



Malware Analysis Report

LOCKBIT 3.0 Ransomware

By: Yusuf Amr

Table of Content

Executive Summar.....	3
Technical Analysis.....	4
Yara Rules.....	19

Executive Summar

MD5 Hash	7f58f9289043b2a83499fecfb99d540
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.

The screenshot shows the VirusTotal analysis page for a file. The file name is 1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32235567.exe. The file size is 155.50 KB, and the last analysis date is 2 days ago. The file is flagged as malicious by 60 security vendors and 1 sandbox. The file is identified as a ransomware, specifically Ransom:Win32/Lockbit.df7d9bff. The file is also identified as a trojan, specifically Trojan[Ransom]/Win32.Convagent. The file is also identified as a trojan, specifically Trojan.Ransom.BlackMatter.110. The file is also identified as a trojan, specifically Win32:Evo-gen [Trj].

Security vendors' analysis	Do you want to automate checks?
AhnLab-V3	<input type="checkbox"/>
ALYac	<input type="checkbox"/>
Arcabit	<input type="checkbox"/>

Technical Analysis

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

pestudio 9.51 - Malware Initial Assessment - www.winitor.com - [c:\users\knvb\desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32235567\lockbit ransomware.exe.xyz]

file settings about

c:\users\knvb\desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32235567\lockbit ransomware.exe.xyz

indicators (sections > writable > anomaly)

virustotal (error)

dos-header (64 bytes)

dos-stub (64 bytes)

rich-header (n/a)

file-header (Intel-386)

optional-header (GUI)

directories (3)

sections (self-modifying)

libraries (3)

imports (flag)

exports (n/a)

tls-callback (n/a)

.NET (n/a)

resources (n/a)

strings (5099)

debug (Jul.2022)

manifest (n/a)

version (n/a)

certificate (n/a)

overlay (n/a)

property	value	detail
windows-driver-model (WDM)	0x0000	false
terminal-server-aware (TSA)	0x8000	true
control-flow-guard (CFG)	0x0000	false
image-bound	0x0000	false
image-isolation	0x0000	false
High-Entropy	0x0000	false
AppContainer	0x0000	false
general		
subsystem	0x0002	GUI
magic	0x010B	PE
file-checksum	0x00030EEC	0x00030EEC
entry-point	0x0001946F	section: itext
base-of-code	0x00001000	section: text
base-of-data	0x0001A000	section: rdata
size-of-code	0x00018400	99328 bytes
size-of-initialized-data	0x0000C600	50688 bytes
size-of-uninitialized-data	0x00000000	0 bytes
size-of-image	0x0002A000	172032 bytes
size-of-Headers	0x00000400	1024 bytes
size-of-stack-reserve	0x00100000	1048576 bytes
size-of-stack-commit	0x00001000	4096 bytes
size-of-heap-reserve	0x00400000	4194304 bytes
size-of-heap-commit	0x00001000	4096 bytes
section-alignment	0x00001000	4096 bytes
file-alignment	0x00000200	512 bytes
directories-count	0x00000010	16
LoaderFlags	0x00000000	0x00000000

phs756- 1866B28B51045944DF18E63C9A5080AEE085F30FF1944DB6544CA76B32235567 exe 32-bit file-type: executable subsystem: GUI entry-point: 0x0001946F

Technical Analysis

utilizing a set of APIs for reconnaissance purposes.

pestudio 9.51 - Malware Initial Assessment - www.winator.com - [c:\users\knvb\desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32235567\lockbit ransomware.exe.xyz]

file settings about

c:\users\knvb\desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32235567\lockbit ransomware.exe.xyz

indicators (sections > writable > anomaly)

indicator (19)	detail	level
sections > writable > anomaly	.text	1
sections > entry-point > suspicious	0x06916913	1
sections > self-modifying	.text	1
imports > flag	2	1
file > entropy	7.983	3
file > sha256sum	1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32235567	3
file > size	159232 bytes	3
security > protection	data-execution-prevention (DEP) > ON	3
security > protection	control-flow-guard (CFG) > OFF	3
security > protection	address-space-layout-randomization (ASLR) > OFF	3
debug > stream > type	PGQ	3
security > protection	code-integrity (CI) > OFF	3
file > subsystem	GUI	3
group > API	windowing	3
group > API	input-output	3
group > API	data-exchange	3
group > API	reconnaissance	3
group > API	dynamic-library	3
imports > imphash	89b43582b27abefb2b74684ab12a2f8e	3

Several library imports and strings appear to be suspicious.

pestudio 9.51 - Malware Initial Assessment - www.winator.com - [c:\users\knvb\desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32235567\lockbit ransomware.exe.xyz]

file settings about

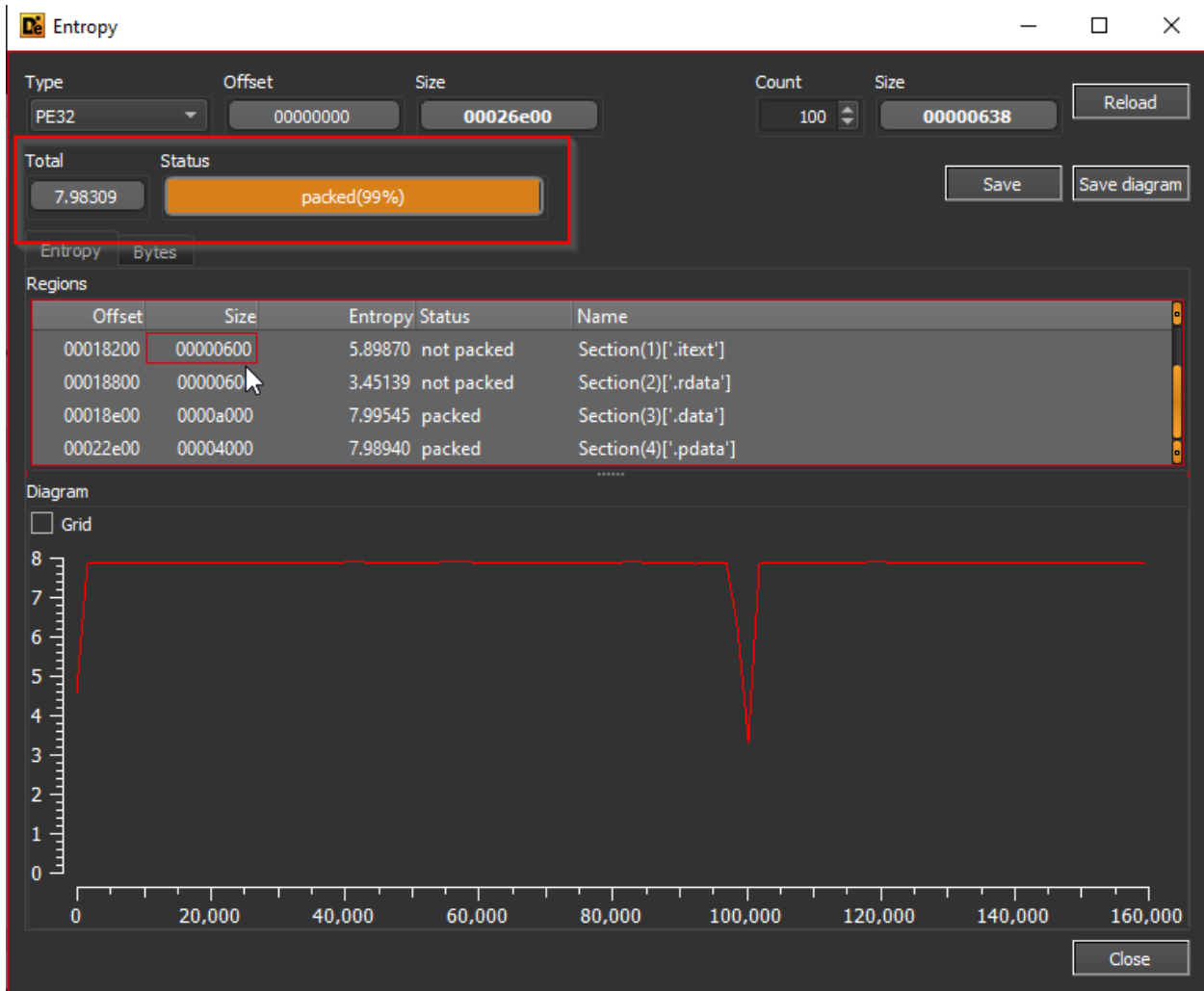
c:\users\knvb\desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32235567\lockbit ransomware.exe.xyz

indicators (sections > writable > anomaly)

size (bytes)	location	flag (2)	label (38)	group (5)	technique (2)	value (5099)
13	0x00018B90	-	import	windowing	-	DefWindowProc
13	0x00018CDA	-	import	reconnaissance	-	GetDateFormat
14	0x00018B8C	x	import	input-output	-	GetKeyNameText
15	0x00018C3C	-	import	dynamic-library	-	GetModuleHandle
13	0x00018C40	-	import	dynamic-library	T1106 Execution through API	LoadLibraryEx
11	0x00018C52	-	import	dynamic-library	T1106 Execution through API	LoadLibrary
11	0x00018BFA	x	import	data-exchange	-	GetAtomName
3	0x0000D0F1	-	utility	-	T1059 Command-Line Interface	CMD
14	0x00018A14	-	import	-	-	CreateWindowMap
14	0x00018B06	-	import	-	-	GetTextCharSet
12	0x00018B18	-	import	-	-	GetTextColor
14	0x00018B28	-	import	-	-	GetTextMetrics
8	0x00018B3A	-	import	-	-	SetPixel
12	0x00018B46	-	import	-	-	SetTextColor
17	0x00018B6C	-	import	-	-	CreateDialogParam
10	0x00018B82	-	import	-	-	CreateMenu
9	0x00018BA2	-	import	-	-	EndDialog
10	0x00018BAE	-	import	-	-	GetDlgItem
9	0x00018BCE	-	import	-	-	LoadImage
13	0x00018BE8	-	import	-	-	FormatMessage
12	0x00018C1C	-	import	-	-	GetLastError
12	0x00018C62	-	import	-	-	SetLastError
3	0x000049C9	-	file	-	-	s.z
3	0x00005592	-	file	-	-	v.H
6	0x00005FA9	-	file	-	-	Rj31.Z
3	0x00012925	-	file	-	-	*.h
3	0x00016437	-	file	-	-	L.z

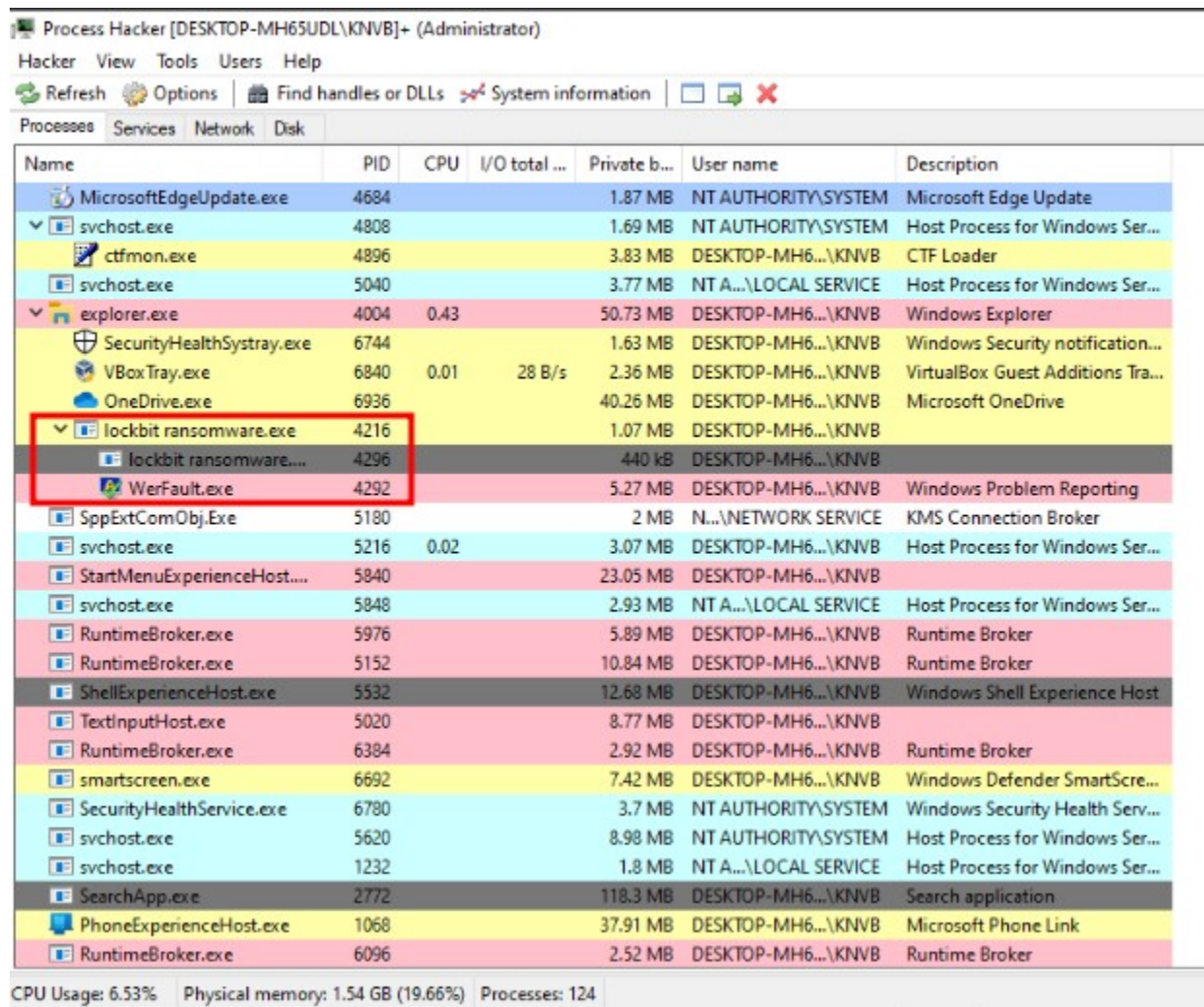
Technical Analysis

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.



Process Hacker [DESKTOP-MH65UDL\KNVB]+ (Administrator)

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information

Processes Services Network Disk

Name	PID	CPU	I/O total ...	Private b...	User name	Description
MicrosoftEdgeUpdate.exe	4684			1.87 MB	NT AUTHORITY\SYSTEM	Microsoft Edge Update
svchost.exe	4808			1.69 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
ctfmon.exe	4896			3.83 MB	DESKTOP-MH6... \KNVB	CTF Loader
svchost.exe	5040			3.77 MB	NT A... \LOCAL SERVICE	Host Process for Windows Ser...
explorer.exe	4004	0.43		50.73 MB	DESKTOP-MH6... \KNVB	Windows Explorer
SecurityHealthSystray.exe	6744			1.63 MB	DESKTOP-MH6... \KNVB	Windows Security notification...
VBoxTray.exe	6840	0.01	28 B/s	2.36 MB	DESKTOP-MH6... \KNVB	VirtualBox Guest Additions Tra...
OneDrive.exe	6936			40.26 MB	DESKTOP-MH6... \KNVB	Microsoft OneDrive
lockbit ransomware.exe	4216			1.07 MB	DESKTOP-MH6... \KNVB	
lockbit ransomware....	4296			440 kB	DESKTOP-MH6... \KNVB	
WerFault.exe	4292			5.27 MB	DESKTOP-MH6... \KNVB	Windows Problem Reporting
SppExtComObj.Exe	5180			2 MB	N... \NETWORK SERVICE	KMS Connection Broker
svchost.exe	5216	0.02		3.07 MB	DESKTOP-MH6... \KNVB	Host Process for Windows Ser...
StartMenuExperienceHost....	5840			23.05 MB	DESKTOP-MH6... \KNVB	
svchost.exe	5848			2.93 MB	NT A... \LOCAL SERVICE	Host Process for Windows Ser...
RuntimeBroker.exe	5976			5.89 MB	DESKTOP-MH6... \KNVB	Runtime Broker
RuntimeBroker.exe	5152			10.84 MB	DESKTOP-MH6... \KNVB	Runtime Broker
ShellExperienceHost.exe	5532			12.68 MB	DESKTOP-MH6... \KNVB	Windows Shell Experience Host
TextInputHost.exe	5020			8.77 MB	DESKTOP-MH6... \KNVB	
RuntimeBroker.exe	6384			2.92 MB	DESKTOP-MH6... \KNVB	Runtime Broker
smartscreen.exe	6692			7.42 MB	DESKTOP-MH6... \KNVB	Windows Defender SmartScre...
SecurityHealthService.exe	6780			3.7 MB	NT AUTHORITY\SYSTEM	Windows Security Health Serv...
svchost.exe	5620			8.98 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1232			1.8 MB	NT A... \LOCAL SERVICE	Host Process for Windows Ser...
SearchApp.exe	2772			118.3 MB	DESKTOP-MH6... \KNVB	Search application
PhoneExperienceHost.exe	1068			37.91 MB	DESKTOP-MH6... \KNVB	Microsoft Phone Link
RuntimeBroker.exe	6096			2.52 MB	DESKTOP-MH6... \KNVB	Runtime Broker

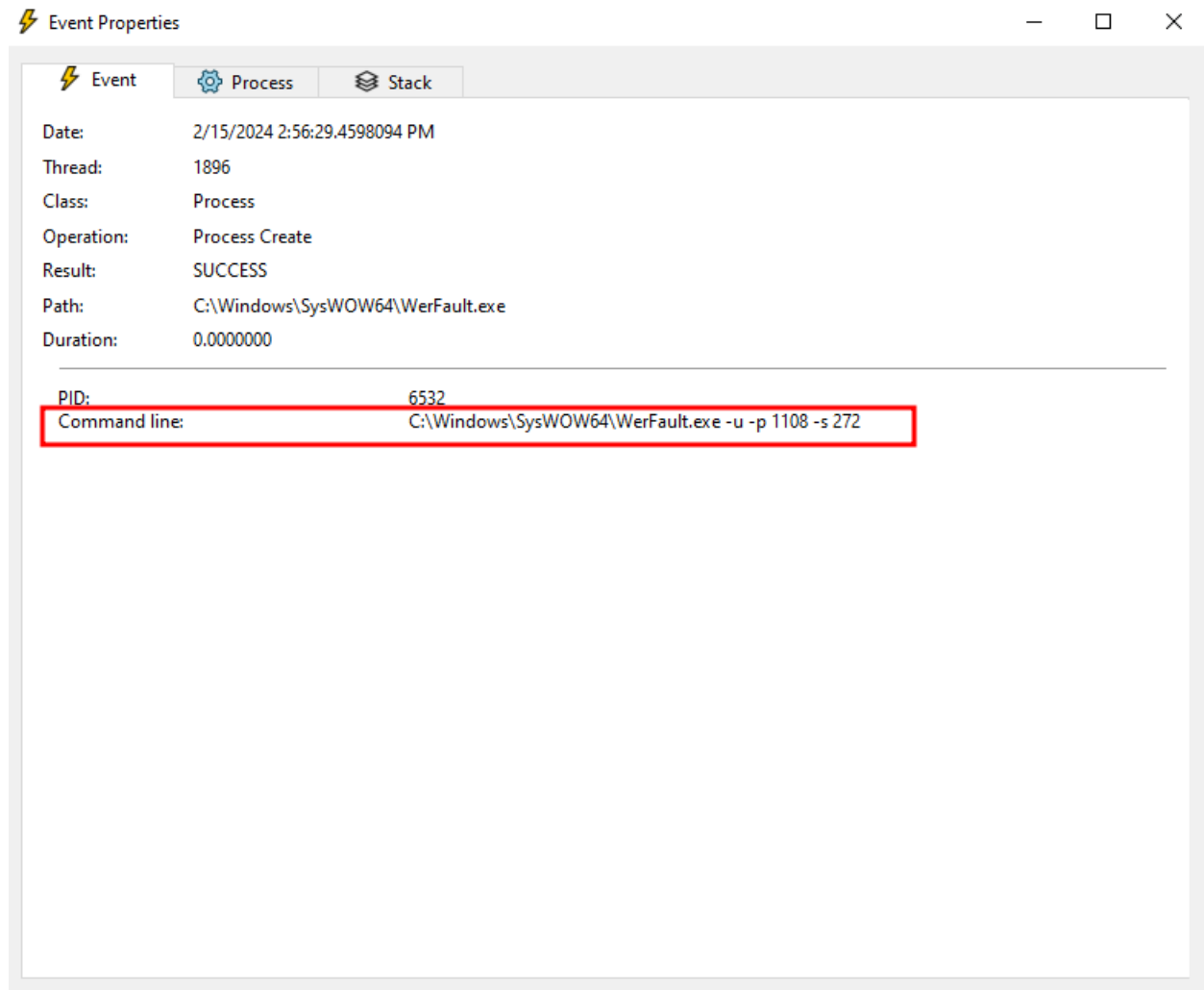
CPU Usage: 6.53% Physical memory: 1.54 GB (19.66%) Processes: 124

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.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
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: Handle Tag...
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: Handle Tag...
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

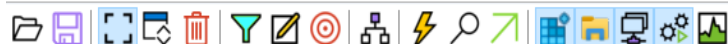


Technical Analysis

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

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help



Time ...	Process Name	PID	Operation	Path	Result	Detail
7:55:1...	lockbit ransom...	3068	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS	KeySetInformation...
7:55:1...	lockbit ransom...	3068	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags...	NAME NOT FOUND	Length: 20
7:55:1...	lockbit ransom...	3068	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS	
7:55:1...	lockbit ransom...	3068	RegOpenKey	HKLM\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS	Desired Access: Q...
7:55:1...	lockbit ransom...	3068	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS	KeySetInformation...
7:55:1...	lockbit ransom...	3068	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags...	NAME NOT FOUND	Length: 20
7:55:1...	lockbit ransom...	3068	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS	
7:55:1...	lockbit ransom...	3068	CreateFile	C:\Users\KNVB\Desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32...	SUCCESS	Desired Access: R...
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Users\KNVB\Desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32...	BUFFER OVERFLOW	Information: Owner
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Users\KNVB\Desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32...	SUCCESS	Information: Owner
7:55:1...	lockbit ransom...	3068	CloseFile	C:\Users\KNVB\Desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32...	SUCCESS	
7:55:1...	lockbit ransom...	3068	CreateFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Desired Access: R...
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	BUFFER OVERFLOW	Information: Owner
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Information: Owner
7:55:1...	lockbit ransom...	3068	CloseFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	
7:55:1...	lockbit ransom...	3068	CreateFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Desired Access: R...
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	BUFFER OVERFLOW	Information: Owner
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Information: Owner
7:55:1...	lockbit ransom...	3068	CloseFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	
7:55:1...	lockbit ransom...	3068	CreateFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Desired Access: R...
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	BUFFER OVERFLOW	Information: Owner
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Information: Owner
7:55:1...	lockbit ransom...	3068	CloseFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	
7:55:1...	lockbit ransom...	3068	CreateFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Desired Access: G...
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	BUFFER OVERFLOW	AllocationSize: 4,0...
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	AllocationSize: 4,0...
7:55:1...	lockbit ransom...	3068	CloseFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	SyncType: SyncTy...
7:55:1...	lockbit ransom...	3068	CreateFile	C:\Windows\SysWOW64\kernel32.dll	FILE LOCKED WITH ONLY READERS	AllocationSize: 4,0...
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	SyncType: SyncTy...
7:55:1...	lockbit ransom...	3068	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	AllocationSize: 4,0...
7:55:1...	lockbit ransom...	3068	CloseFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	SyncType: SyncTy...
7:55:1...	lockbit ransom...	3068	CreateFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Offset: 50,176, Len...
7:55:1...	lockbit ransom...	3068	ReadFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Offset: 320,512, Le...
7:55:1...	lockbit ransom...	3068	ReadFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	
7:55:1...	lockbit ransom...	3068	CreateFile	C:\Users\KNVB\Desktop\1866b28b51045944df18e63c9a5989afe985e30ff1944db6544ca76b32...	SUCCESS	Desired Access: G...
7:55:1...	lockbit ransom...	3068	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	SUCCESS	Desired Access: Q...
7:55:1...	lockbit ransom...	3068	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	SUCCESS	KeySetInformation...
7:55:1...	lockbit ransom...	3068	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	SUCCESS	Type: REG_SZ, Le...

Showing 322 of 903,672 events (0.035%)

Backed by virtual memory

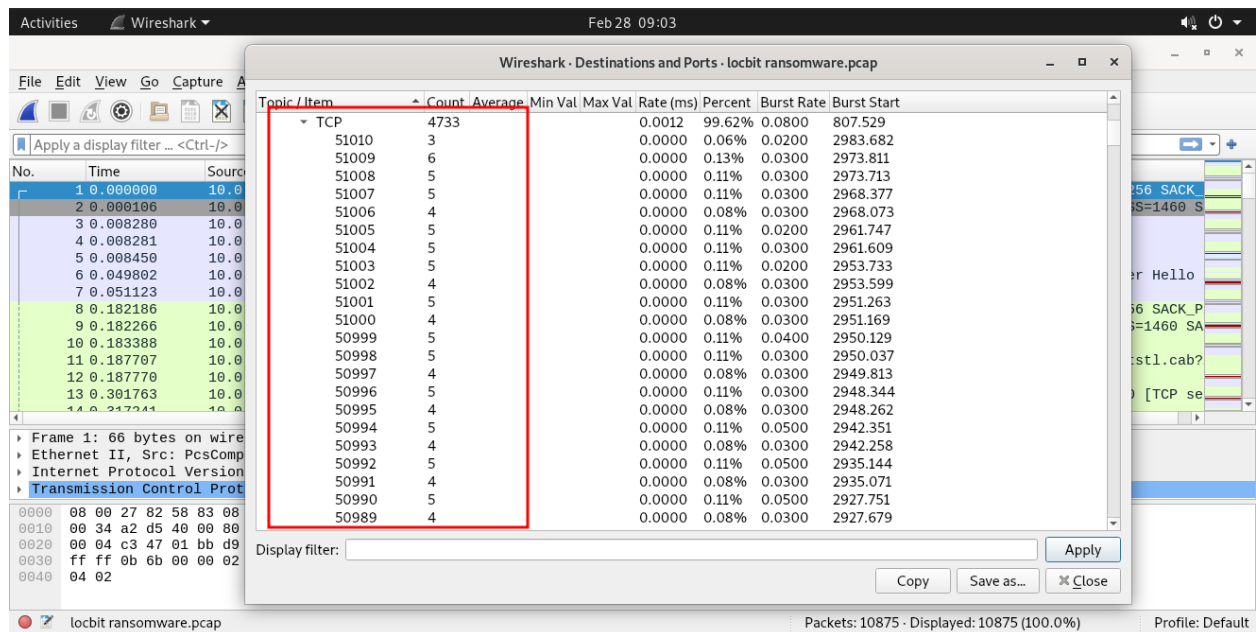
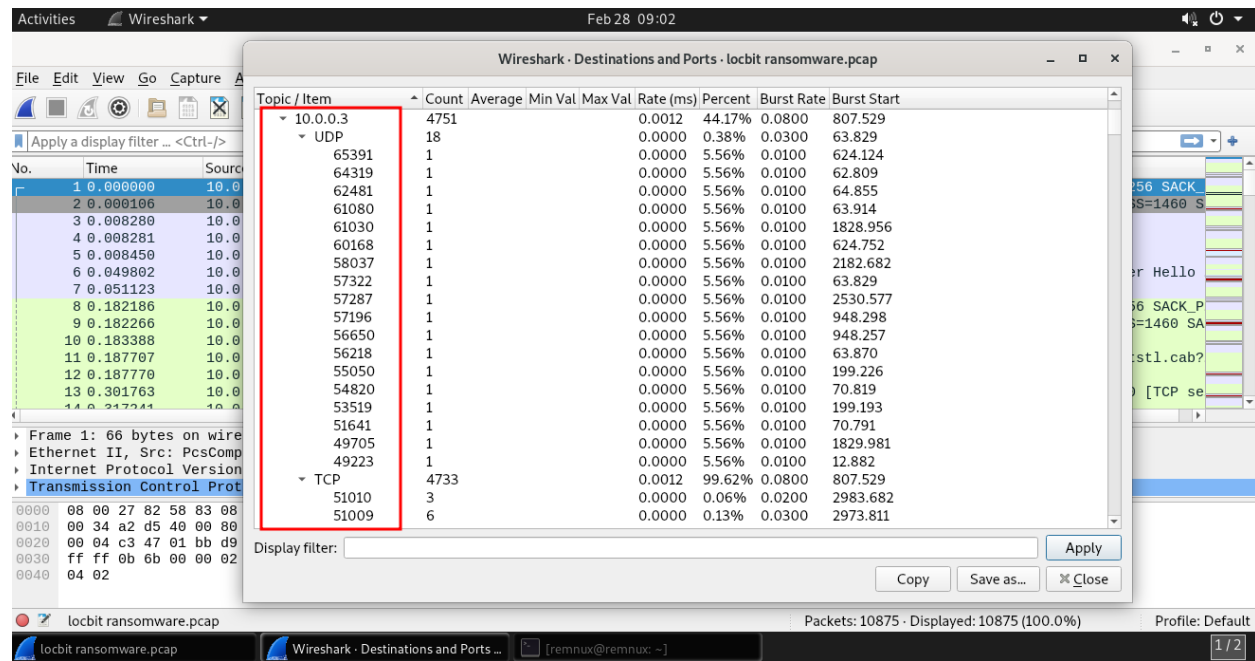
Technical Analysis

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

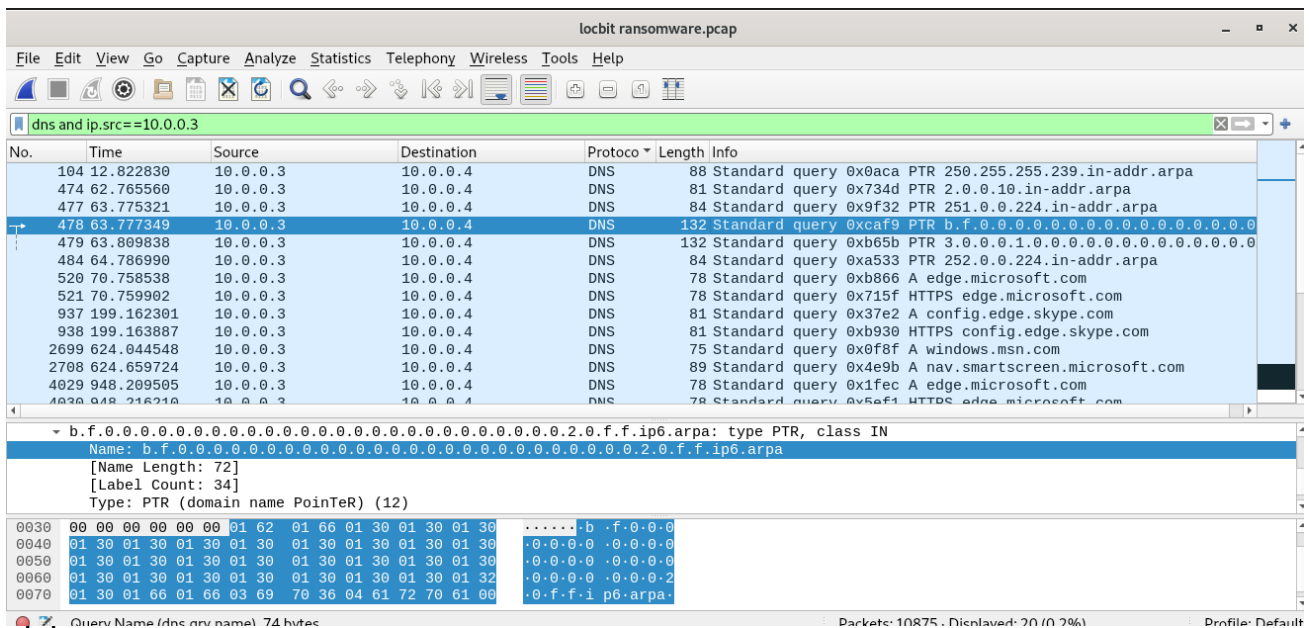
Process Monitor - Sysinternals: www.sysinternals.com							
File Edit Event Filter Tools Options Help							
Time ...	Process Name	PID	Operation	Path	Result	Detail	TID
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\System\CurrentControlSet\Control\Error Message Instrument	NAME NOT FOUND	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	REPARSE	Desired Access: Q...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	Desired Access: Q...	1704
3:53:1...	lockbit ransom...	4044	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	KeySetInformation...	1704
3:53:1...	lockbit ransom...	4044	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	Query: HandleTag...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\lockbit ransomware.exe	NAME NOT FOUND	Desired Access: Q...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Display	REPARSE	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Display	NAME NOT FOUND	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Display	REPARSE	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Display	NAME NOT FOUND	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	Query: HandleTag...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\lockbit ransomware.exe	NAME NOT FOUND	Desired Access: Q...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Display	REPARSE	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Display	NAME NOT FOUND	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Display	REPARSE	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Display	NAME NOT FOUND	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	REPARSE	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	KeySetInformation...	1704
3:53:1...	lockbit ransom...	4044	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles	NAME NOT FOUND	Length: 20	1704
3:53:1...	lockbit ransom...	4044	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS		1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	REPARSE	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	KeySetInformation...	1704
3:53:1...	lockbit ransom...	4044	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableUmpdBufferSizeCheck	NAME NOT FOUND	Length: 20	1704
3:53:1...	lockbit ransom...	4044	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS		1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\lockbit ransomware.exe	NAME NOT FOUND	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegQueryValue	HKCU\Control Panel\Desktop\EnablePerProcessSystemDPI	NAME NOT FOUND	Length: 20	1704
3:53:1...	lockbit ransom...	4044	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS		1704
3:53:1...	lockbit ransom...	4044	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS	Desired Access: R...	1704
3:53:1...	lockbit ransom...	4044	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32\lockbit ransomware	NAME NOT FOUND	Length: 172	1704
3:53:1...	lockbit ransom...	4044	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS		1704
Showing 150 of 695,945 events (0.021%)				Backed by virtual memory			

Technical Analysis

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



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.

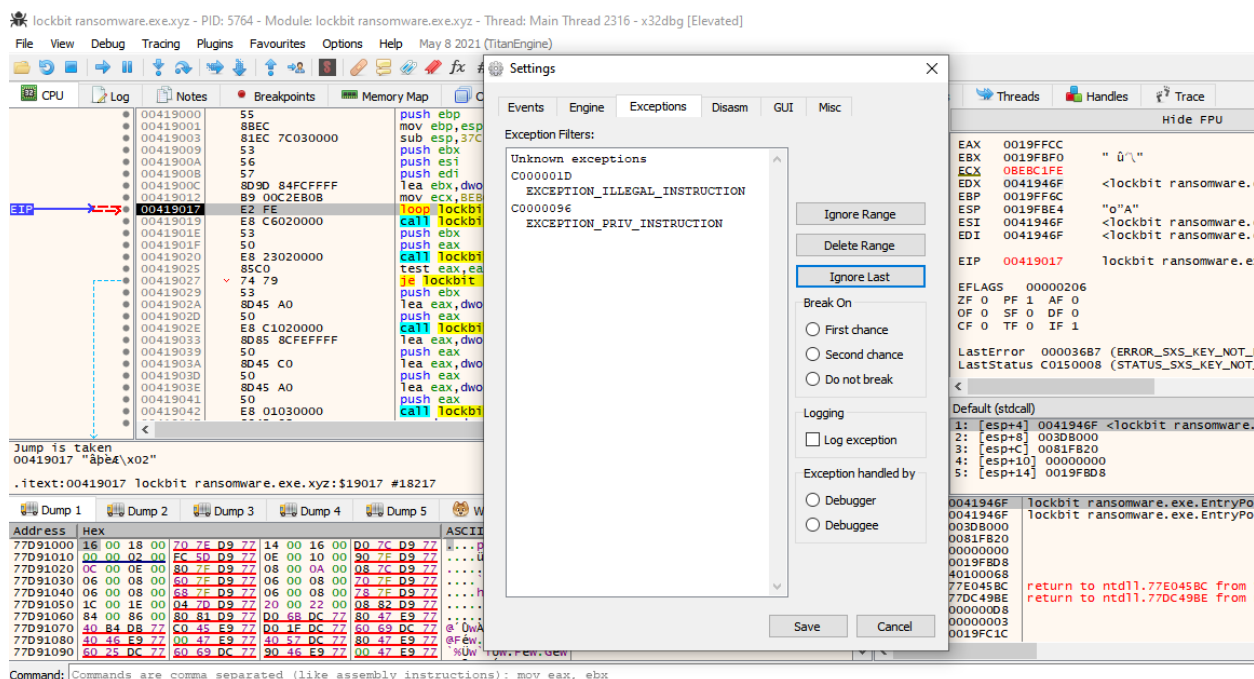


The malware employs a debugger evasion technique known as 'Exception Flooding.' The sample contains a significant number of function calls designed to cause a denial of service (DoS) on a debugger



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.

The screenshot shows the Immunity Debugger interface with the assembly window displaying the following code:

```
0040997E E9 5619CF77 jmp 780F82D9
00409983 1890 A845603C sbb byte ptr ds:[eax+3C6045A8],dl
00409989 EE out dx,al
0040998A 90 nop
0040998B 90 nop
0040998C 90 nop
0040998D 90 nop
0040998E 90 nop
0040998F 64:5E pop esi
00409991 A9 8ABD0548 test eax,4805BD8A
00409996 F2:8B01 mov eax,dword ptr ds:[ecx]
00409999 36:1D 96481529 sbb eax,29154896
0040999F 90 nop
004099A0 BE A8F7A66A mov esi,6AA6F7A8
004099A5 1E push ds
004099A6 90 nop
004099A7 90 nop
004099A8 90 nop
004099A9 8F and byte ptr ds:[ecx-6B2E90A7],ch
004099AA 20A9 596FD194
004099AB FE
004099AC 3C 1D cmp al,1D
004099AD 53 push ebx
004099AE D2E1 shl cl,cl
004099AF 020CEA add cl,byte ptr ds:[edx+ebp*8]
004099B0 B8 FA688148 mov eax,488168FA
```

The instruction at address 004099A9 is highlighted with a red box. The CPU window shows the instruction is being executed. The Exception window shows a "Last chance exception on 004099A9 (C000001D, EXCEPTION_ILLEGAL_INSTRUCTION)".

The memory dump window shows the following data:

Address	Hex	ASCII
77D91000	16 00 18 00 70 7E D9 77p~Uw....D Uw
77D91010	00 00 02 00 EC 5D D9 77u]Uw....Uw
77D91020	0C 00 0E 00 80 7E D9 77Uw....Uw
77D91030	06 00 08 00 60 7E D9 77Uw....p.Uw
77D91040	06 00 08 00 68 7E D9 77h.Uw....K.Uw
77D91050	1C 00 1E 00 04 7D D9 77}Uw....Uw
77D91060	84 00 86 00 80 81 D9 77UwDkUw.Gew
77D91070	40 B4 D8 77 C0 45 E9 77	@UwAewD.Uw'iUw
77D91080	40 46 E9 77 00 47 E9 77	@Few.GewwUw.Gew
77D91090	60 25 DC 77 60 69 DC 77	%Uw'iUw.Few.Gew

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

```
90 nop
90 nop
90 nop
90 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.

lockbit ransomware.exe.xyz - PID: 5764 - Module: msvcp_win.dll - Thread: Main Thread 2316 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help May 8 2021 (TitanEngine)

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Th

76FF1654 70 15 10 msvcp_win.76FF1668
76FF1656 0077 70 add byte ptr ds:[edi+70],dh
76FF1659 07 pop es
76FF165A 0077 80 add byte ptr ds:[edi-80],dh
76FF165D 17 pop ss
76FF165E 0077 E0 add byte ptr ds:[edi-20],dh
76FF1661 60 insd
76FF1662 0177 10 add dword ptr ds:[edi+10],esi
76FF1665 74 01 je <msvcp_win.&?do_encoding?@\$codecvt@GDU_Mbstatet@@std@MBEHXZ>
76FF1667 77 E0 ja msvcp_win.76FF1659
76FF1669 60 insd
76FF166A 0177 20 add dword ptr ds:[edi+20],esi
76FF166D 6E outsb
76FF166E 0177 10 add dword ptr ds:[edi+10],esi
76FF1671 75 01 jne <msvcp_win.&?do_unshift?@\$codecvt@GDU_Mbstatet@@std@MBEHAAU_Mbstatet@@PA
76FF1673 ja msvcp_win.76FF1615
76FF1675 78 01 jmp <msvcp_win.&?do_length?@\$codecvt@_WDU_Mbstatet@@std@MBEHAAU_Mbstatet@@PB
76FF1677 ja msvcp_win.76FF16B9
76FF1679 jb msvcp_win.76FF167C
76FF167B ja msvcp_win.76FF16E1
76FF167D 2AFF sub bh,bh
76FF167F 76 30 jbe msvcp_win.76FF16B1
76FF1681 sbb al,0
76FF1683 ja msvcp_win.76FF16F5
76FF1685 pop es
76FF1686 add byte ptr ds:[edi-80],dh

Jump is taken
msvcp_win.76FF1659

.text:76FF1667 msvcp_win.dll:\$1667 #A67

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct

Address	Hex	ASCII
77D91000	16 00 18 00 70 7E D9 77 14 00 16 00 D0 7C D9 77	...p-Uw...D Uw
77D91010	00 00 02 00 EC 5D D9 77 0E 00 10 00 90 7E D9 77	...u Uw... Uw
77D91020	0C 00 0E 00 80 7E D9 77 08 00 0A 00 08 7C D9 77	...t Uw... Uw
77D91030	06 00 08 00 60 7E D9 77 06 00 08 00 70 7E D9 77	...p Uw... Uw
77D91040	06 00 08 00 68 7E D9 77 06 00 08 00 78 7E D9 77	...h Uw... x Uw
77D91050	1C 00 1E 00 04 7D D9 77 20 00 22 00 08 82 D9 77	...} Uw... " Uw
77D91060	84 00 86 00 80 81 D9 77 D0 68 DC 77 80 47 E9 77	...UwDkUw.Gew
77D91070	40 84 D8 77 C0 45 E9 77 D0 1F DC 77 60 69 DC 77	@'UwAEewD.Uw'Uw
77D91080	40 46 E9 77 00 47 E9 77 40 57 DC 77 80 47 E9 77	@Few.GewWUw.Gew
77D91090	60 25 DC 77 60 69 DC 77 90 46 E9 77 00 47 E9 77	%Uw'Uw.Few.Gew

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused INT3 breakpoint "entry breakpoint" at <lockbit ransomware.exe.EntryPoint> (0041946F)!

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.

lockbit ransomware.exe.xyz - PID: 5764 - Module: msvcp_win.dll - Thread: Main Thread 2316 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help May 8 2021 (TitanEngine)

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Thre

76FF1A09 6201 bound eax,qword ptr ds:[ecx]
76FF1A0B 77 70 j3 msvcp_win.76FF1A7D
76FF1A0D 07 pop es
76FF1A0E 0077 80 add byte ptr ds:[edi-80],dh
76FF1A11 17 pop ss
76FF1A12 0077 E0 add byte ptr ds:[edi-20],dh
76FF1A15 60 insd
76FF1A16 0177 20 add dword ptr ds:[edi+20],esi
76FF1A19 74 01 j3 <msvc_win.76FF1A7D>
76FF1A1B 77 20 j3 msvcp_win.76FF1A3D
76FF1A1D 8500 test dword ptr ds:[eax],eax
76FF1A1F 77 A0 j3 msvcp_win.76FF1A3C
76FF1A21 6E outsb
76FF1A22 0177 00 add dword ptr ds:[edi],esi
76FF1A25 76 01 jbe <msvc_win.76FF1A7D>
76FF1A27 77 40 j3 msvcp_win.76FF1A69
76FF1A29 7C 01 j1 <msvc_win.76FF1A7D>
76FF1A2B 77 80 j3 msvcp_win.76FF1A3D
76FF1A2D 72 01 jb msvcp_win.76FF1A30
76FF1A2F 77 0C j3 msvcp_win.76FF1A3D
76FF1A31 37 aaa
76FF1A32 FF76 50 push dword ptr ds:[esi+50]
76FF1A35 65 0177 A0 add dword ptr gs:[edi-60],esi
76FF1A39 8401 test byte ptr ds:[ecx],al
76FF1A3B 77 70 j3 msvcp_win.76FF1A3D
76FF1A3D 37 aaa

Jump is not taken
<msvc_win.76FF1A7D>
.text:76FF1A25 msvcp_win.dll:1A25 #E25

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct

Address	Hex	ASCII
77D91000	16 00 18 00 70 7E D9 77 14 00 16 00 D0 7C D9 77	W...p-Uw...D Uw
77D91010	00 00 02 00 EC 5D D9 77 0E 00 10 00 90 7E D9 77UjUw...Uw
77D91020	0C 00 0E 00 80 7E D9 77 08 00 0A 00 08 7C D9 77Uw...Uw
77D91030	06 00 08 00 60 7E D9 77 06 00 08 00 70 7E D9 77Uw...p.Uw
77D91040	06 00 08 00 68 7E D9 77 06 00 08 00 78 7E D9 77h.Uw...x.Uw
77D91050	1C 00 1E 00 04 7D D9 77 20 00 22 00 08 82 D9 77Uw...Uw
77D91060	84 00 86 00 80 81 D9 77 D0 68 DC 77 80 47 E9 77UwUw.Gew
77D91070	40 B4 D8 77 C0 45 E9 77 D0 1F DC 77 60 69 DC 77	@UwAewD.Uw'Uw
77D91080	40 46 E9 77 00 47 E9 77 40 57 DC 77 80 47 E9 77	@Fw.GewUw.Gew
77D91090	60 25 DC 77 60 69 DC 77 90 46 E9 77 00 47 E9 77	%Uw'Uw.Few.Gew

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

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
}
```