Cerber Ransomware Malware Analysis Report

Date: April 28, 2025
Analyst: Richa Sharma
Malware Identified: Cerber Ransomware
Executable MD5: 8b6bc16fd137c09a08b02bbe1bb7d670
Analysis Environment:

- OS: Windows 7 (Oracle VirtualBox)

  Tools: INetSim, Process Monitor, Process Hacker, RegShot, OllyDbg, Ghidra, X32dbg

  Strings, wireshark

Objective

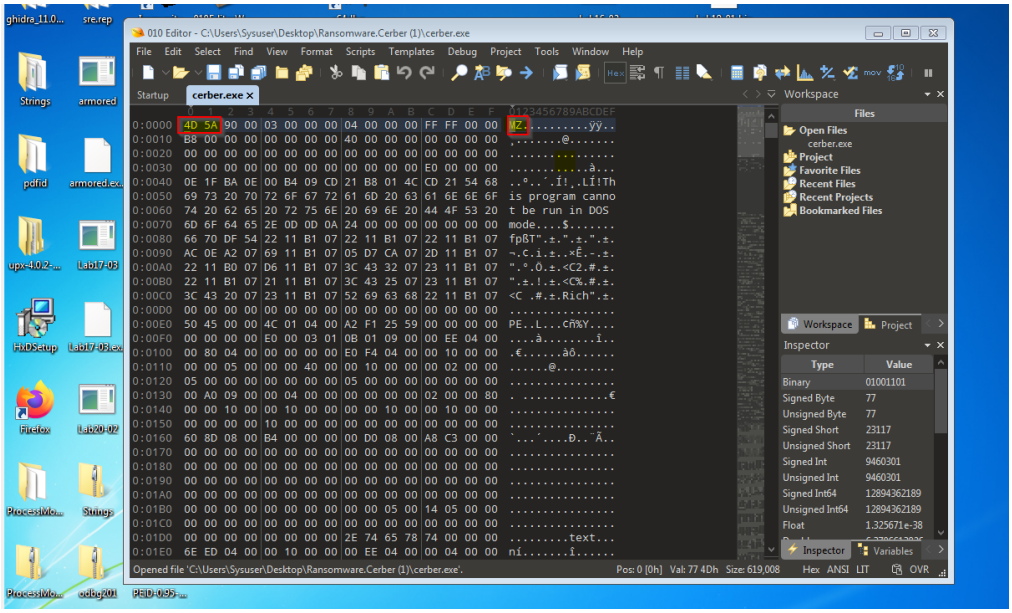
The objective of this analysis is to conduct an in-depth examination of the Cerber ransomware sample using both static and dynamic analysis techniques. The analysis aims to uncover the malware's behavior, including its execution flow, persistence mechanisms, file encryption strategies, evasion tactics, and network communications. Using industry-standard tools in a controlled environment, this investigation seeks to identify indicators of compromise (IOCs), understand Cerber's interaction with system resources, and evaluate the impact on compromised systems. The findings will support the development of effective detection, mitigation, and incident response strategies against Cerber and similar ransomware threats.

Unpacking the Malware

Tools Used: PEiD, 010 Editor

- **File Signature:** Confirmed Portable Executable (PE) via magic bytes MZ (0x4D 0x5A)
- **Packer Detection:** No known packer detected (possibly custom packed)
- **Entry Point:** Located at 0x0044FE40 in .text section

Observation: No unpacking required initially suitable for both static and dynamic analysis.



Imported API Methods (Observed via Ghidra + Dynamic Logs)

Cerber makes extensive use of Windows APIs for encryption, persistence, and stealth. It uses native tools to blend in and avoid detection.

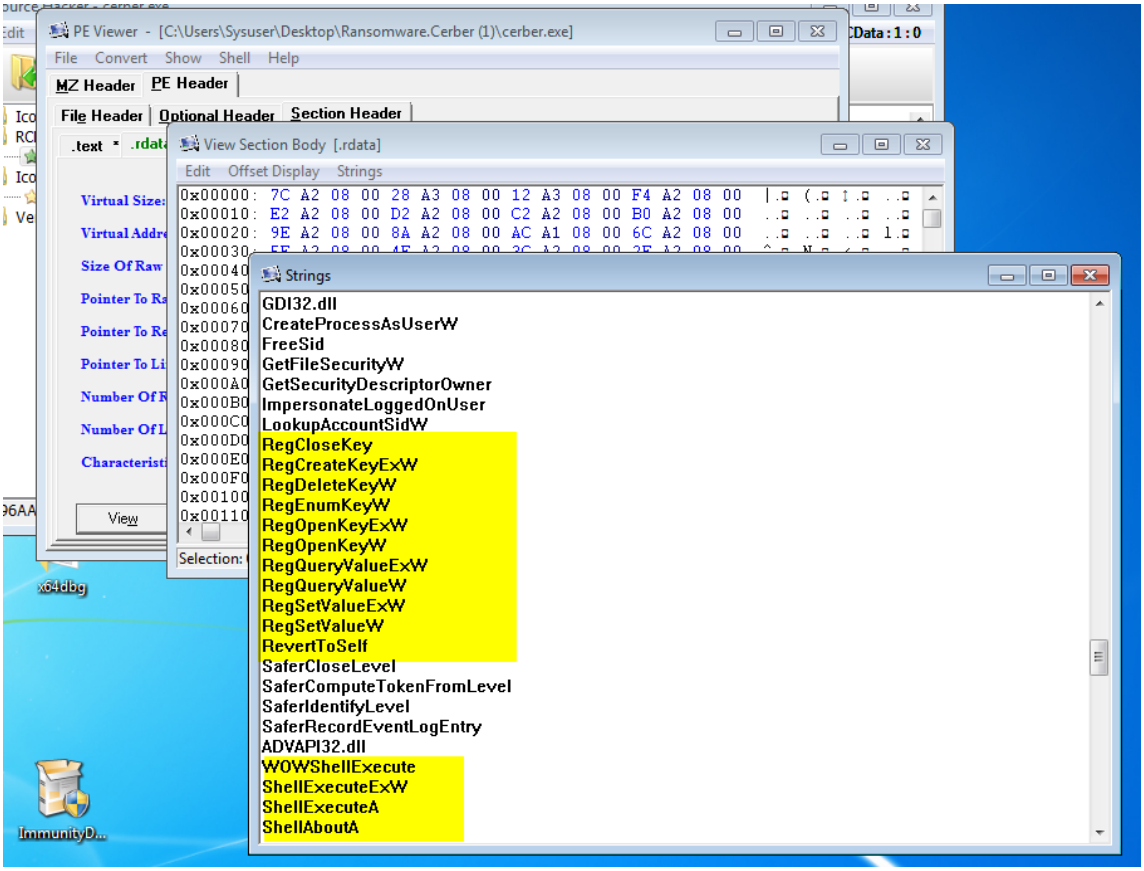
Important Imports

These DLLs form the core toolkit of most Windows ransomware

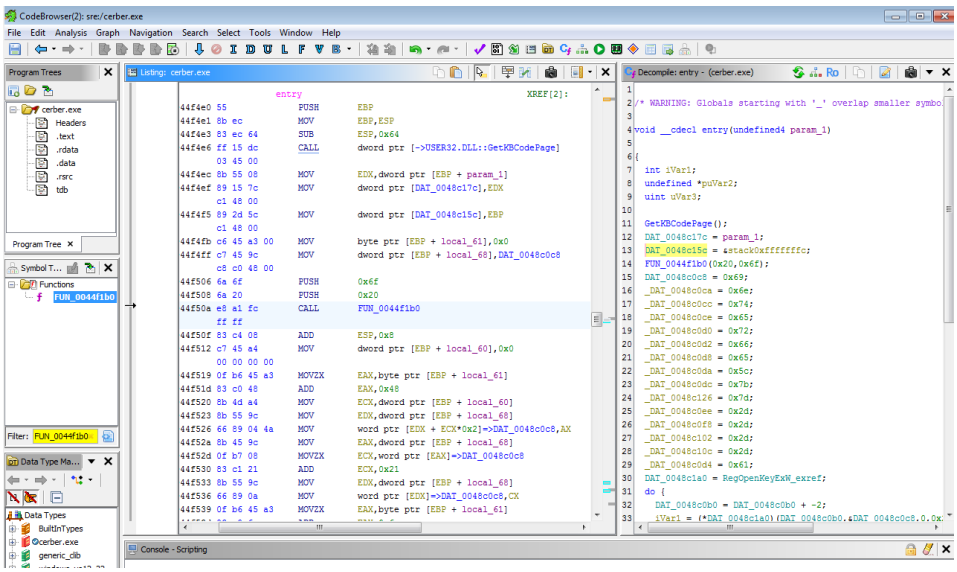
- KERNEL32.dll and ADVAPI32.dll are for file encryption and system modification.
- USER32.dll, GDI32.dll, and SHELL32.dll support user interaction and messaging.
- msvcrt.dll underpins basic operational logic.
- ShellExecuteA/W, WOWShellExecute, ShellAboutA

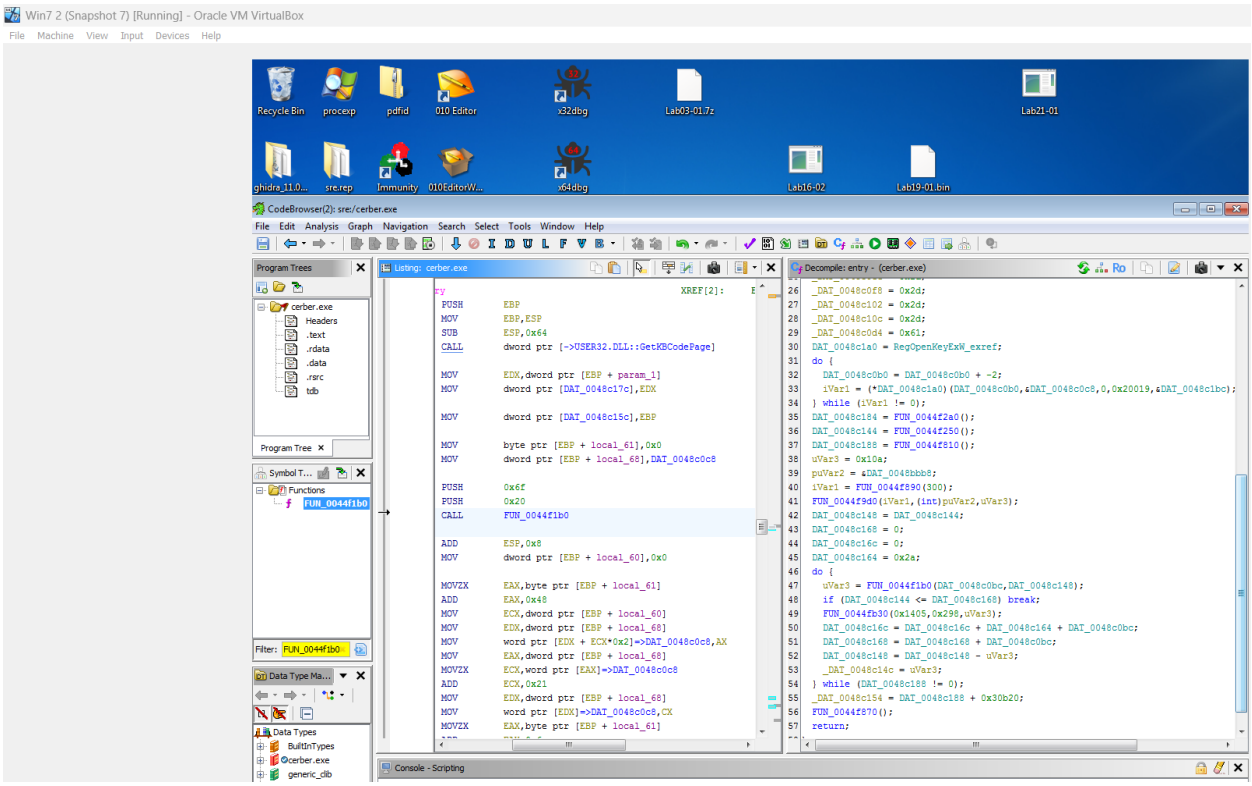
These are commonly used to

- Launch the ransom note in a web browser or text file (often using ShellExecuteW).
- Trigger external tools, like PowerShell scripts or batch files for encryption, deletion, or evasion.
- Possibly display a GUI warning using ShellAboutA.



Writing ASCII/Unicode Constants into Memory



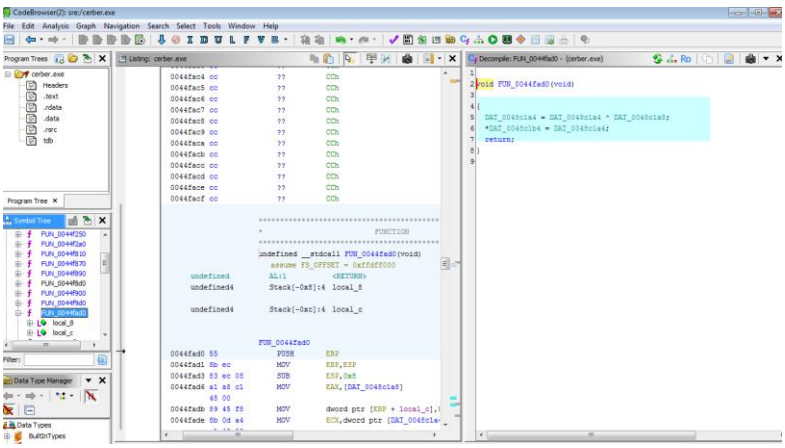


Likely Function Purpose FUN_0044f1b0:

This function acts as a oader or Decryptor, Allocating memory for decrypted or unpacked content.

- Processing encrypted blobs embedded in the binary.
- Preparing payloads or runtime configuration for later stages like, file encryption logic, C2 addresses, ransom message templates.

XOR Key is for unpacking/deobfuscation at runtime



DAT_0048c1a8 → XOR key

DAT_0048c1a4 → value being XORed (possibly encrypted)

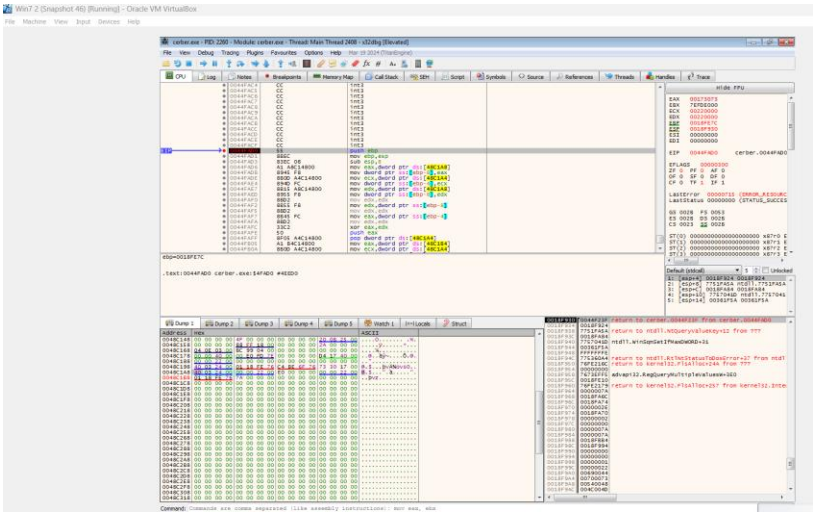
DAT_0048c1b4 → output (decrypted result)

In x32dbg (as you previously did):

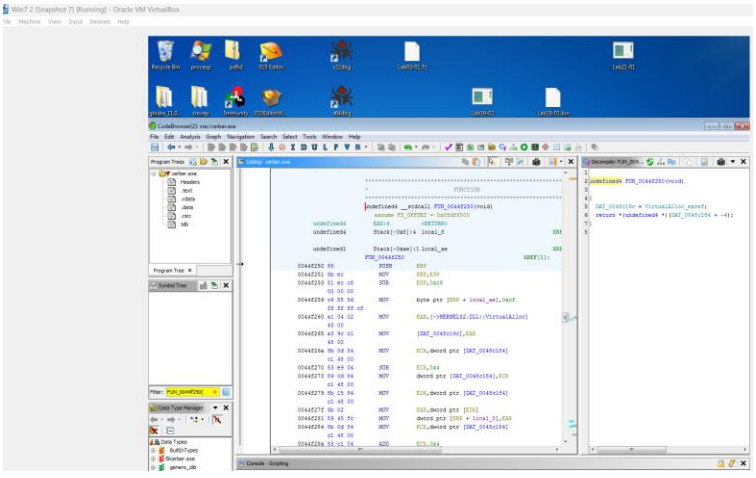
At address: 0x0048C1A8

The 4 bytes there (little-endian) are your XOR keys.

40 23 02 0A → 0x0A022340 (XOR key)



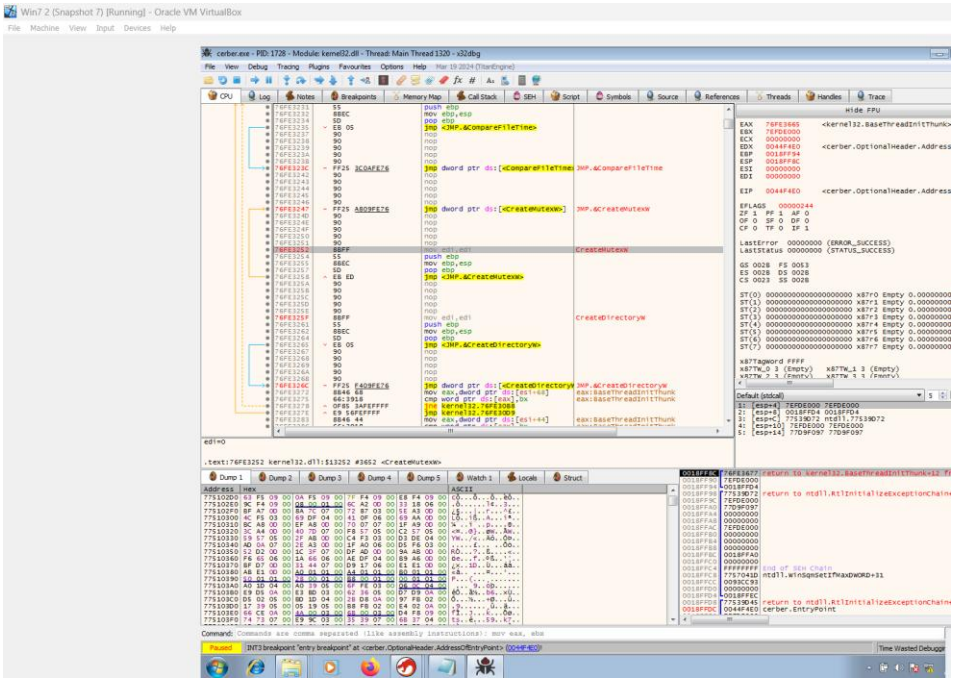
Reverse Engineered FUN_0044f250

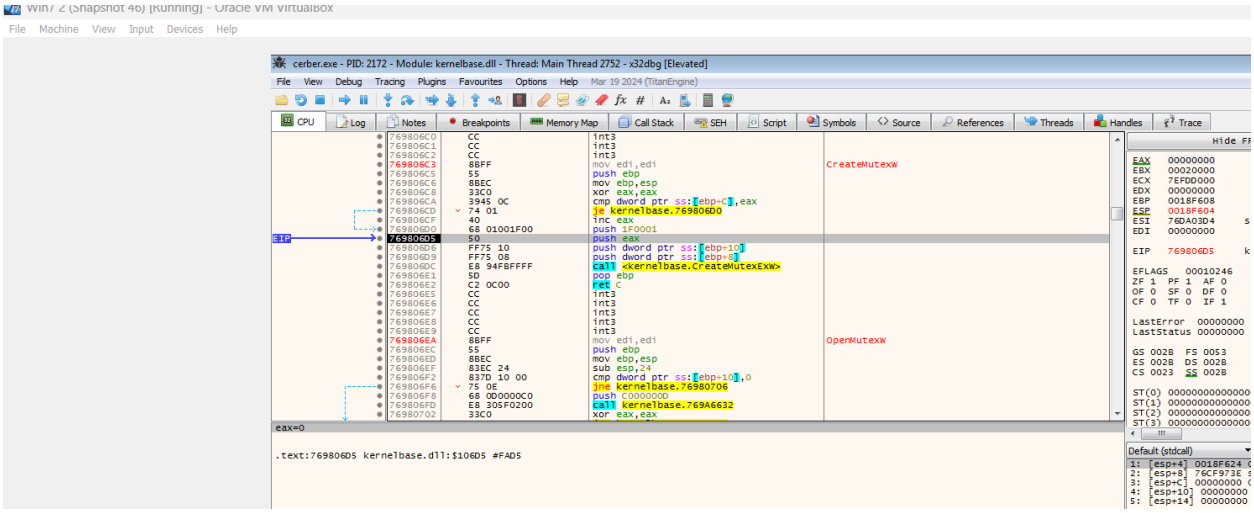


Retrieves VirtualAlloc pointer and adjusts a pointer related to decryption logic.

The malware is called VirtualAlloc, a Windows API used for allocating memory in the address space of the calling process. The returned memory address is stored in the global variable DAT_0046184c. It then reads (returns) a DWORD value from an offset (+4) within the newly allocated memory block suggesting the payload or configuration data might be stored there after dynamic decryption or unpacking.

Dynamic Analysis – x32dbg Runtime Inspection





Behavior Observed

- Execution begins at 0044FE40
- Breakpoint triggered on first instruction (INT3), confirming entry into actual malware logic.

Mutex Behavior

Call to CreateMutexW:

CALL dword ptr ds: [CreateMutexW]

Indicates that Cerber is creating a mutex object, likely to:

- Ensure only one instance is running.

File/Directory Activity

can also see CreateDirectoryW being resolved right below, which suggests

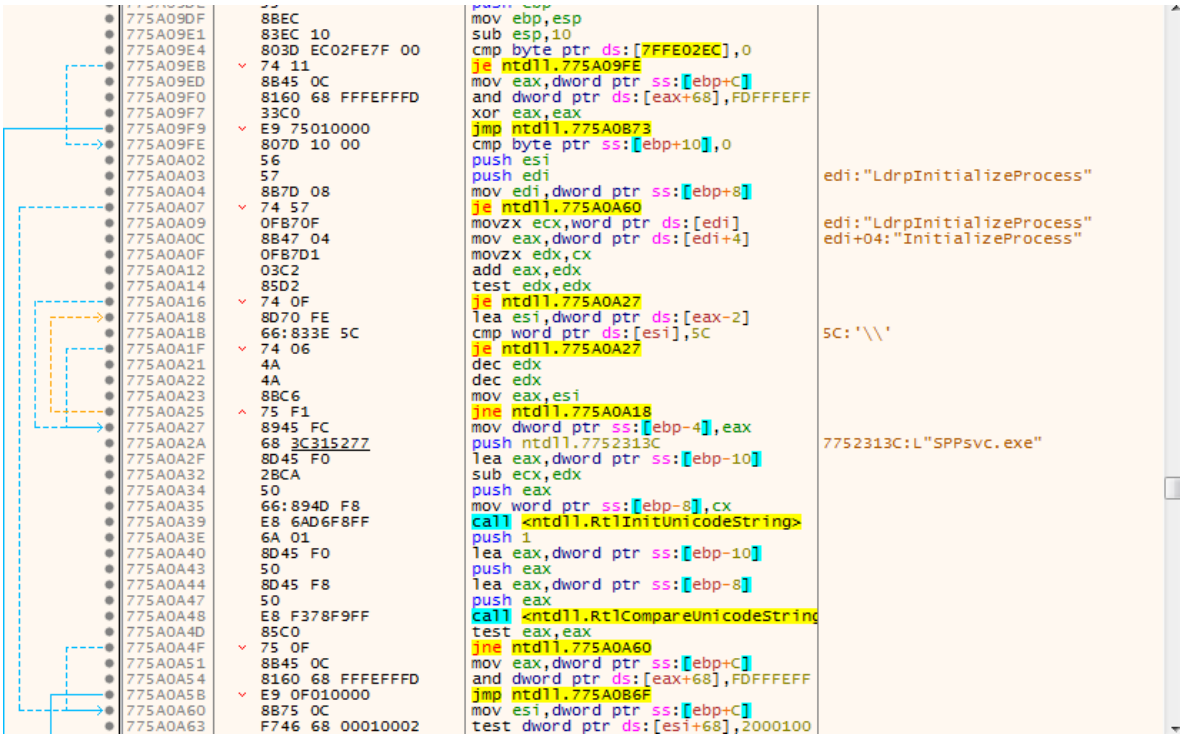
- Cerber attempts to create directories, possibly to:
    - Drop encrypted files or payloads
    - Store logs, ransom notes, or config

Execution Flow

- In screenshot it can be seen, we are at the entry point (EP): 0044FE40, inside the malware's main routine.
- Successfully broke at the first instruction, which is great for unpacking or instrumentation.
- The instructions call Windows API and it suggests that the unpacking stub has passed and entered in the real payload.

CreateMutexW	Ensures singleton instance.
CreateDirectoryW	Create directories for ransom notes or file drops.
CompareFileTime	It may be used to check the last modified timestamps on files or to evade check on sandbox time.

During reverse engineering, the string **SPSvc.exe** was identified which was being compared to using Unicode string. This executable is not a legitimate Windows system file and appears to be used by Cerber ransomware either for self-identification or for creating a fake service to work stealthily in infected systems.

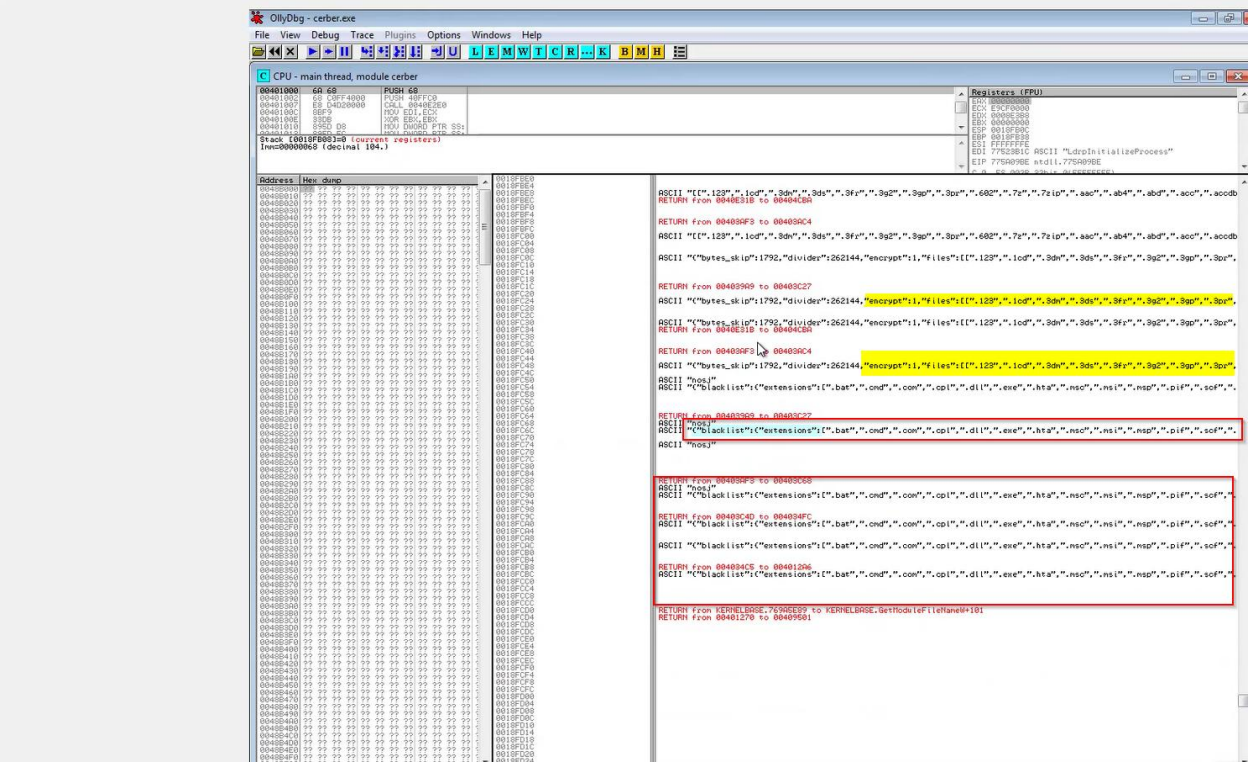


3. Ollydbg Runtime Inspection

It was observed that it decrypts the data using CryptoAPI, which contains the following information:

- Certain file types and directories are blocked from processing.
- Countries are excluded based on their system Language ID settings.
- Specific file types are deliberately targeted for action.
- The public RSA encryption key and ransom note are encoded in Base64 and delivered in HTML format.
- A plain text (txt) version of the ransom note is also provided.

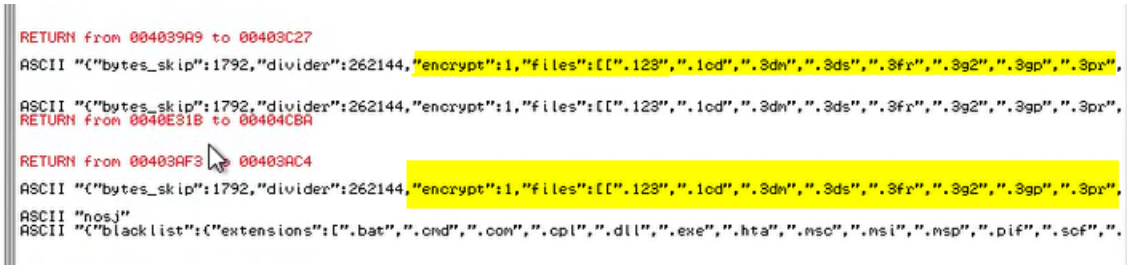
This screenshot shows **OllyDbg** running a Cerber ransomware sample, revealing decrypted strings that provide valuable insights into its behavior.



Key Observations from the (Decrypted Strings)

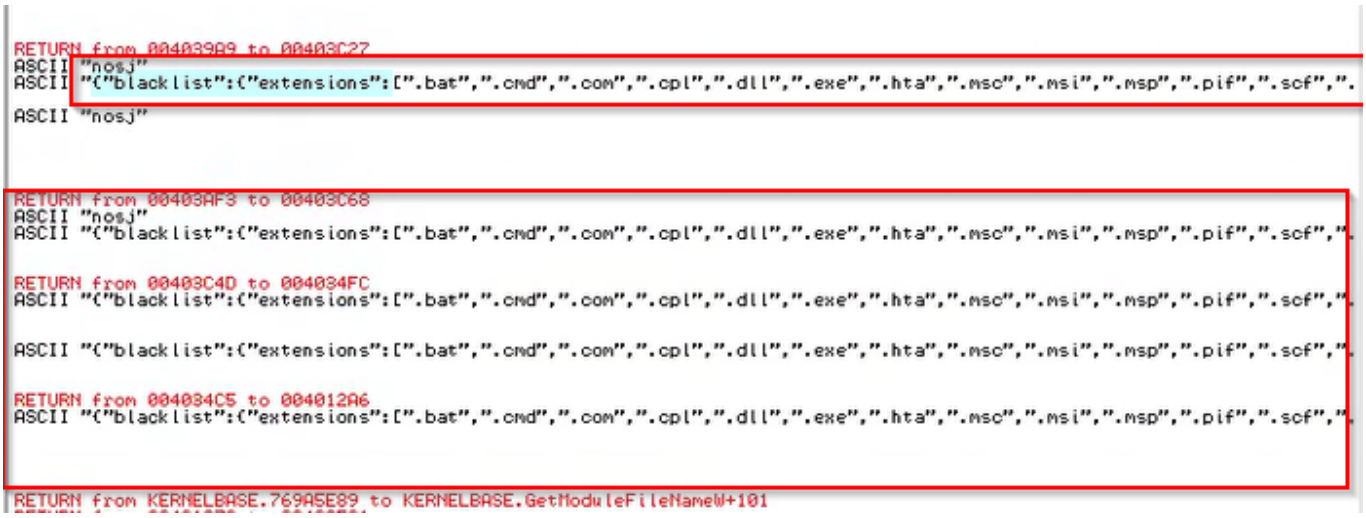
Encryption Configuration

The highlighted strings indicates Cerber's encryption configuration, targeting specific file extensions for encryption.

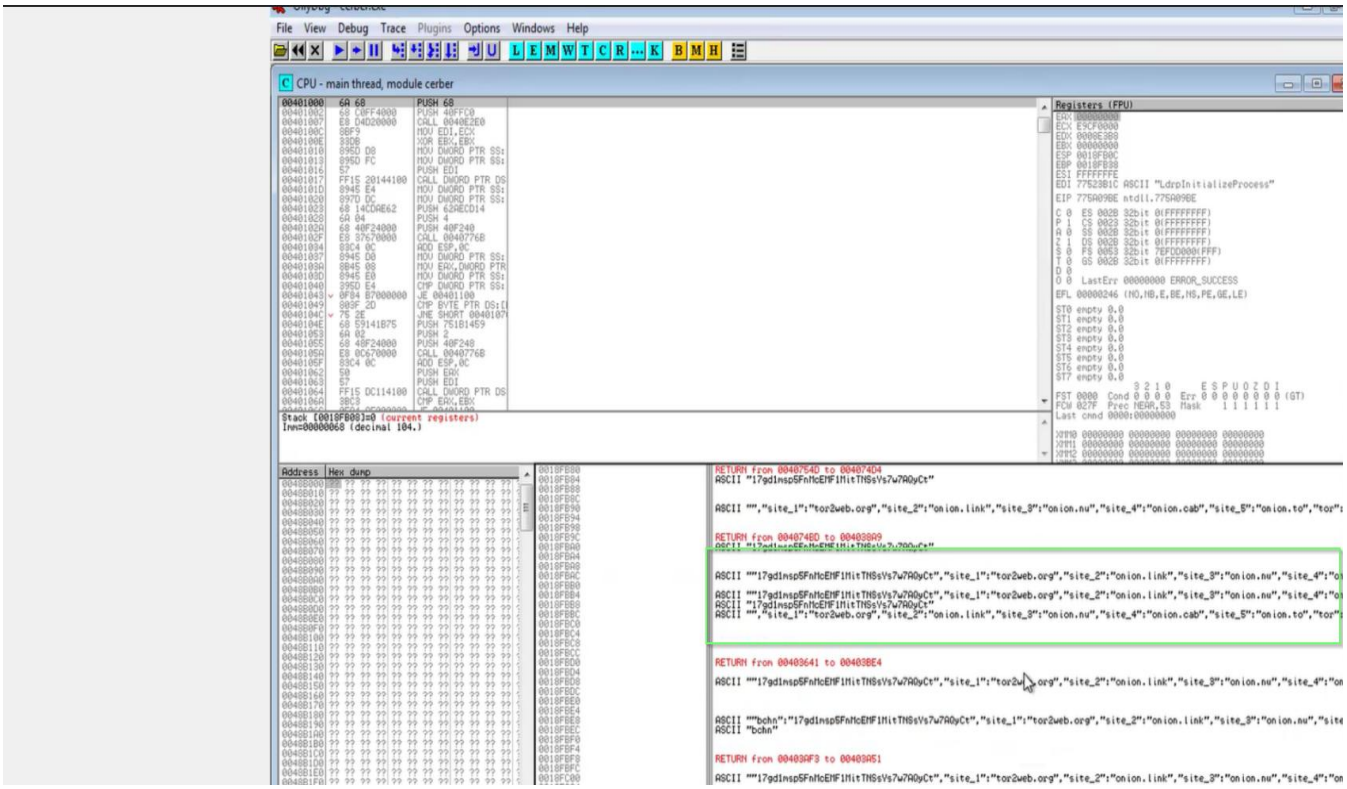


Targeted File Types

It shows that Cerber malware avoids encrypting the system's critical and executable files. It helps ensure system works well, ensuring the ransom message can still be displayed and the system isn't crashed before payment.



The screenshot below from OllyDbg shows more decrypted data from the Cerber, focusing on its command-and-control (C2) infrastructure and payment sites. It was seen that Tor gateway domains that map. Onion addresses regular web access via clear web.



String Repetition Across Returns

The decrypted data below reveals that Cerber includes a list of Tor gateway domains to contact its servers without requiring a Tor browser. These may be used for delivering the ransom note, accepting decryption keys, or communicating status.

Repeats across different return logs. It can be possibly-

- An encrypted user session key
- A ransomware campaign ID or
- A hardcoded identifier for decoding or validation

Targeted Folders

These show Cerber's targeting critical and user-specific directories like Microsoft Office, Excel, and SQL Server data folders. These typically might contain sensitive information:

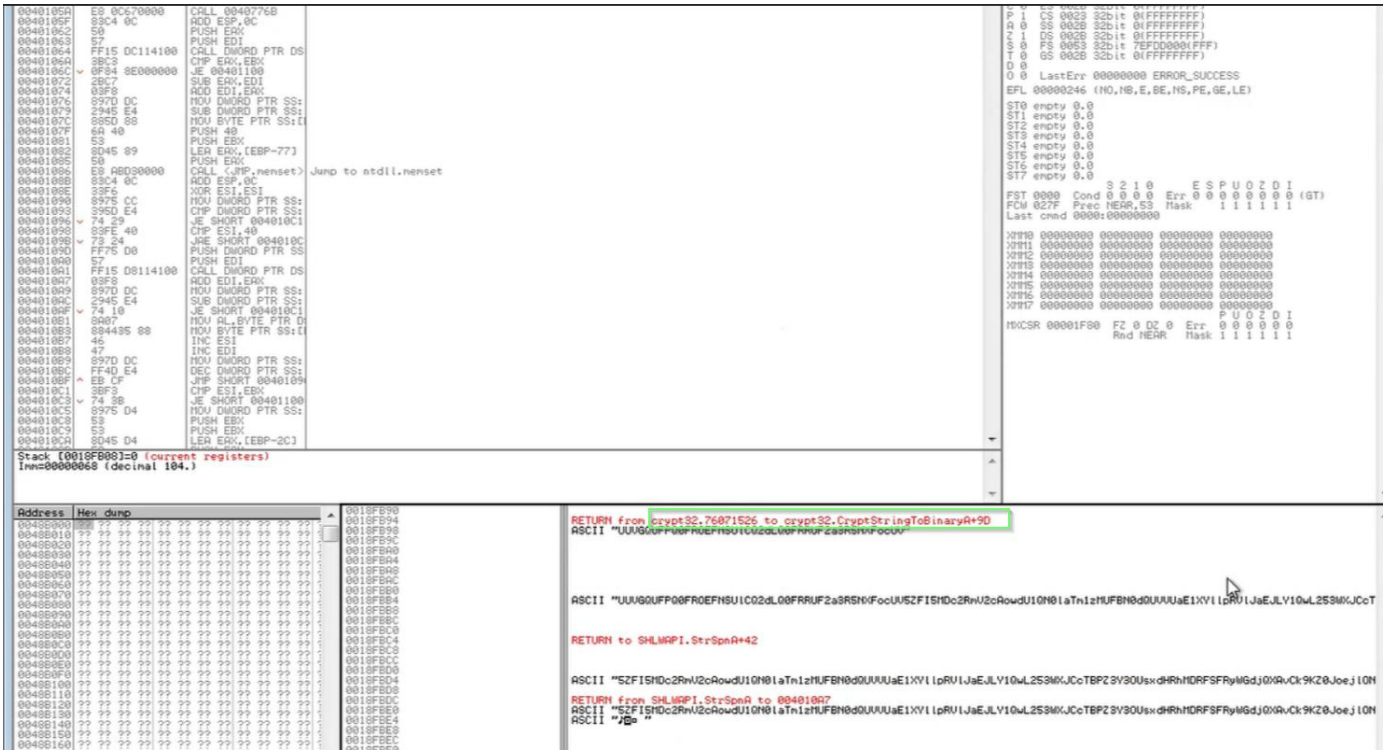
- Business sensitive documents
- Financial spreadsheets
- Database backups, etc.

Cerber to maximize impact and encourage ransom payment uses these directories.

Decryption Keys / Encryption Configuration

```
ASCII ""\\microsoft sql server\\","\\microsoft\\excel\\","\\microsoft\\microsoft sql server\\","\\microsoft\\office\\","

RETURN from 0040767E to 0040777E
```



This is a base64-encoded binary, which can be:

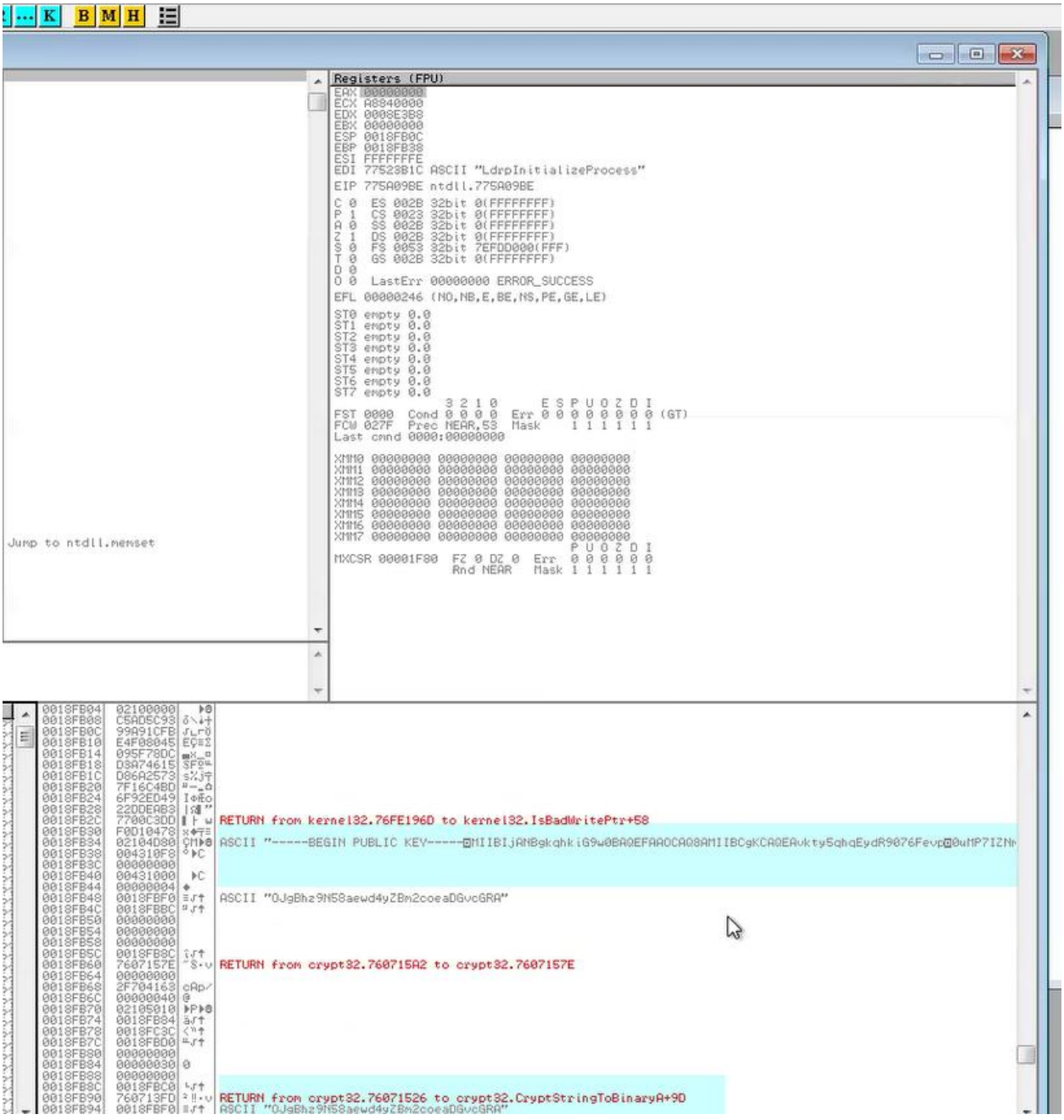
- An embedded public key for file encryption
- AES key

The API CryptoStringToBinaryW confirms this is being decoded and interpreted at runtime.

- Decrypt base64 string using CryptoStringToBinaryW
- Use resulting binary as cryptographic key.
- Proceed to encrypt files using WinAPI cryptographic calls.

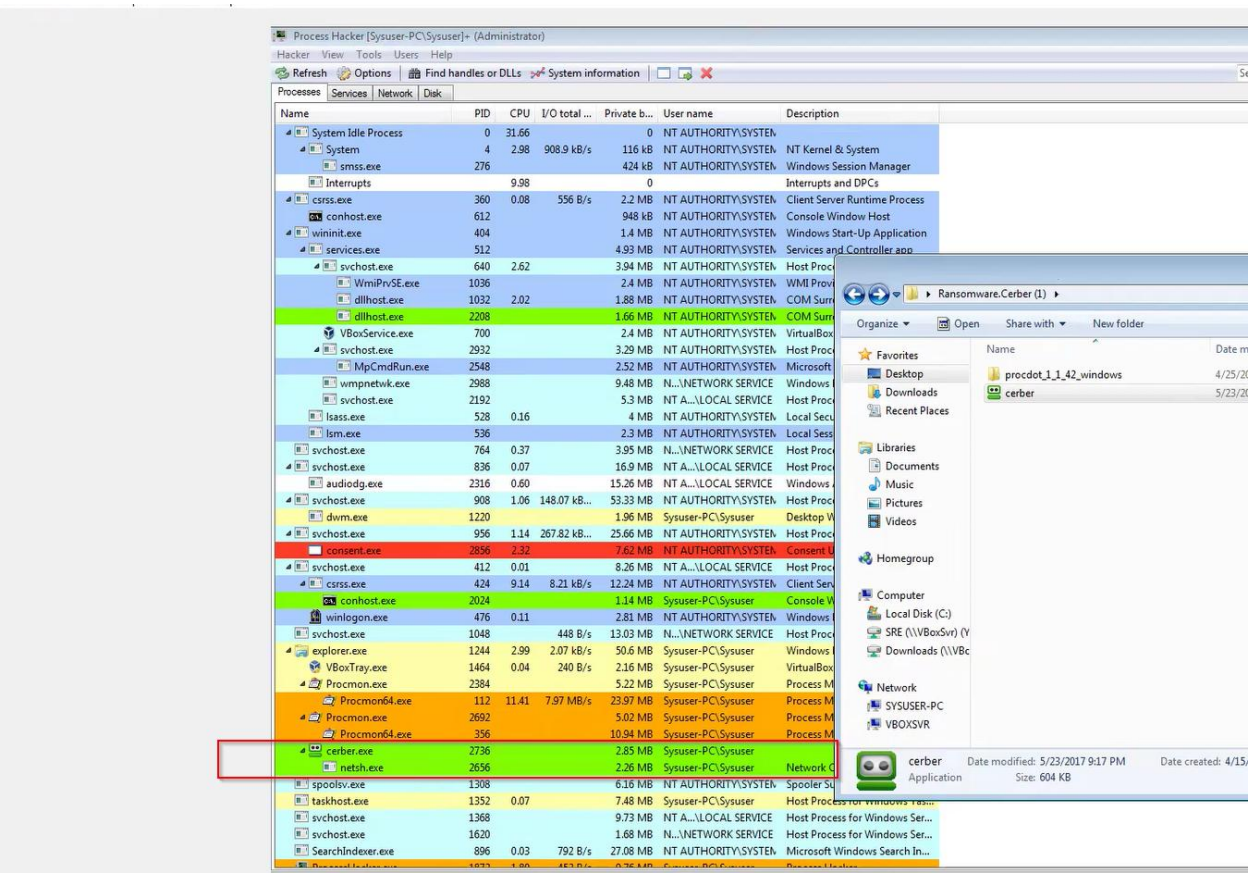
This is the **attacker's public key**.

Used by Cerber to **encrypt the symmetric keys** (AES keys) used on each victim file.



- Without the corresponding private key, decrypting victim files is impossible This captured public key could help in research to identify variants but won't allow direct file recovery without a flaw or the private key.

Cerber's runtime payload Execution

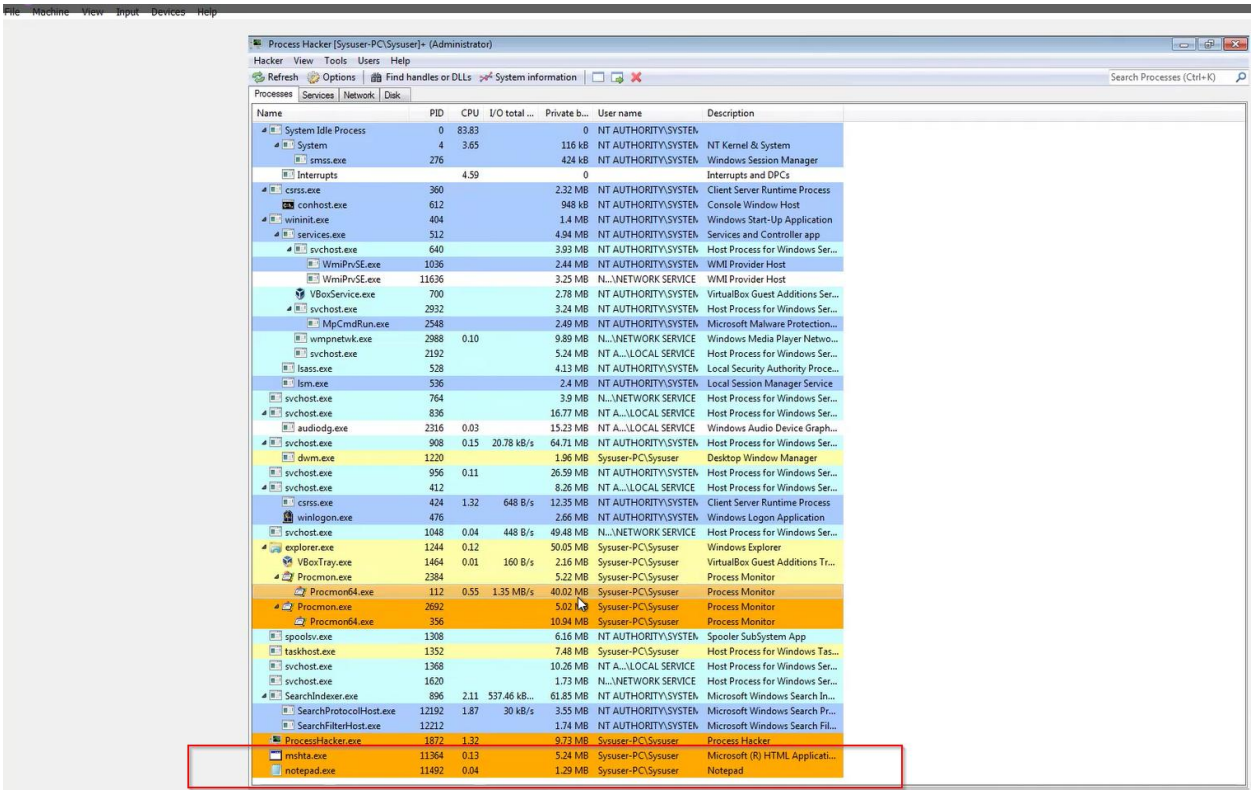


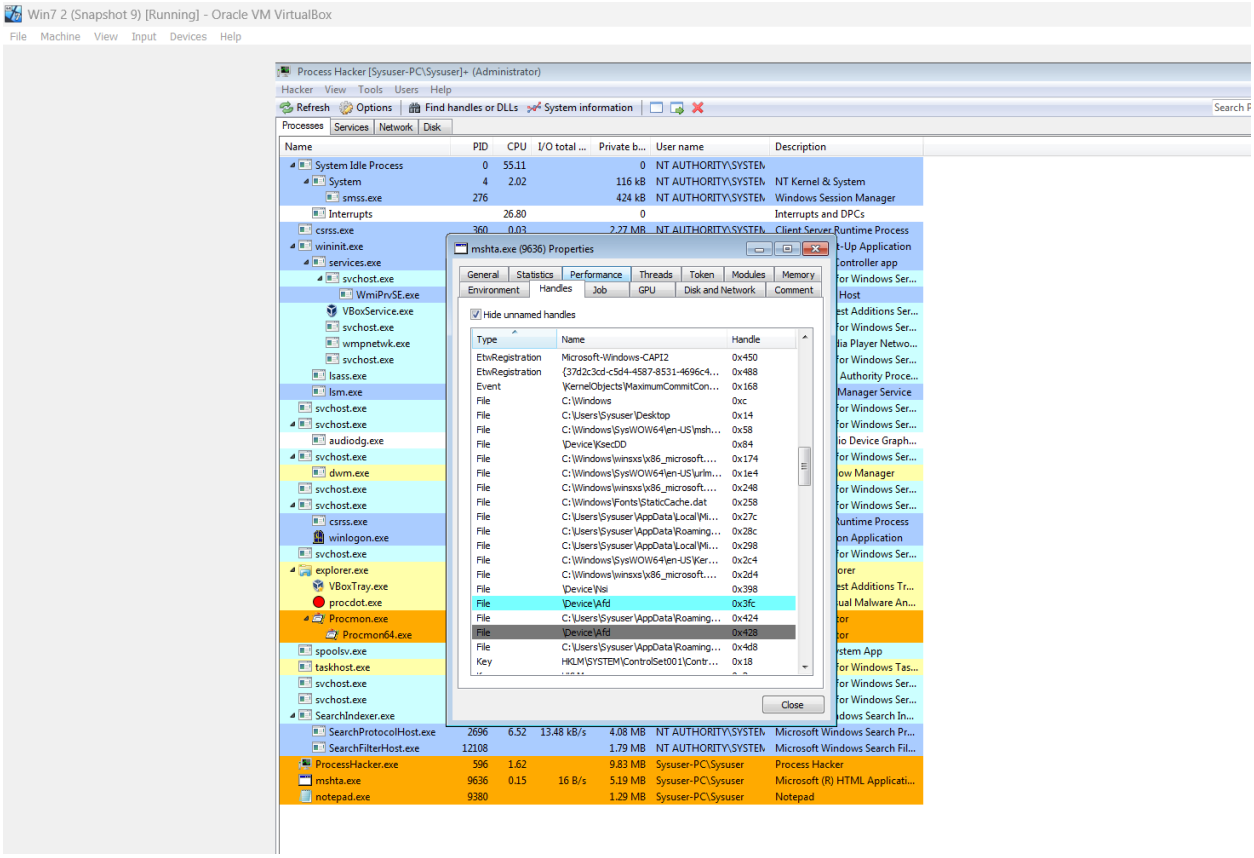
Using Process Explorer, we can see that cerber.exe spawns two other processes, mshta.exe and notepad.exe and then kills itself. (The Notepad and mshta.exe applications display ransom messages.

- Cerber spawns mshta.exe to show ransom notes.
- Parent process of mshta.exe that is cerber killed itself (dropper removed itself)
- Handle to \Device\Afd as shown in below screenshot confirms network connection from mshta.exe

Command Line:

- mshta.exe "C:\Users\Syuser\Desktop\R_E_A_D__T_H_I_S__B_O_S_S_.hta"


File Machine View Input Devices Help
Process Hacker [Sysuser-PC\Sysuser]+ (Administrator)
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk
Name PID CPU I/O total ... Private b... User name Description
System Idle Process 0 83.83 0 NT AUTHORITY\SYSTEM
System 4 3.65 116 kB NT AUTHORITY\SYSTEM NT Kernel & System
smss.exe 276 424 kB NT AUTHORITY\SYSTEM Windows Session Manager
Interrupts 4.59 0 Interrupts and DPCs
csrss.exe 360 2.32 MB NT AUTHORITY\SYSTEM Client Server Runtime Process
conhost.exe 612 948 kB NT AUTHORITY\SYSTEM Console Window Host
wininit.exe 404 1.4 MB NT AUTHORITY\SYSTEM Windows Start-Up Application
services.exe 512 4.94 MB NT AUTHORITY\SYSTEM Services and Controller app
svchost.exe 640 3.93 MB NT AUTHORITY\SYSTEM Host Process for Windows Ser...
WmiPrvSE.exe 1036 2.44 MB NT AUTHORITY\SYSTEM WMI Provider Host
WmiPrvSE.exe 11636 3.25 MB N...\NETWORK SERVICE WMI Provider Host
VBoxService.exe 700 2.78 MB NT AUTHORITY\SYSTEM VirtualBox Guest Additions Ser...
svchost.exe 2932 3.24 MB NT AUTHORITY\SYSTEM Host Process for Windows Ser...
MpCmdRun.exe 2548 2.49 MB NT AUTHORITY\SYSTEM Microsoft Malware Protection...
wmpnetwk.exe 2988 0.10 9.89 MB N...\NETWORK SERVICE Windows Media Player Netwo...
svchost.exe 2192 5.24 MB NT A...\LOCAL SERVICE Host Process for Windows Ser...
lsass.exe 528 4.13 MB NT AUTHORITY\SYSTEM Local Security Authority Proce...
lsm.exe 536 2.4 MB NT AUTHORITY\SYSTEM Local Session Manager Service
svchost.exe 764 3.9 MB N...\NETWORK SERVICE Host Process for Windows Ser...
svchost.exe 836 16.77 MB NT A...\LOCAL SERVICE Host Process for Windows Ser...
audiodg.exe 2316 0.03 15.23 MB NT A...\LOCAL SERVICE Windows Audio Device Graph...
svchost.exe 908 0.15 20.78 kB/s 64.71 MB NT AUTHORITY\SYSTEM Host Process for Windows Ser...
dwm.exe 1220 1.96 MB Sysuser-PC\Sysuser Desktop Window Manager
svchost.exe 956 0.11 26.59 MB NT AUTHORITY\SYSTEM Host Process for Windows Ser...
svchost.exe 412 8.26 MB NT A...\LOCAL SERVICE Host Process for Windows Ser...
csrss.exe 424 1.32 648 B/s 12.35 MB NT AUTHORITY\SYSTEM Client Server Runtime Process
winlogon.exe 476 2.66 MB NT AUTHORITY\SYSTEM Windows Logon Application
svchost.exe 1048 0.04 448 B/s 49.48 MB N...\NETWORK SERVICE Host Process for Windows Ser...
explorer.exe 1244 0.12 50.05 MB Sysuser-PC\Sysuser Windows Explorer
VBoxTray.exe 1464 0.01 160 B/s 2.16 MB Sysuser-PC\Sysuser VirtualBox Guest Additions Tr...
Procmon.exe 2384 5.22 MB Sysuser-PC\Sysuser Process Monitor
Procmon64.exe 112 0.55 1.35 MB/s 40.02 MB Sysuser-PC\Sysuser Process Monitor
Procmon.exe 2692 5.02 MB Sysuser-PC\Sysuser Process Monitor
Procmon64.exe 356 10.94 MB Sysuser-PC\Sysuser Process Monitor
spoolsv.exe 1308 6.16 MB NT AUTHORITY\SYSTEM Spooler SubSystem App
taskhost.exe 1352 7.48 MB Sysuser-PC\Sysuser Host Process for Windows Tas...
svchost.exe 1368 10.26 MB NT A...\LOCAL SERVICE Host Process for Windows Ser...
svchost.exe 1620 1.73 MB N...\NETWORK SERVICE Host Process for Windows Ser...
SearchIndexer.exe 896 2.11 537.46 kB... 61.85 MB NT AUTHORITY\SYSTEM Microsoft Windows Search In...
SearchProtocolHost.exe 12192 1.87 30 kB/s 3.55 MB NT AUTHORITY\SYSTEM Microsoft Windows Search Pr...
SearchFilterHost.exe 12212 1.74 MB NT AUTHORITY\SYSTEM Microsoft Windows Search Fil...
ProcessHacker.exe 1872 1.32 9.73 MB Sysuser-PC\Sysuser Process Hacker
mshta.exe 11364 0.13 5.24 MB Sysuser-PC\Sysuser Microsoft (R) HTML Applicati...
notepad.exe 11492 0.04 1.29 MB Sysuser-PC\Sysuser Notepad

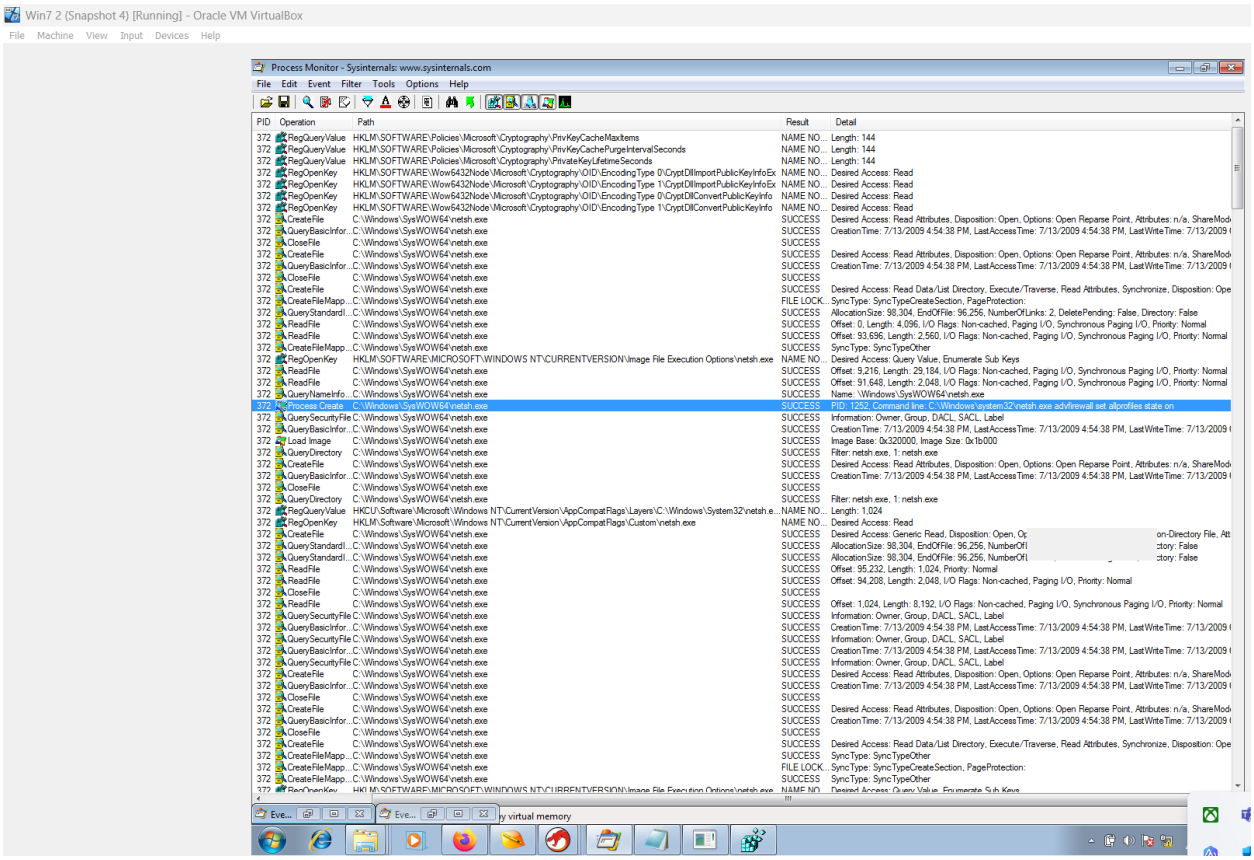

Win7 2 (Snapshot 9) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Process Hacker [Sysuser-PC\Sysuser]+ (Administrator)
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Processes Services Network Disk
Name PID CPU I/O total ... Private b... User name Description
System Idle Process 0 55.11 0 NT AUTHORITY\SYSTEM
System 4 2.02 116 kB NT AUTHORITY\SYSTEM NT Kernel & System
smss.exe 276 424 kB NT AUTHORITY\SYSTEM Windows Session Manager
Interrupts 26.80 0 Interrupts and DPCs
csrss.exe 360 0.03 2.27 MB NT AUTHORITY\SYSTEM Client Server Runtime Process
wininit.exe
services.exe
svchost.exe
WmiPrvSE.exe
VBoxService.exe
svchost.exe
wmpnetwk.exe
svchost.exe
lsass.exe
lsm.exe
svchost.exe
svchost.exe
audiodg.exe
svchost.exe
dwm.exe
svchost.exe
svchost.exe
csrss.exe
winlogon.exe
svchost.exe
explorer.exe
VBoxTray.exe
procdot.exe
Procmon.exe
Procmon64.exe
spoolsv.exe
taskhost.exe
svchost.exe
svchost.exe
SearchIndexer.exe
SearchProtocolHost.exe 2696 6.52 13.48 kB/s 4.08 MB NT AUTHORITY\SYSTEM Microsoft Windows Search Pr...
SearchFilterHost.exe 12108 1.79 MB NT AUTHORITY\SYSTEM Microsoft Windows Search Fil...
ProcessHacker.exe 596 1.62 9.83 MB Sysuser-PC\Sysuser Process Hacker
mshta.exe 9636 0.15 16 B/s 5.19 MB Sysuser-PC\Sysuser Microsoft (R) HTML Applicati...
notepad.exe 9380 1.29 MB Sysuser-PC\Sysuser Notepad
mshta.exe (9636) Properties
General Statistics Performance Threads Token Modules Memory
Environment Handles Job GPU Disk and Network Comment
Hide unnamed handles
Type Name Handle
EtwRegistration Microsoft-Windows-CAPI2 0x450
EtwRegistration {37d2c3cd-c5d4-4587-8531-4696c4... 0x488
Event \KernelObjects\MaximumCommitCon... 0x168
File C:\Windows 0xc
File C:\Users\Sysuser\Desktop 0x14
File C:\Windows\SysWOW64\en-US\msh... 0x58
File \Device\KsecDD 0x84
File C:\Windows\winsxs\x86_microsoft.... 0x174
File C:\Windows\SysWOW64\en-US\urlm... 0x1e4
File C:\Windows\winsxs\x86_microsoft.... 0x248
File C:\Windows\Fonts\StaticCache.dat 0x258
File C:\Users\Sysuser\AppData\Local\Mi... 0x27c
File C:\Users\Sysuser\AppData\Roaming... 0x28c
File C:\Users\Sysuser\AppData\Local\Mi... 0x298
File C:\Windows\SysWOW64\en-US\Ker... 0x2c4
File C:\Windows\winsxs\x86_microsoft.... 0x2d4
File \Device\Nsi 0x398
File \Device\Afd 0x3fc
File C:\Users\Sysuser\AppData\Roaming... 0x424
File \Device\Afd 0x428
File C:\Users\Sysuser\AppData\Roaming... 0x4d8
Key HKLM\SYSTEM\ControlSet001\Contr... 0x18
Close

The presence of \Device\Afd in the handles tab for mshta.exe is a key behavioral indicator in malware analysis.

Active network socket, proving that mshta.exe might have attempted a C2 callback.

5. Evasion and Persistence Techniques

Cerber exhibits advanced capabilities by identifying and configuring Windows firewall rules to stop outbound traffic from installed firewalls, antivirus, and anti-spyware products. This tactic aims to disrupt the communication and functionality of these security tools, potentially enhancing the ransomware's ability to evade detection. This sophisticated evolving nature of Cerber, posing a significant challenge for cybersecurity.



Process Information

- Executable: C:\Windows\SysWOW64\netsh.exe

- Process ID (PID): 372
- Command Line Used:

netsh.exe advfirewall set allprofiles state on

- This command enables the Windows Firewall for all profiles (Domain, Private, Public).

Suspicious Behavior Indicators

1. Use of netsh.exe

- netsh.exe is a legitimate Windows utility used for network configuration.
- Malware mainly abuses it to manipulate firewall settings.
- In this case, turning the firewall ON is odd because:
    - Cerber seemed disabling the firewall to allow outbound traffic (C2 communication).
    - If it's turning it ON, it might be trying to block incident response or stop Antivirus communications after the payload execution.

2. Registry Interaction

Accesses Image File Execution Options under:

- HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\netsh.exe

This suggests debugging prevention or redirection, used to:

- Hijack or monitor the execution of a binary.
- Implement persistence or anti-analysis techniques.

AppCompatFlags Entries seen accessing

These are usually used to modify compatibility settings for binaries.

- HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom

Malware can abuse these to make changes in the behavior of certain programs or bypass UAC.

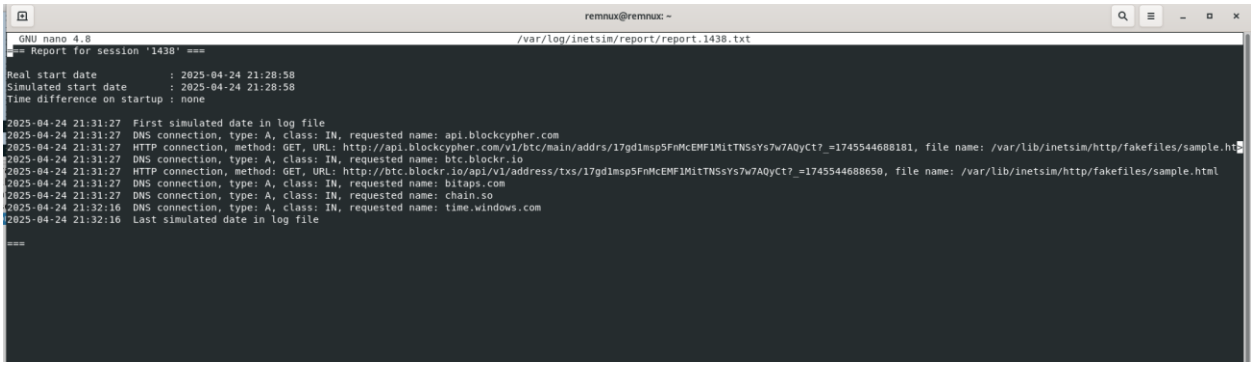
3. Strings of Interest (Post-Unpacking)

- shell1.ipc. {E4C88EE9-9C38-F0AB-9AA0-FDB1C0E16328} – Mutex/IPC channel identifier

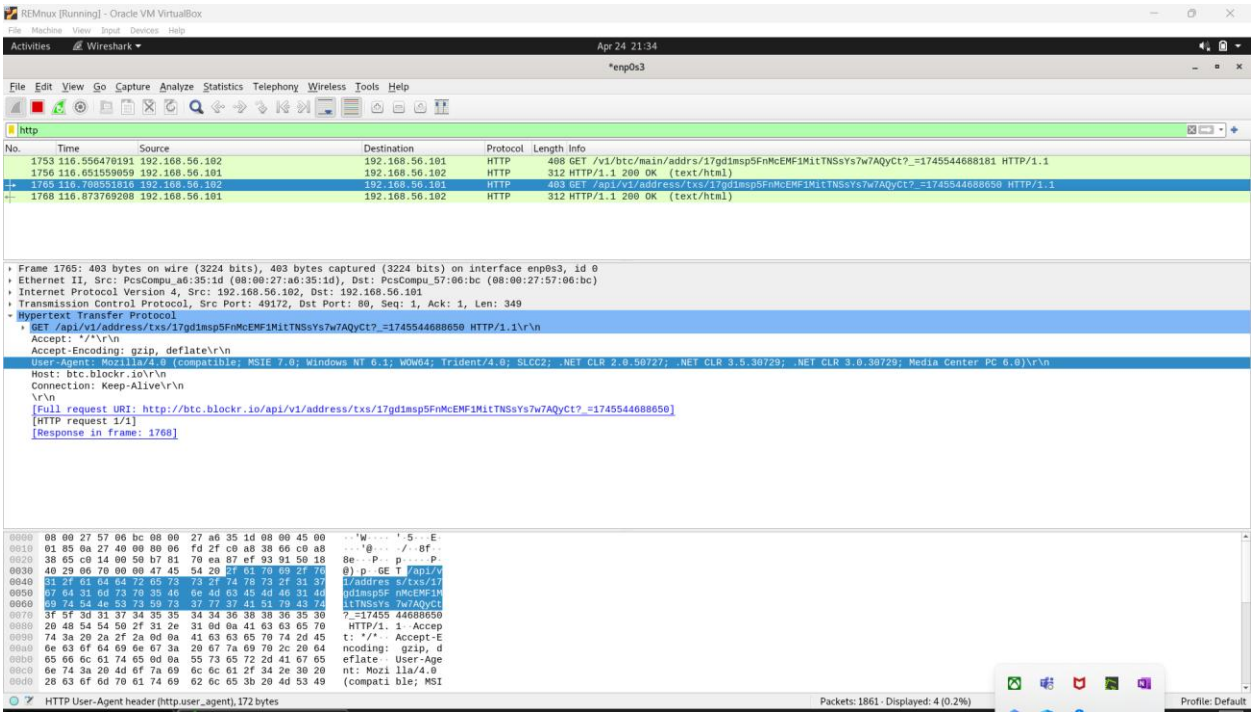
- R_E_A_D__T_H_I_S__<random>.hta – Naming convention for dropped ransom notes
- /v9/windowsupdate/redir/muv4wuredir.cab – Used in HEAD request evasion
- watson.microsoft.com/StageOne/Generic/WindowsUpdateFailure – It suggest it is pretending to be legitimate error reporting

These strings suggest C2 prep, evasion of sandbox detection, and use of legitimate URLs/domains to appear benign.

Network Traffic (via INetSim and Wireshark)



The INetSim session log reveals that the malware initiated several DNS and HTTP requests to cryptocurrency-related domains such as api.blockcypher.com, btc.blockr.io, bitaps.com, and chain.so, indicating an attempt to interact with public Bitcoin block explorers. The malware queried the balance and transaction history of the Bitcoin wallet address 17gdlmsp5FnMcEMFlMitTNSsYs7w7AQyCt, which suggests it was monitoring for incoming ransom payments. Additionally, the request to time.windows.com is commonly used for system time synchronization and could be part of timing evasion techniques. These behaviors are characteristic of ransomware, which rely on publicly available services to covertly verify ransom payments without directly exposing their command-and-control infrastructure.



api.blockcypher.com/v1/btc/main/addrs/17gdlmsp5FnMcEMFlMitTNSsYs7w7AQyCt?

btc.blockr.io/api/v1/address/txs/17gdlmsp5FnMcEMFlMitTNSsYs7w7AQyCt?...

Analysis

Both URLs referencing Bitcoin wallet address 17gdlmsp5FnMcEMFlMitTNSsYs7w7AQyCt.

The malware is checking wallet activity, likely to:

It confirms ransom payment & Track victim transactions.

Accessed fake file: /var/lib/inetsim/http/fakefiles/sample.html (generated by INetSim)

FUN_0044f1b0(0x20,0x6f); // Likely a memory init or allocation

- "interface\...}" or similar
- It may be preparing a registry key name or file path for access later.

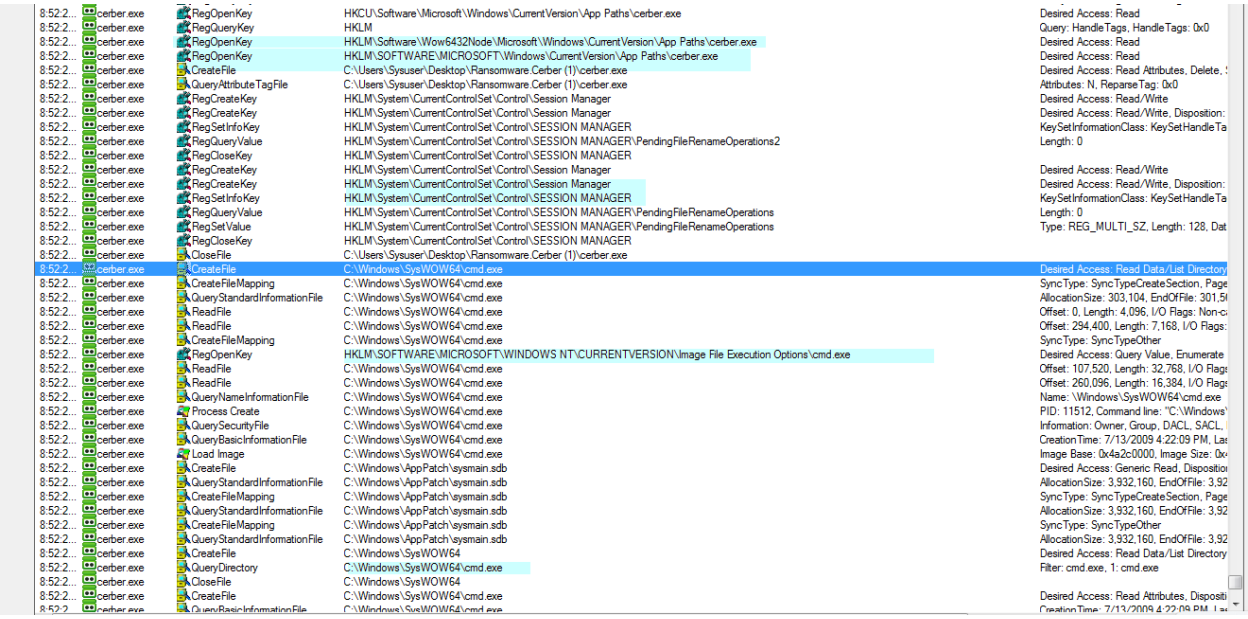
Registry Changes (via Reshot & ProcMon)

HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ImageExecutionOptions\cmd.exe

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\PendingFileRenameOperatios

HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers



8:52:2...	cerber.exe	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\App Paths\cerber.exe	Desired Access: Read
8:52:2...	cerber.exe	RegQueryKey	HKLM	Query: HandleTags, HandleTags: 0x0
8:52:2...	cerber.exe	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\App Paths\cerber.exe	Desired Access: Read
8:52:2...	cerber.exe	RegOpenKey	HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\App Paths\cerber.exe	Desired Access: Read
8:52:2...	cerber.exe	CreateFile	C:\Users\Sysuser\Desktop\Ransomware.Cerber (1)\cerber.exe	Desired Access: Read Attributes, Delete,
8:52:2...	cerber.exe	QueryAttributeTagFile	C:\Users\Sysuser\Desktop\Ransomware.Cerber (1)\cerber.exe	Attributes: N, ReparseTag: 0x0
8:52:2...	cerber.exe	RegCreateKey	HKLM\System\CurrentControlSet\Control\Session Manager	Desired Access: Read/Write
8:52:2...	cerber.exe	RegCreateKey	HKLM\System\CurrentControlSet\Control\Session Manager	Desired Access: Read/Write, Disposition:
8:52:2...	cerber.exe	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	KeySetInformationClass: KeySetHandleTa
8:52:2...	cerber.exe	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\PendingFileRenameOperations2	Length: 0
8:52:2...	cerber.exe	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	
8:52:2...	cerber.exe	RegCreateKey	HKLM\System\CurrentControlSet\Control\Session Manager	Desired Access: Read/Write
8:52:2...	cerber.exe	RegCreateKey	HKLM\System\CurrentControlSet\Control\Session Manager	Desired Access: Read/Write, Disposition:
8:52:2...	cerber.exe	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	KeySetInformationClass: KeySetHandleTa
8:52:2...	cerber.exe	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\PendingFileRenameOperations	Length: 0
8:52:2...	cerber.exe	RegSetValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\PendingFileRenameOperations	Type: REG_MULTI_SZ, Length: 128, Dat
8:52:2...	cerber.exe	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	
8:52:2...	cerber.exe	CloseFile	C:\Users\Sysuser\Desktop\Ransomware.Cerber (1)\cerber.exe	
8:52:2...	cerber.exe	CreateFile	C:\Windows\SysWOW64\cmd.exe	Desired Access: Read Data/List Directory
8:52:2...	cerber.exe	CreateFileMapping	C:\Windows\SysWOW64\cmd.exe	SyncType: SyncTypeCreateSection, Page
8:52:2...	cerber.exe	QueryStandardInformationFile	C:\Windows\SysWOW64\cmd.exe	AllocationSize: 303,104, EndOfFile: 301,5
8:52:2...	cerber.exe	ReadFile	C:\Windows\SysWOW64\cmd.exe	Offset: 0, Length: 4,096, I/O Flags: Non-c
8:52:2...	cerber.exe	ReadFile	C:\Windows\SysWOW64\cmd.exe	Offset: 294,400, Length: 7,168, I/O Flags:
8:52:2...	cerber.exe	CreateFileMapping	C:\Windows\SysWOW64\cmd.exe	SyncType: SyncTypeOther
8:52:2...	cerber.exe	RegOpenKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options\cmd.exe	Desired Access: Query Value, Enumerate
8:52:2...	cerber.exe	ReadFile	C:\Windows\SysWOW64\cmd.exe	Offset: 107,520, Length: 32,768, I/O Flags
8:52:2...	cerber.exe	ReadFile	C:\Windows\SysWOW64\cmd.exe	Offset: 260,096, Length: 16,384, I/O Flags
8:52:2...	cerber.exe	QueryNameInformationFile	C:\Windows\SysWOW64\cmd.exe	Name: \Windows\SysWOW64\cmd.exe
8:52:2...	cerber.exe	Process Create	C:\Windows\SysWOW64\cmd.exe	PID: 11512, Command line: "C:\Windows\
8:52:2...	cerber.exe	QuerySecurityFile	C:\Windows\SysWOW64\cmd.exe	Information: Owner, Group, DACL, SACL,
8:52:2...	cerber.exe	QueryBasicInformationFile	C:\Windows\SysWOW64\cmd.exe	CreationTime: 7/13/2009 4:22:09 PM, Las
8:52:2...	cerber.exe	Load Image	C:\Windows\SysWOW64\cmd.exe	Image Base: 0x4a2c0000, Image Size: 0x
8:52:2...	cerber.exe	CreateFile	C:\Windows\AppPatch\sysmain.sdb	Desired Access: Generic Read, Disposition
8:52:2...	cerber.exe	QueryStandardInformationFile	C:\Windows\AppPatch\sysmain.sdb	AllocationSize: 3,932,160, EndOfFile: 3,92
8:52:2...	cerber.exe	CreateFileMapping	C:\Windows\AppPatch\sysmain.sdb	SyncType: SyncTypeCreateSection, Page
8:52:2...	cerber.exe	QueryStandardInformationFile	C:\Windows\AppPatch\sysmain.sdb	AllocationSize: 3,932,160, EndOfFile: 3,92
8:52:2...	cerber.exe	CreateFileMapping	C:\Windows\AppPatch\sysmain.sdb	SyncType: SyncTypeOther
8:52:2...	cerber.exe	QueryStandardInformationFile	C:\Windows\AppPatch\sysmain.sdb	AllocationSize: 3,932,160, EndOfFile: 3,92
8:52:2...	cerber.exe	CreateFile	C:\Windows\SysWOW64	Desired Access: Read Data/List Directory
8:52:2...	cerber.exe	QueryDirectory	C:\Windows\SysWOW64\cmd.exe	Filter: cmd.exe, 1: cmd.exe
8:52:2...	cerber.exe	CloseFile	C:\Windows\SysWOW64	
8:52:2...	cerber.exe	CreateFile	C:\Windows\SysWOW64\cmd.exe	Desired Access: Read Attributes, Disposi
8:52:2...	cerber.exe	QueryBasicInformationFile	C:\Windows\SysWOW64\cmd.exe	CreationTime: 7/13/2009 4:22:09 PM, La

During the analysis of Cerber ransomware, several key registry modifications were observed that contribute to its persistence, evasion, and user restriction strategies. The Image File Execution Options registry key was used to hijack the execution of cmd.exe, preventing users from accessing the command prompt for analysis. Cerber also modified the Explorer\Shell Folders key under the current user to obfuscate or redirect file paths, making it harder for victims to locate encrypted files. The PendingFileRenameOperations key under the Session Manager was leveraged to schedule the deletion of its components upon reboot, allowing Cerber to clean up its dropper or artifacts post-infection. Furthermore, ransomware abused the AppCompatFlags\Layers registry entry to alter the behavior of native Windows binaries, this can bypass security prompts or enforce compatibility modes that favor malicious execution. Lastly, Cerber targeted the Applets\Regedit key to disable or manipulate access to the Windows Registry Editor, effectively blocking users from investigating or reversing registry-level changes. These registry edits collectively demonstrate Cerber's focus on stealth, persistence, and disruption of system-level recovery mechanisms.

Also, HKLM\SYSTEM\...\Firewall Rules\... Cerber modified firewall rules (Action=Allow, Active=FALSE) for various services and UDP/TCP ports — likely to allow its own communication or reduce detection by disabling logging or interfering with firewall enforcement

In detail about cmd.exe

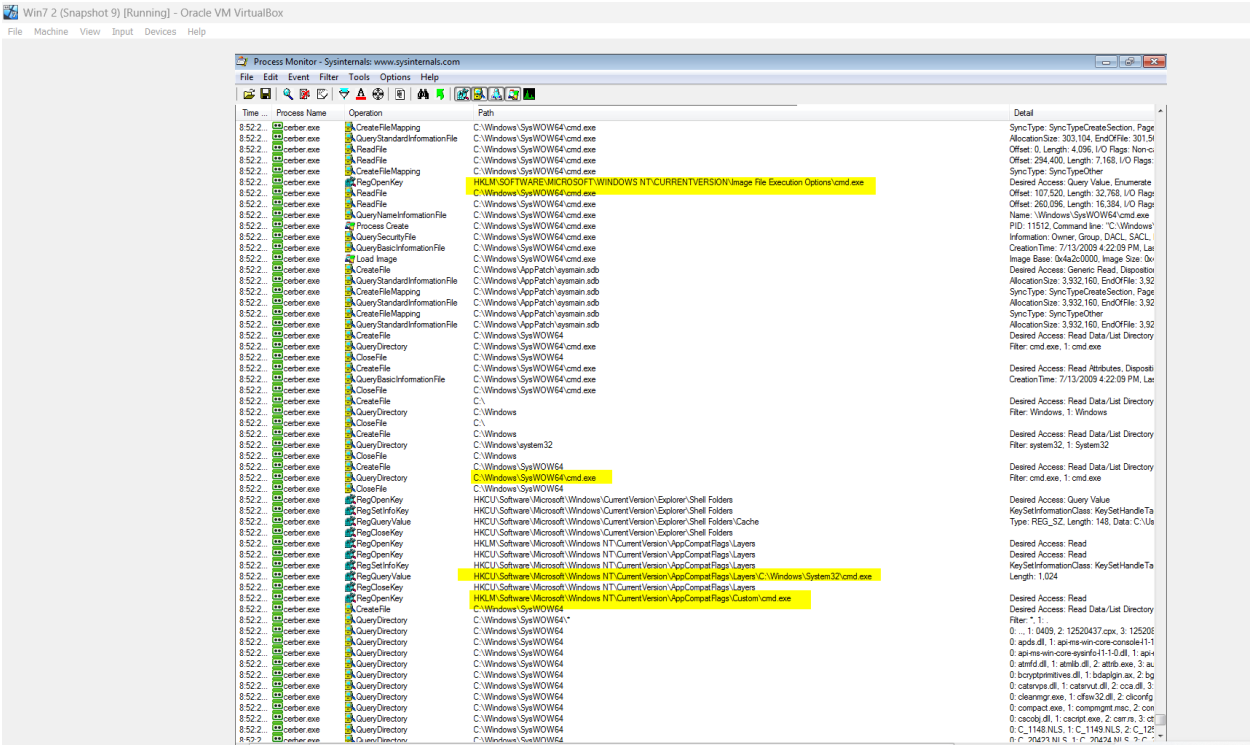
Command Line (cmd.exe) Abuse

C:\Windows\SysWOW64\cmd.exe

- Multiple reads, mappings, and process creations.
- Indicates Cerber may invoke scripts or commands silently.
- Also manipulated via registry at:

Image File Execution Options\cmd.exe

Impact: Post-encryption scripting, registry manipulation, or system hijacking.



<u>Post malware execution changes were made to the filesystem</u>

File Modifications (ProcMon)

File Encryption Behavior

From multiple screenshots (esp. the first and second):

- Cerber accesses and modifies files on desktop and there
- Files are read and then written with .hta, .bt, .8856 extensions and renamed.
- Ransomware behavior:
    - Read original → Encrypt in memory → Write encrypted version → delete original

Encrypted user documents in desktop. After further analysis it was observed it wasn't only affecting the desktop but another folder as well.

How Encryption Worked

The malware generates an RSA key pair, utilizing the public key to encrypt a randomly generated AES key. This AES key is then employed to encrypt the victim's files. The corresponding RSA private key is retained by the threat actors to enable file decryption upon payment of the ransom. The encryption process is extremely fast, capable of encrypting gigabytes of data within minutes or hours. Once a victim's files are encrypted, Cerber displays a ransom note with payment instructions. The ransom note is displayed as a text file.

Ransom Note Dropping

Seen in multiple paths like:

- R_E_A_D__T_H_I_S__BBHU4H0_.hta
- R_E_A_D__T_H_I_S__6L6MYZQ_.hta
- R_E_A_D__T_H_I_S__TOD2D_.hta

These ransom notes:

- Are generated dynamically
- Dropped into multiple folders where files are encrypted
- Likely rendered via **mshta.exe** after encryption

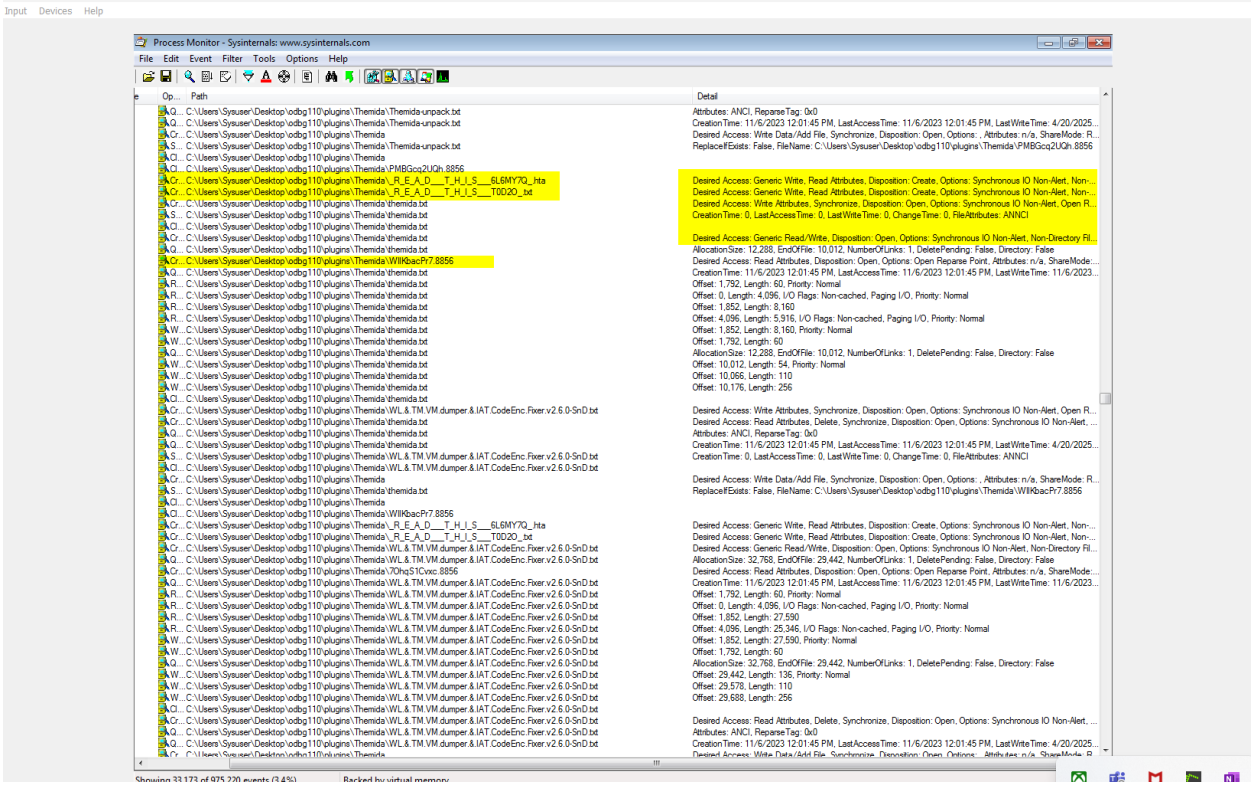
Impact: Ensures victim sees ransom instructions regardless of where they browse.

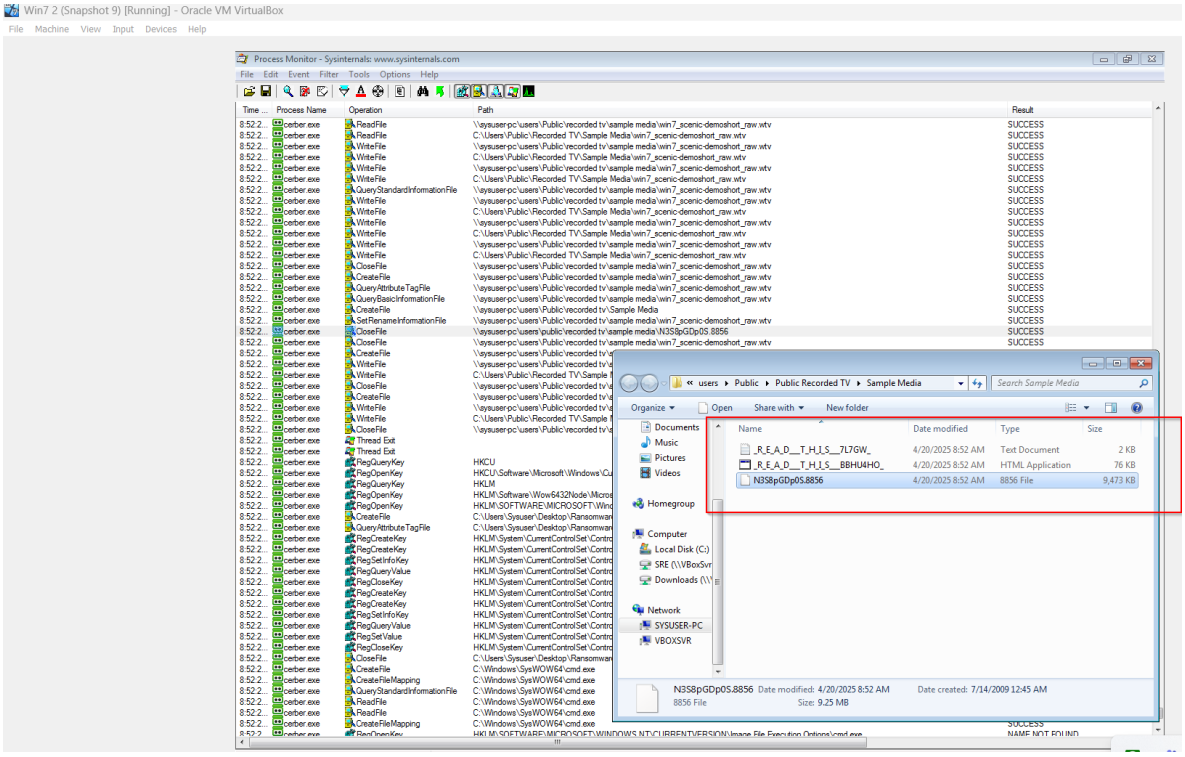
Modified Files:

- *.py, *.txt, *.8856, *.bt, *.wtv, .sdb extensions encrypted
- Ransom notes dropped:
    - R_E_A_D__T_H_I_S__TOD2D_.hta
    - R_E_A_D__T_H_I_S__B_O_S_S_.hta

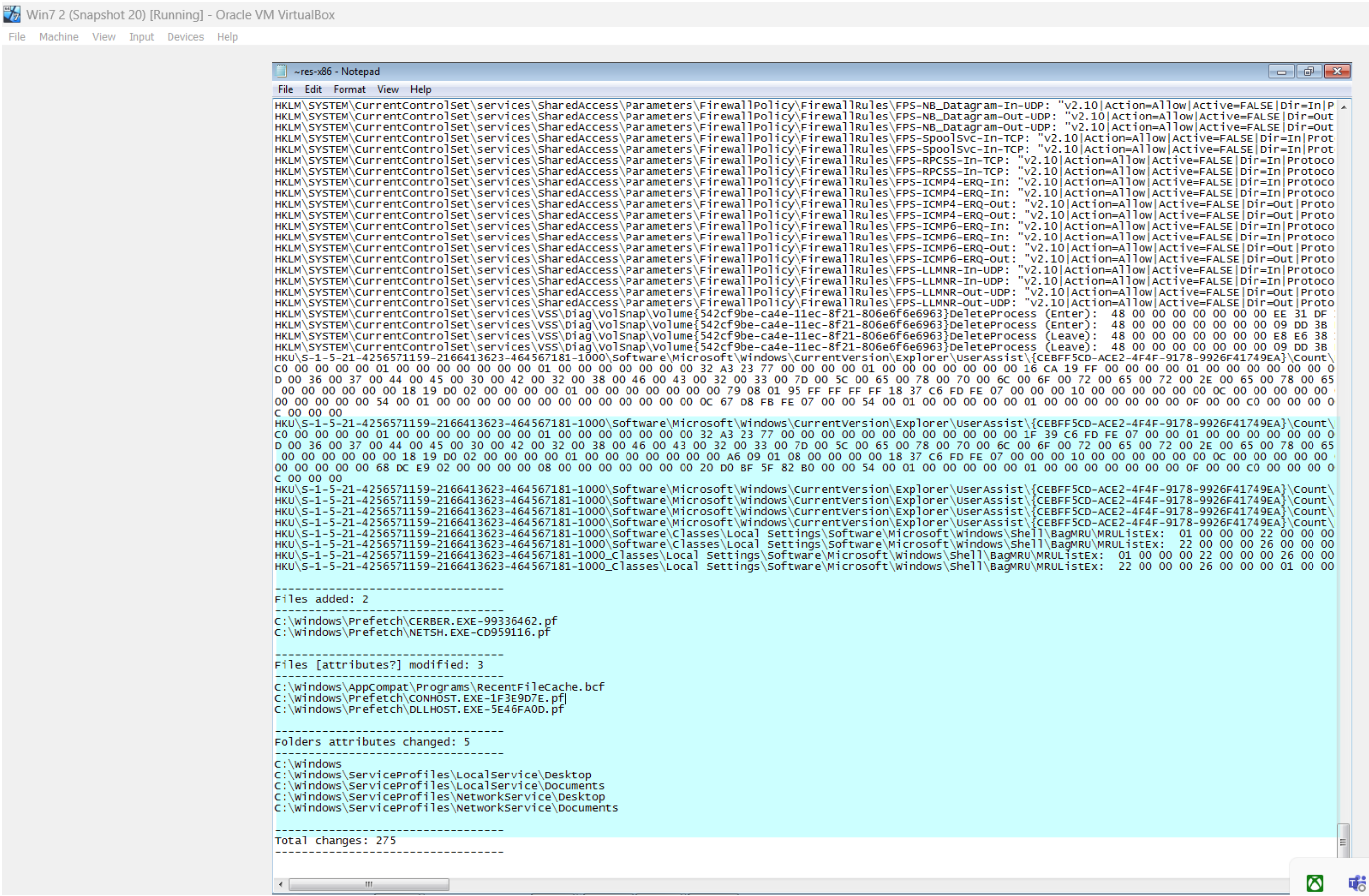
Observations:

- Files are read, encrypted, and written with random extensions
- Multiple ransom notes ensure victim visibility


Input Devices Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Op... Path
Detail


Win7 2 (Snapshot 9) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name Operation Path Result
Organize Open Share with New folder
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Network
SYSUSER-PC
VBOXSVR
Name Date modified Type Size
_R_E_A_D___T_H_I_S___7L7GW_ 4/20/2025 8:52 AM Text Document 2 KB
_R_E_A_D___T_H_I_S___BBHU4HO_ 4/20/2025 8:52 AM HTML Application 76 KB
N3S8pGDp0S.8856 4/20/2025 8:52 AM 8856 File 9,473 KB
N3S8pGDp0S.8856 Date modified: 4/20/2025 8:52 AM Date created: 7/14/2009 12:45 AM
8856 File Size: 9.25 MB

Regshot Analysis



Cerber opens multiple ports and protocols for potential C2 (command-and-control) communication.

It could allow incoming or outgoing communication, making it easier for ransomware to report infection, send encryption stats, or download additional payloads

Deletion of System Services

Detected deletion of services, particularly related to Volume Shadow Copy:

DeleteProcess (GUID referencing VSS)

Implication:
This reflects a common ransomware tactic aimed at disabling Windows backup mechanisms, thereby preventing victims from restoring encrypted files without paying the ransom.

Prefetch Files Created

New Prefetch entries were found:

C:\Windows\Prefetch\CERBER.EXE-99336462.pf

C:\Windows\Prefetch\MSTSH.EXE-C0599116.pf

These files confirm execution of the ransomware binary and related components, providing forensic artifacts of Cerber's activity on the system.

Modification of System Artifacts

Modifications were observed and alteration of recent program execution traces suggests Cerber may perform anti-forensic activities by manipulating system logs to obscure evidence of its execution.

Changes to Service Profile Folders

These folders are typically reserved for system service accounts. Cerber’s modification indicates that it likely placed ransom notes or encrypted files within these directories, targeting all possible user spaces for maximum impact.

Directory changes detected in:

C:\Windows\ServiceProfiles\LocalService\Desktop

C:\Windows\ServiceProfiles\NetworkService\Desktop

C:\Windows\ServiceProfiles\LocalService\Documents

C:\Windows\ServiceProfiles\NetworkService\Documents

Cerber ransomware shows a sophisticated multi-stage attack involving:

- Widen network access via firewall rule modification
- Destruction of backup and recovery points
- Strategic file system and registry tampering
- Leaving strong forensic artifacts (Prefetch files)
- Extensive file system encryption across service profiles

These behaviors align with known Cerber Tactics, Techniques, and Procedures (TTPs), exhibiting both persistence and evasion strategies typical of advanced ransomware families

Conclusion

Cerber Ransomware Capabilities and Impact

Through a combination of static and dynamic analysis techniques, this investigation successfully uncovered the behavior of the Cerber ransomware sample. Cerber employs sophisticated tactics to ensure effective encryption, persistence, evasion, and victim intimidation. It manipulates Windows firewall rules to maintain outbound communication channels, disables system recovery features such as Volume Shadow Copy, and extensively encrypt user and service profile data to maximize operational disruption.

The ransomware dynamically decrypts configuration data at runtime, including encryption parameters, targeted file types, Tor-based C2 communication details, and an embedded RSA public key for securing encryption keys. Observed runtime behaviors, such as the spawning of mshta.exe and the deployment of ransom notes, illustrate Cerber's focus on visibility and victim coercion while maintaining operational stealth.

Registry modifications, file system alterations, and the manipulation of critical Windows binaries further demonstrate Cerber's intent to obstruct forensic investigation and user remediation efforts. Notably, the presence of the SPSvc.exe string comparison suggests an attempt to self-identify or create a stealthy service, reinforcing the malware's emphasis on persistence and camouflage.

Cerber showcases a highly structured and professional malware architecture that blends evasion, disruption, and monetization techniques. The findings from this analysis provide valuable indicators of compromise (IOCs) and insights that can enhance detection, response, and recovery strategies against ransomware threats of similar complexity.