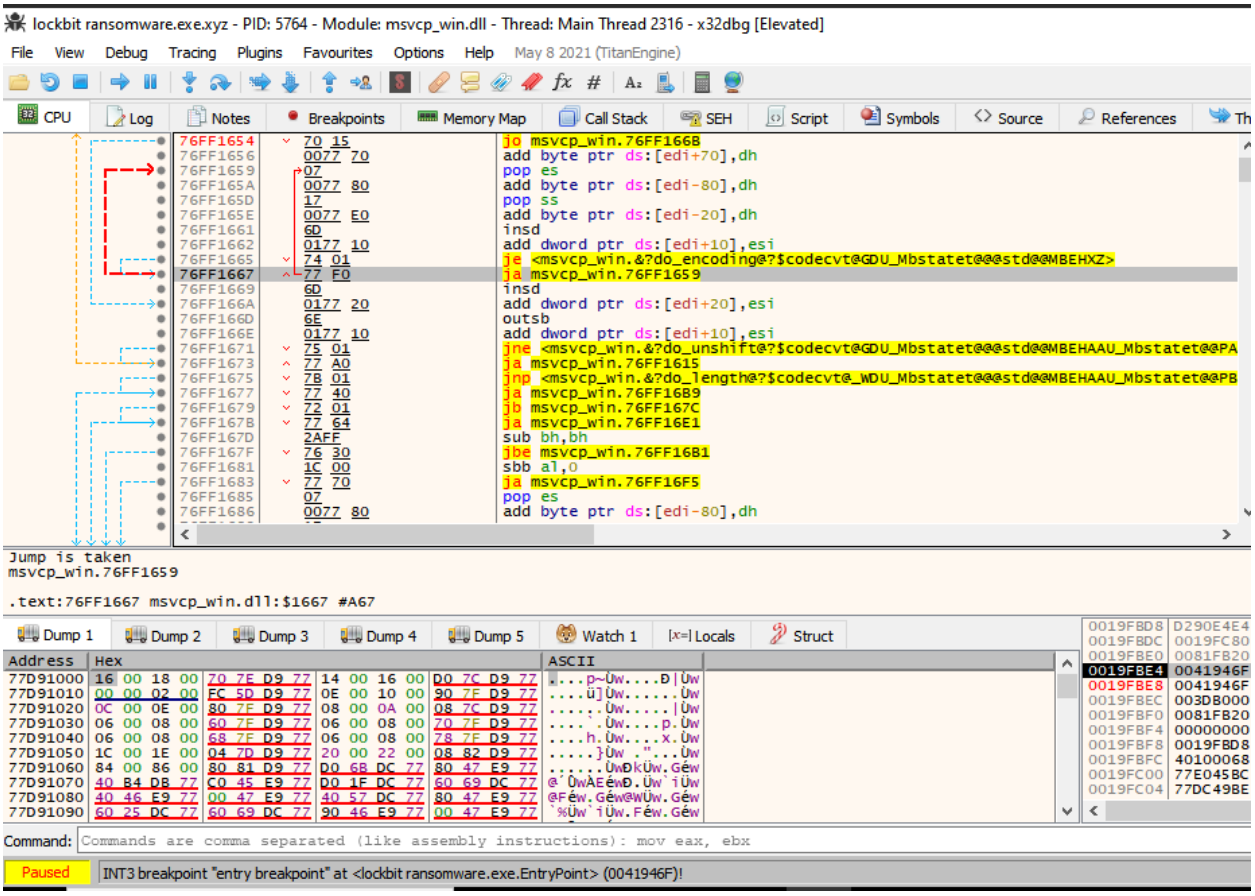
Alternatively, this issue can be addressed by performing a patch of the file during analysis to replace these instructions with NOP (No Operation) bytes.



As you can see exception for illegal instruction, so we can bypass that by doing the nop.

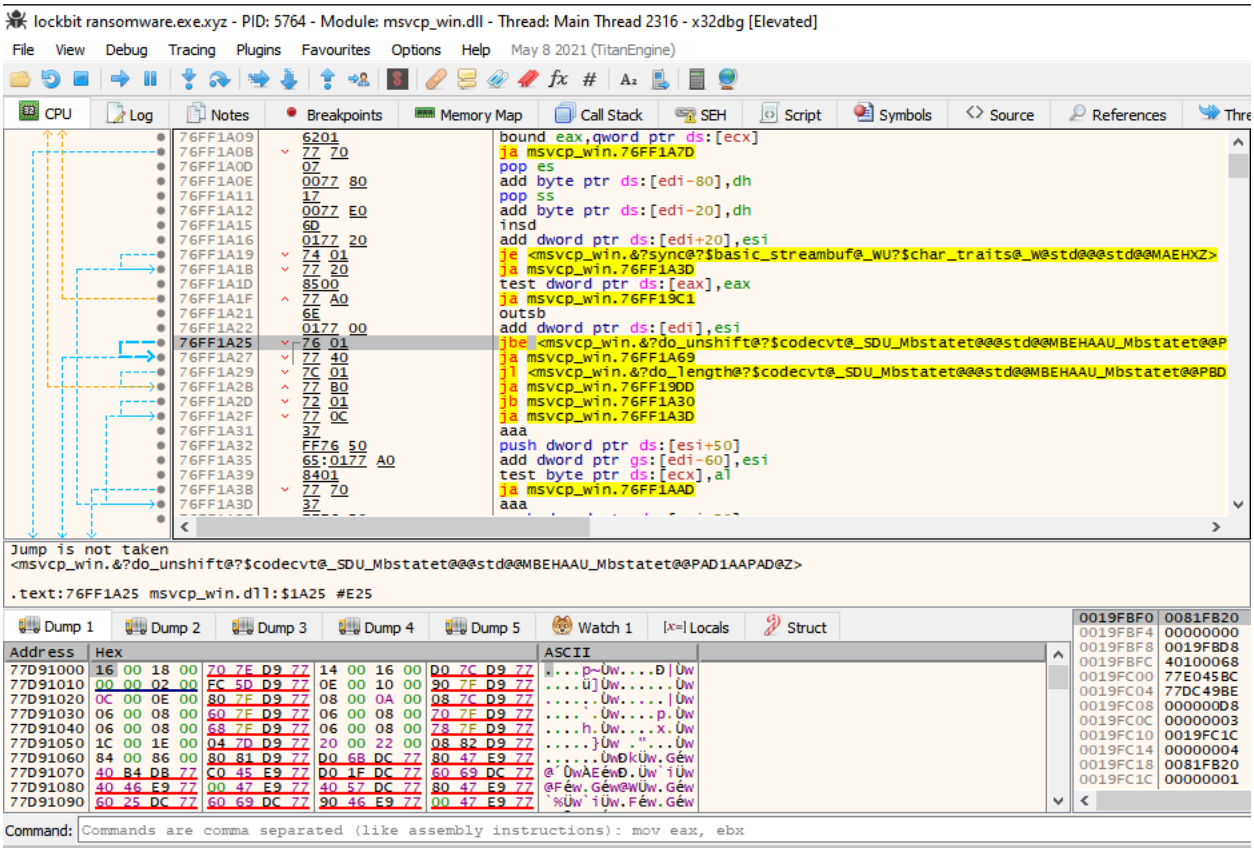
Technical Analysis

The do_encoding function is a member function of the std::codecvt class of C++. It is used to perform encoding and decoding operations on character sequences.



Technical Analysis

The do_unshift function is also a member function of the std::codecvt class. It is used to perform unshifting operations on character sequences.



Overall, the ransomware is designed to evade detection by security software and prevent its discovery. This includes employing obfuscation techniques to hide its presence on the victim's computer, as well as initiating reconnaissance as the first stage of its operation.

Yara Rules

```
rule lockbit3_detection_rule {
  meta:
    description = "Detecting lockbit3.0 indicators."
    last_updated = "2024-02-28"
    author = "Yusuf Amr"

  strings:
    $entrypoint = {90 0F 1F 44 00 00 E8 86 FB FF FF 66 90 E8 0F CF FE FF 0F 1F 84
00 00 00 00 00 E8 F2 04 FF FF 90 E8}
    $cmdfound = "CMd" ascii fullword
    $zzzdbg = ".rdata$zzzdbg" ascii fullword
    $mnfound = ".text$mn" ascii fullword

  condition:
    $entrypoint or $cmdfound or $zzzdbg or $mnfound
}
```