Static Analysis

1. Virus Total Analysis

Hash Analysis

- File Hash: [Insert MD5, SHA-1, SHA-256 hash value]
  - MD5: 5ef83811304bc53b79628202f9b8891b
  - SHA-1: 29b8a02a98404b1f80342badc952f8f9ba600edf
  - SHA-256: 547812259c4887610d6482eb78dd01717cf37b6f7d38cd2314f56927cd6fb6d1
- Method of hash acquisition: [Describe process]
  - Found on VirusTotal
- [Link to VirusTotal results]
  - https://www.virustotal.com/gui/file/547812259c4887610d6482eb78dd01717cf37b6f7d38cd2314f56927cd6fb6d1/summary

Vendor Analysis

- Number of vendors flagging as malicious: [X/Y]: 62/72
- Analysis of vendor results:
  - [Discuss patterns in detection]
    - Ransomware Trojan
    - Worm
  - [Common malware names identified]
    - WannaCryptor
    - Win32:WanaCry-A Trojan
    - WannaCry
    - Ransom.Zenshirsh.SL8
  - [Notable vendor disagreements]
    - Some say WannaCry, some say WannaCrypt
    - They all seem to point to a ransomware trojan

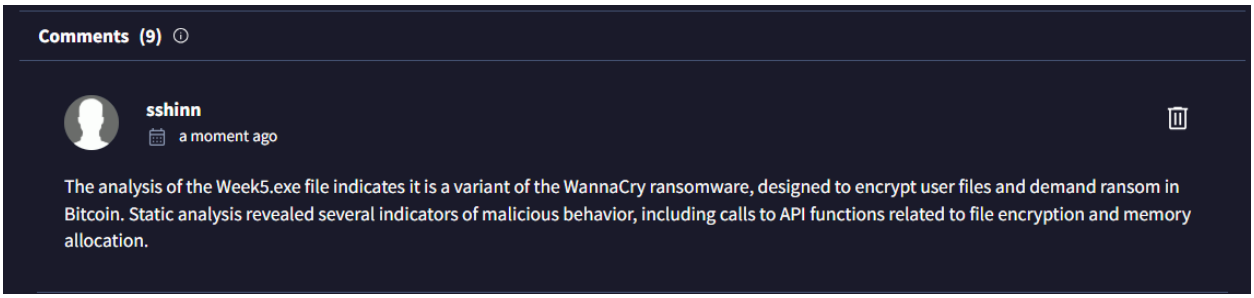
File History

- First Submission Date: [Date]
  - First Submission: 2025-02-19 17:05:51 UTC
- File Creation Date from Windows: [Date]
  - Creation Time: 2010-11-20 09:05:05 UTC
- Analysis of submission timeline:
  - [Discussion of file age]
    - It was not released or discovered for approximately 14 years since when it was created
  - [Notable resubmissions or changes]

        - It has been submitted and resubmitted a few times in the last few days, probably because of this class

Community Score

- [Link to your VirusTotal community contribution]
- https://www.virustotal.com/gui/file/547812259c4887610d6482eb78dd01717cf37b6f7d38cd2314f56927cd6fb6d1/community

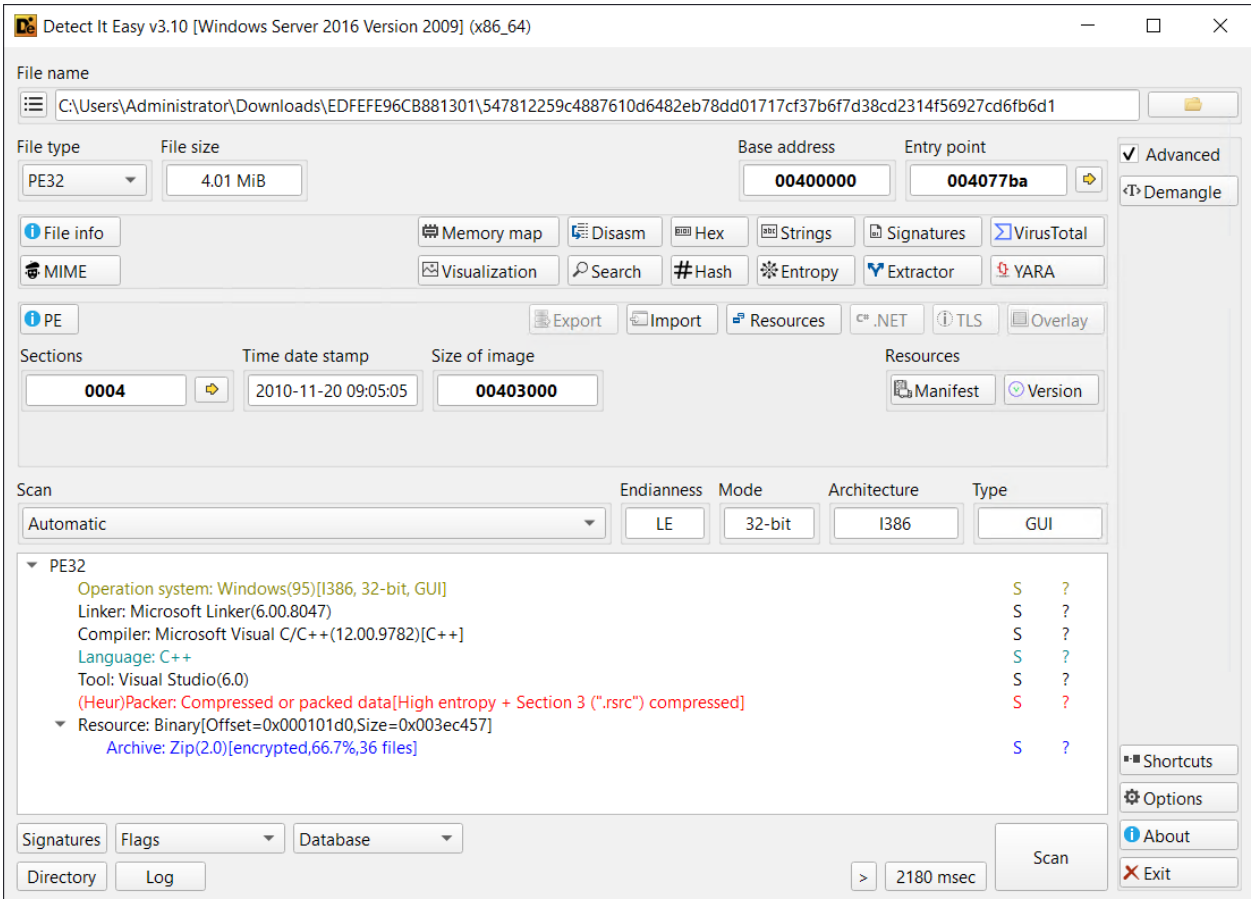


- Summary of initial findings posted to the community:
    - [Key observations] The analysis of the Week5.exe file indicates it is a variant of the WannaCry ransomware, designed to encrypt user files and demand ransom in Bitcoin. Static analysis revealed several indicators of malicious behavior, including calls to API functions related to file encryption and memory allocation.
    - [Potential indicators of compromise]: encrypted files, ransom note demanding bitcoin

2. Detect It Easy (DIE) Analysis

File Information

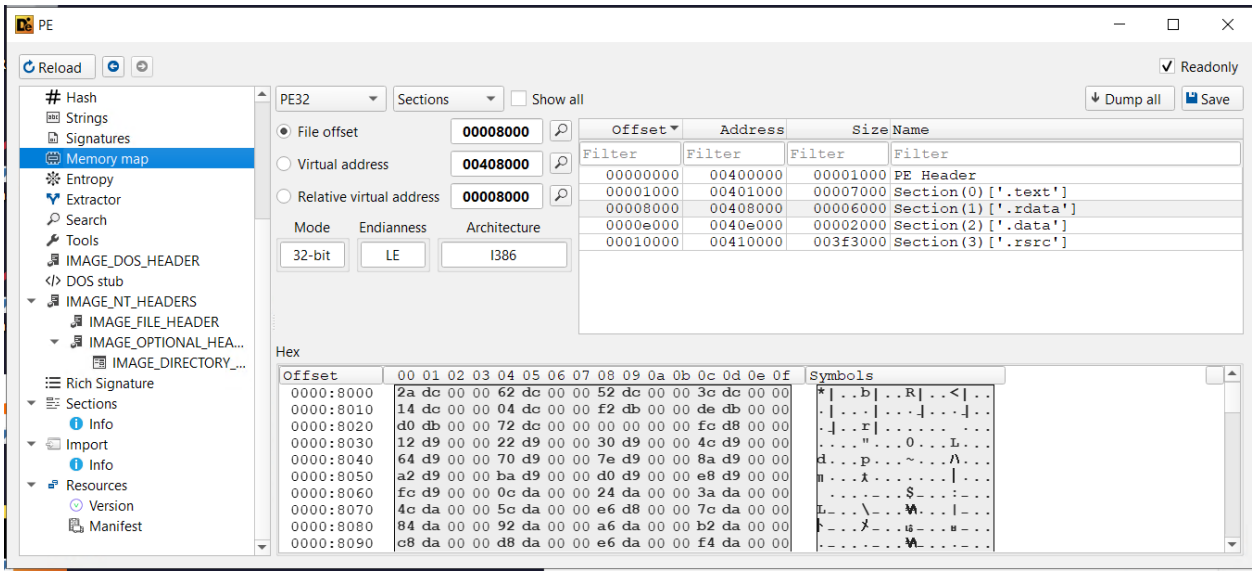
- File type: [Type] : PE32
- Architecture: [Architecture] : i386
- Compiler: [Compiler information] :
    - Compiler: Microsoft Visual C/C++(12.00.9782)[C++]
- Additional relevant information:
    - [List notable file characteristics]
        - Packed .rdata and .rsrc sections
    - [Unusual headers or structures]
        - 4 sections
        - Archive, zip
        - Encrypted
        - Windows 95
        - Language: C/C++



Memory Map Analysis

- Section breakdown:
  - [.text section analysis]
    - File offset: 00001000
    - Virtual address: 00401000
    - Size: 00007000
  - [.data section analysis]
    - File offset: 0000e000
    - Virtual address: 0040e000
    - Size: 00002000
    - WanaCrypt0r string found
  - [.rsrc section analysis]
    - File offset: 00010000
    - Virtual address: 00410000
    - Size: 003f3000
    - Found VirtualAlloc api call
  - [Other relevant sections]
    - .rdata
      - File offset: 00008000
      - Virtual address: 00408000

        - Size: 00006000
- Notable findings:
    - [Unusual section permissions]
        - .rdata had RW permissions
    - [Section size anomalies]
        - .rsrc was large (003f3000)

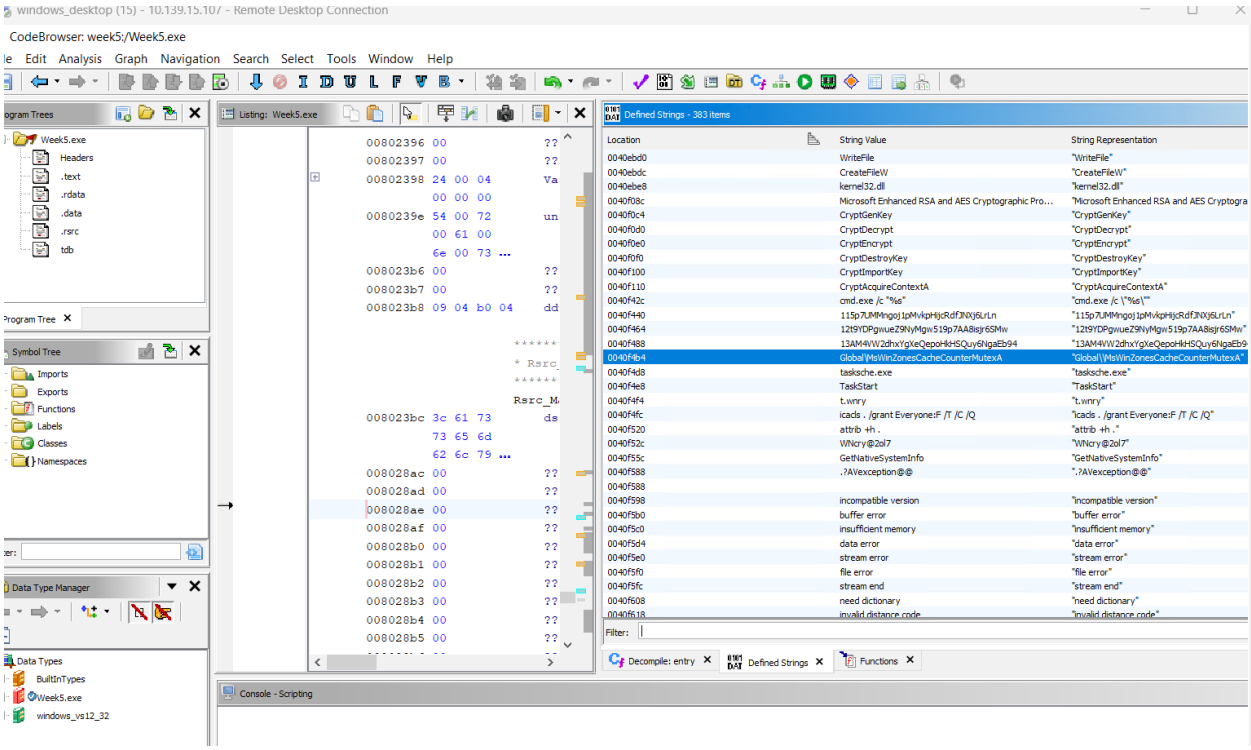


String Analysis

- Notable strings discovered:
- Sleep
- OpenMutexA
- GetFullPathNameA
- CopyFileA
- GetModuleFileNameA
- VirtualAlloc
- VirtualFree
- VirtualProtect
- WANACRY!
- CloseHandle
- DeleteFileW
- MoveFileExW
- MoveFileW
- ReadFile
- WriteFile
- CreateFileW
- kernel32.dll
- Microsoft Enhanced RSA and AES Cryptographic Provider
- CryptGenKey
- CryptDecrypt
- CryptEncrypt
- CryptDestroyKey
- CryptImportKey
- CryptAcquireContextA
- Global\MsWinZonesCacheCounterMutexA
- tasksche.exe
- TaskStart
- t.wnry
- 4043233_ANIME_AWAY_FACE_NO_NOBODY_ICON
- VS_VERSION_INFO
- StringFileInfo
- 040904B0

- CompanyName
- CYBV 454 Week 5 Malware Analysis
- FileDescription
- Week5 Malware Analysis
- FileVersion
- 1.1.4821.13121
- InternalName
- week5.exe
- LegalCopyright
- © 2025 Michael Galde. All rights reserved.
- OriginalFilename
- week5.exe
- ProductName
- University of Arizona ® Week5® Spring 2025 Malware Analysis
- ProductVersion
- 6.1.7601.17514

  - [URLs/IPs]
    - Urn:schemas-microsoft-com
  - File paths]
    - Software\
    - Global\MsWinZonesCacheCounterMutexA
  - [Command lines]
    - cmd.exe /c "%s"
  - [API calls]
    - VirtualAlloc
    - VirtualProtect
    - ReadFile
    - WriteFile
    - CreateFile
- Analysis of string findings:
  - [Potential functionality indicated]
    - Allocate space for payload
      - VirtualAlloc
      - VirtualProtect
    - Payload is encrypted:
      - Microsoft Enhanced RSA and AES Cryptographic Provider
      - CryptGenKey
      - CryptDecrypt
      - CryptEncrypt
      - CryptDestroyKey
      - CryptImportKey
      - CryptAcquireContextA
  - [Suspicious patterns]
    - WANACRY! - variant of WannaCry ransomware
    - Used for educational purposes
    - Encrypted

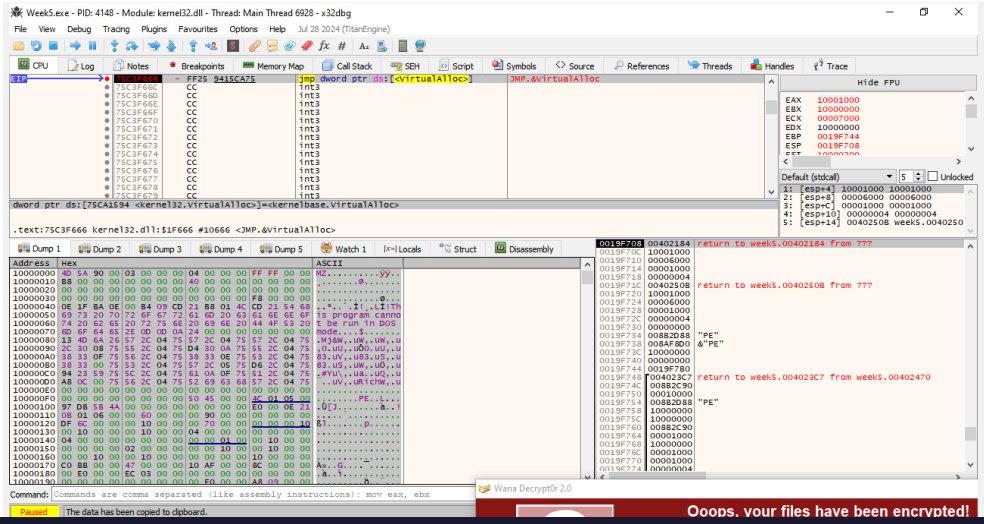


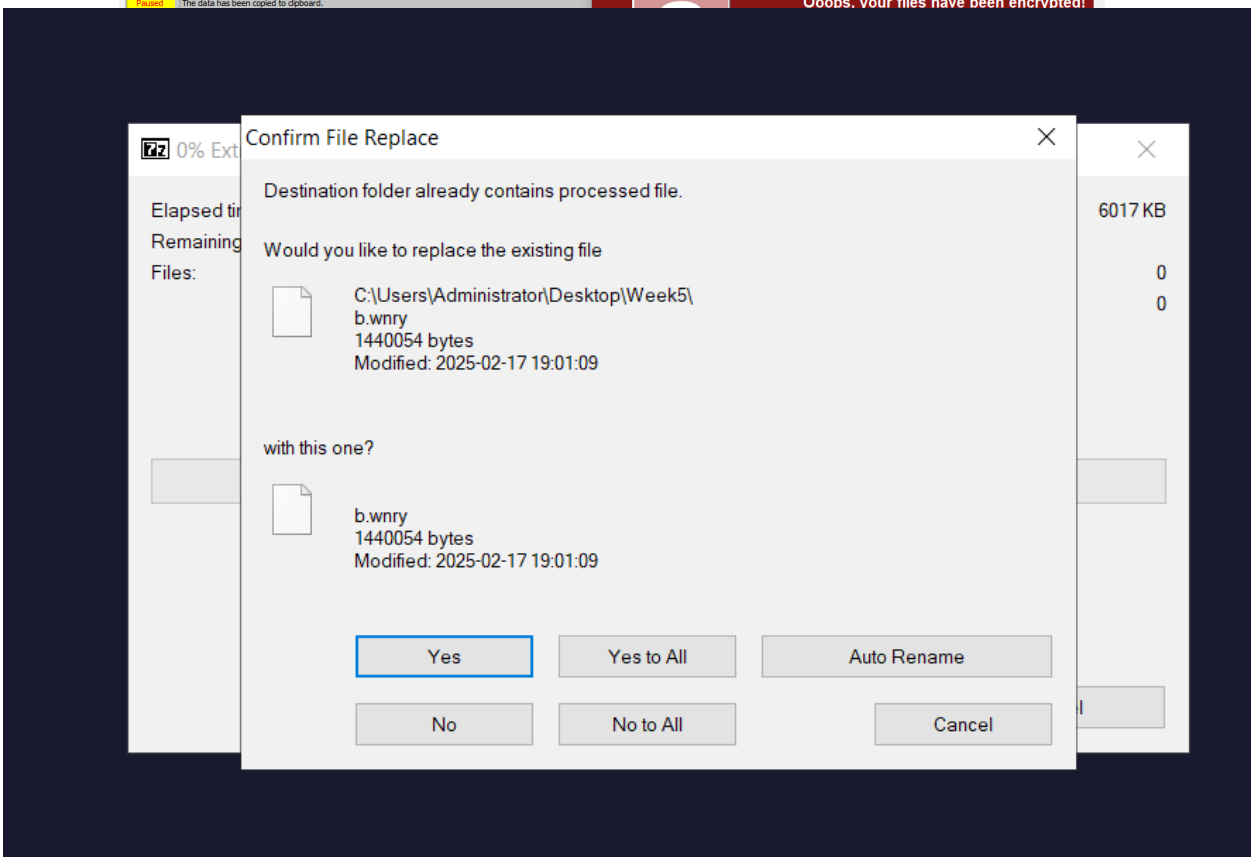
Entropy Analysis

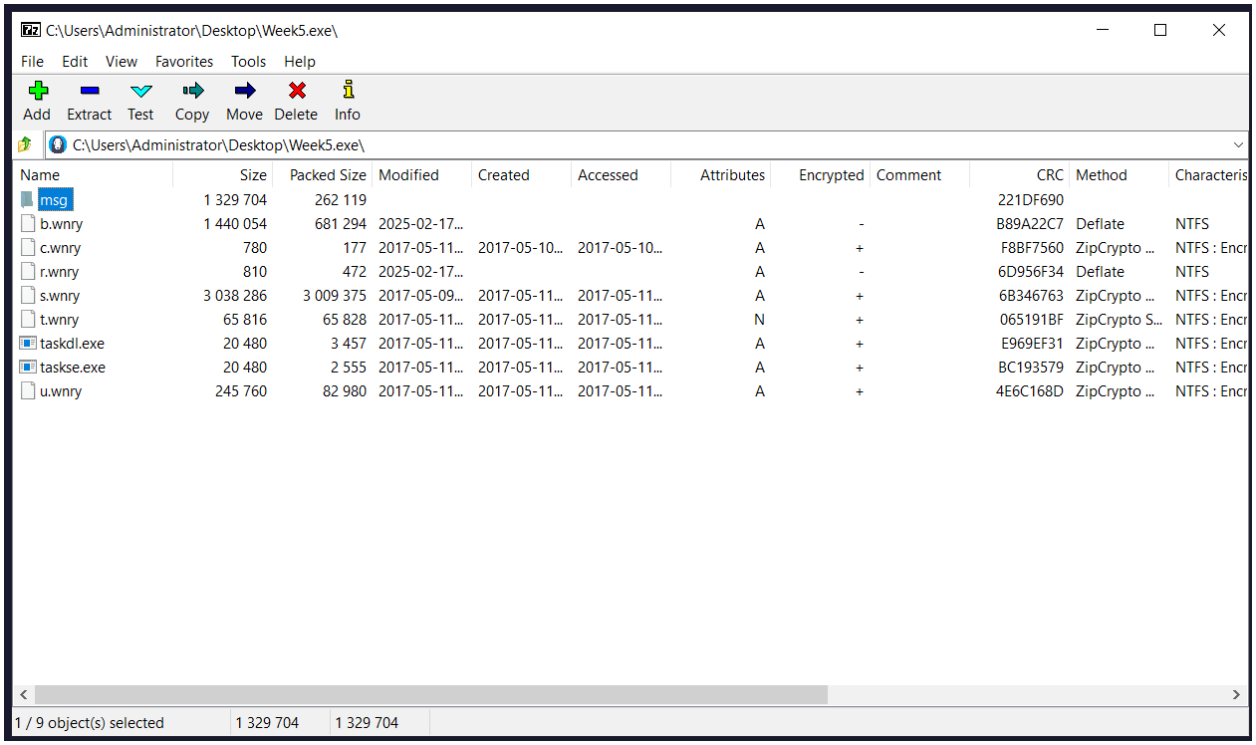
- Overall entropy score: [Score]: 7.99599
- Section-specific entropy:
  - [List sections with unusual entropy]
  - .text: 6.40429
  - .rdata: 6.66363
  - .rsrc: 7.99951
- Packing analysis:
  - [Packed/Unpacked determination]
    - .rdata and .rsrc are packed, .data and .text are not packed
  - [Packer identified (if applicable)]
    - I could not identify the packer
  - [Unpacking methodology (if attempted)]
    - I could not unpack the .rdata and .rsrc sections using conventional methods
  - [Alternative unpacking approaches (if needed)]
    - I tried to analyze the memory address pointed to by VirtualAlloc to find the payload using x32dbg
    - I was able to see contents of Week5.exe as a zipfile using 7zip

3. Static Analysis Summary

- Key findings from static analysis:
  - [Major indicators of malicious behavior]
    - Strings to encrypt files and possibly encrypt payload
    - VirtualAlloc and VirtualProtect
    - References to WannaCry, a famous ransomware
    - VirusTotal flagged as malicious
  - [Potential functionality]
    - To find the payload in the malware after identifying the VirtualAlloc function, I utilized x32dbg. Initially, I searched for VirtualAlloc by checking the Import Table for API calls, using the Memory Map to locate kernel32.dll. Once I identified the VirtualAlloc call, I set a breakpoint on its first instruction and ran the program until it hit the breakpoint.
    - Upon hitting the breakpoint, I inspected the arguments passed to VirtualAlloc by checking the stack. After stepping over the RET instruction, I used the Registers pane to examine the EAX register, which contained the allocated memory address. I copied the value of EAX and opened the Memory Map to find the corresponding memory region.
    - Seeing hex data written to the allocated address, I employed HxD to extract the payload. I utilized the "Binary Dump" feature to create a dump of the memory contents from the selected address, saving it as a new file for further analysis.
  - [Risk indicators]
    - I right-clicked the Week5.exe to “Open With” 7zip and I was able to see a preview of the unzipped contents of the file. It shows two executables, taskdl.exe and taskse.exe. These files run the malware. I also see b.wnry, c.wnry, r.wnry, s..wnry, t..wnry, and u..wnry, which is suspicious. I got a warning, which warned me that if I unzipped the file, it would change the names of the Week5.exe file, which allowed me to get a peek at the wannacry encrypting function. I chose no, do not unzip, I was afraid if I did it would run the malware.


Week5.exe - PID: 4148 - Module: kernel32.dll - Thread: Main Thread 6928 - x32dbg
File View Debug Tracing Plugins Favourites Options Help Jul 28 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct Disassembly
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused The data has been copied to clipboard.
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!


0% Ext
Elapsed ti
Remaining
Files:
6017 KB
0
0
Confirm File Replace
Destination folder already contains processed file.
Would you like to replace the existing file
C:\Users\Administrator\Desktop\Week5\
b.wnry
1440054 bytes
Modified: 2025-02-17 19:01:09
with this one?
b.wnry
1440054 bytes
Modified: 2025-02-17 19:01:09
Yes
Yes to All
Auto Rename
No
No to All
Cancel



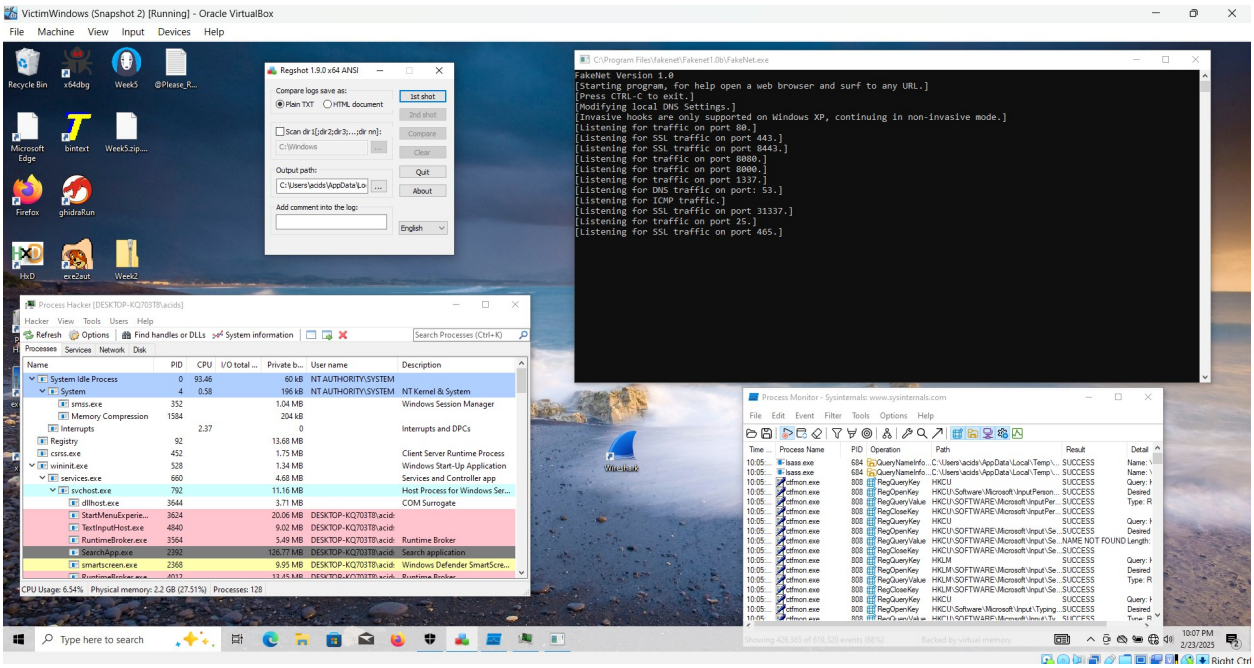
Name	Size	Packed Size	Modified	Created	Accessed	Attributes	Encrypted	Comment	CRC	Method	Characteris
msg	1 329 704	262 119							221DF690		
b.wnry	1 440 054	681 294	2025-02-17...			A	-		B89A22C7	Deflate	NTFS
c.wnry	780	177	2017-05-11...	2017-05-10...	2017-05-10...	A	+		F8BF7560	ZipCrypto ...	NTFS : Encr
r.wnry	810	472	2025-02-17...			A	-		6D956F34	Deflate	NTFS
s.wnry	3 038 286	3 009 375	2017-05-09...	2017-05-11...	2017-05-11...	A	+		6B346763	ZipCrypto ...	NTFS : Encr
t.wnry	65 816	65 828	2017-05-11...	2017-05-11...	2017-05-11...	N	+		065191BF	ZipCrypto S...	NTFS : Encr
taskdl.exe	20 480	3 457	2017-05-11...	2017-05-11...	2017-05-11...	A	+		E969EF31	ZipCrypto ...	NTFS : Encr
taskse.exe	20 480	2 555	2017-05-11...	2017-05-11...	2017-05-11...	A	+		BC193579	ZipCrypto ...	NTFS : Encr
u.wnry	245 760	82 980	2017-05-11...	2017-05-11...	2017-05-11...	A	+		4E6C168D	ZipCrypto ...	NTFS : Encr

Dynamic Analysis

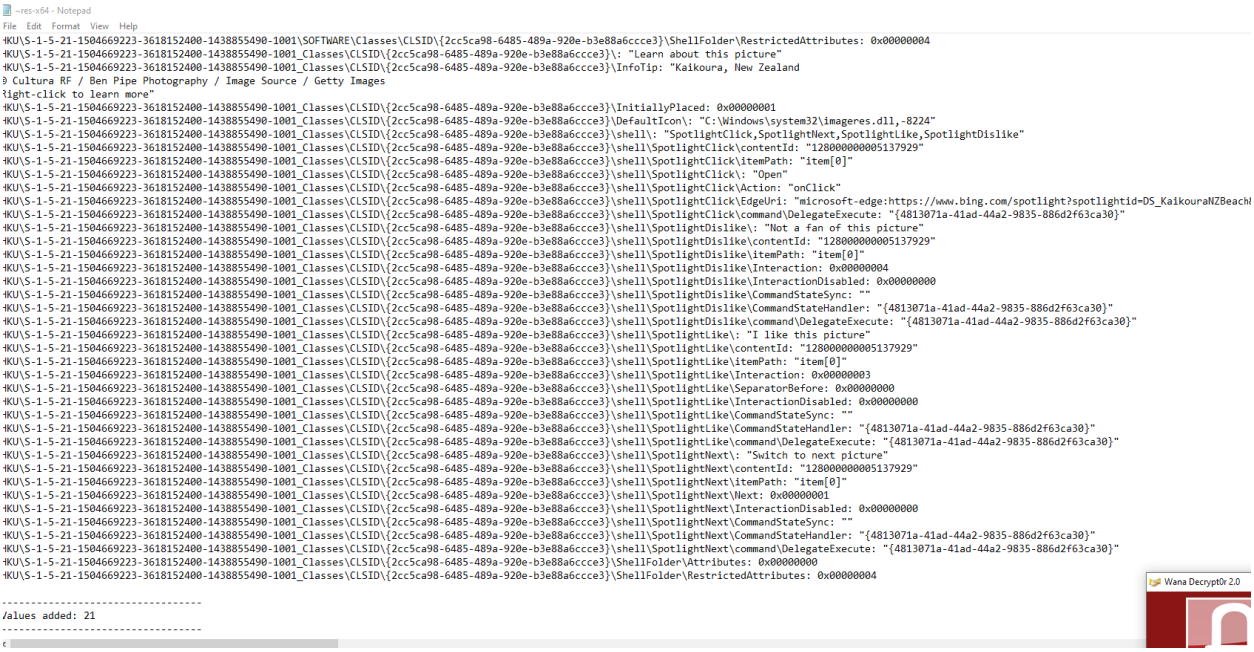
1. Analysis Environment

Environment Setup

- Virtual Machine specifications:
  - [OS version] Windows 10
  - [Memory allocation] 8GB
  - [Network configuration] Not Attached



- Monitoring tools deployed:
  - [Process monitoring] ProcMon, Process Hacker,,
  - [Network monitoring] FakeNet
  - RegShot
    - Keys:394379
    - Values:675302
    - Compare:
      - Keys deleted: 26
      - Values added: 21
      - Values modified: 61
      - Total changes: 216



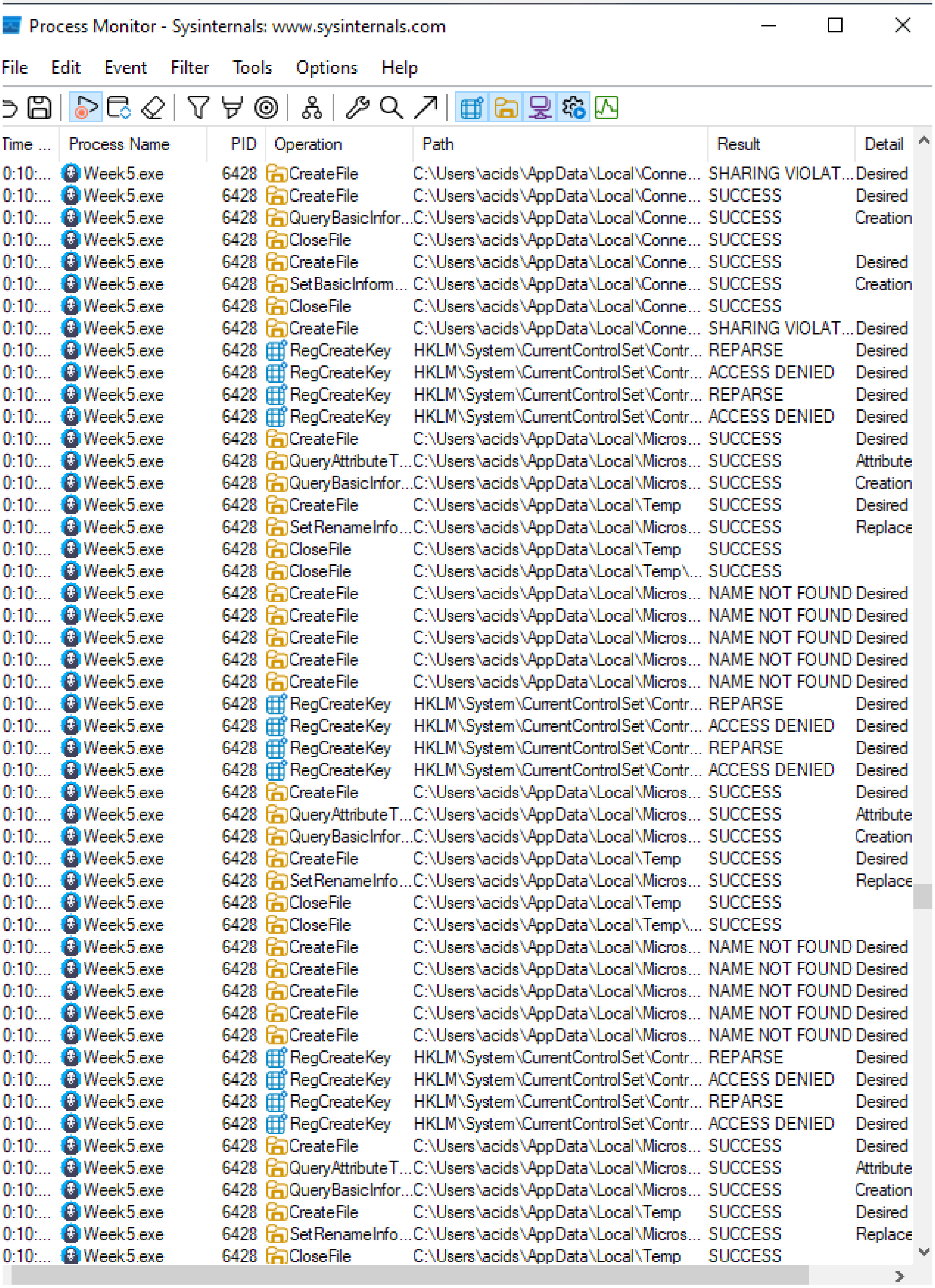
```
~res-x64 - Notepad
File  Edit  Format  View  Help
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001\SOFTWARE\Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\ShellFolder\RestrictedAttributes: 0x00000004
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\: "Learn about this picture"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\InfoTip: "Kaikoura, New Zealand
9 Cultura RF / Ben Pipe Photography / Image Source / Getty Images
Right-click to learn more"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\InitiallyPlaced: 0x00000001
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\DefaultIcon\: "C:\Windows\system32\imageres.dll,-8224"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\: "SpotlightClick,SpotlightNext,SpotlightLike,SpotlightDislike"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightClick\contentId: "1280000000005137929"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightClick\itemPath: "item[0]"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightClick\: "Open"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightClick\Action: "onClick"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightClick\EdgeUri: "microsoft-edge:https://www.bing.com/spotlight?spotlightid=DS_KaikouraNZBeachl
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightClick\command\DelegateExecute: "{4813071a-41ad-44a2-9835-886d2f63ca30}"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightDislike\: "Not a fan of this picture"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightDislike\contentId: "1280000000005137929"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightDislike\itemPath: "item[0]"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightDislike\Interaction: 0x00000004
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightDislike\InteractionDisabled: 0x00000000
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightDislike\CommandStateSync: ""
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightDislike\CommandStateHandler: "{4813071a-41ad-44a2-9835-886d2f63ca30}"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightDislike\command\DelegateExecute: "{4813071a-41ad-44a2-9835-886d2f63ca30}"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightLike\: "I like this picture"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightLike\contentId: "1280000000005137929"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightLike\itemPath: "item[0]"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightLike\Interaction: 0x00000003
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightLike\SeparatorBefore: 0x00000000
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightLike\InteractionDisabled: 0x00000000
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightLike\CommandStateSync: ""
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightLike\CommandStateHandler: "{4813071a-41ad-44a2-9835-886d2f63ca30}"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightLike\command\DelegateExecute: "{4813071a-41ad-44a2-9835-886d2f63ca30}"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightNext\: "Switch to next picture"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightNext\contentId: "1280000000005137929"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightNext\itemPath: "item[0]"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightNext\Next: 0x00000001
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightNext\InteractionDisabled: 0x00000000
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightNext\CommandStateSync: ""
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightNext\CommandStateHandler: "{4813071a-41ad-44a2-9835-886d2f63ca30}"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\shell\SpotlightNext\command\DelegateExecute: "{4813071a-41ad-44a2-9835-886d2f63ca30}"
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\ShellFolder\Attributes: 0x00000000
HKU\S-1-5-21-1504669223-3618152400-1438855490-1001_Classes\CLSID\{2cc5ca98-6485-489a-920e-b3e88a6ccce3}\ShellFolder\RestrictedAttributes: 0x00000004

----------------------------------
Values added: 21
----------------------------------
```


- Safety measures implemented:
  - [Network isolation] Not attached to network
  - [Snapshot configuration] snapshot saved with tools installed
  - [Additional protections] fakenet, and no internet

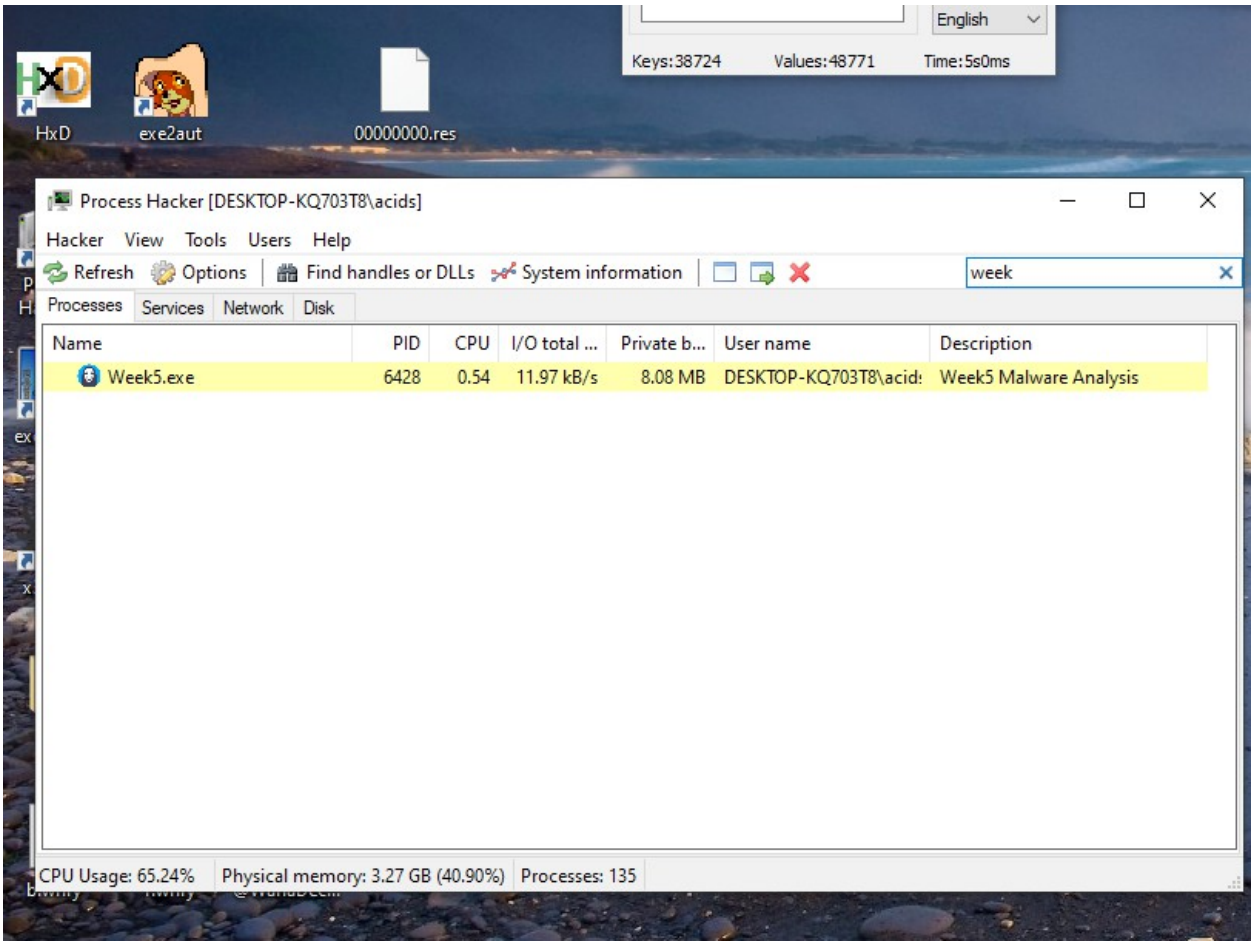
2. Runtime Observations

Initial Execution

- [Immediate system changes]:
  - Files encrypted on desktop
  - Files created on desktop
  - Files changed name
  - Pop up with WannaCry ransom notice to pay Bitcoin
- [Process creation]
  - Files created
  - Files renamed
  - Files closed



Time ...	Process Name	PID	Operation	Path	Result	Detail
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Conne...	SHARING VIOLAT...	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Conne...	SUCCESS	Desired
0:10:...	Week5.exe	6428	QueryBasicInfor...	C:\Users\acids\AppData\Local\Conne...	SUCCESS	Creation
0:10:...	Week5.exe	6428	CloseFile	C:\Users\acids\AppData\Local\Conne...	SUCCESS	
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Conne...	SUCCESS	Desired
0:10:...	Week5.exe	6428	SetBasicInform...	C:\Users\acids\AppData\Local\Conne...	SUCCESS	Creation
0:10:...	Week5.exe	6428	CloseFile	C:\Users\acids\AppData\Local\Conne...	SUCCESS	
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Conne...	SHARING VIOLAT...	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	ACCESS DENIED	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	ACCESS DENIED	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Desired
0:10:...	Week5.exe	6428	QueryAttributeT...	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Attribute
0:10:...	Week5.exe	6428	QueryBasicInfor...	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Creation
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Temp	SUCCESS	Desired
0:10:...	Week5.exe	6428	SetRenameInfo...	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Replace
0:10:...	Week5.exe	6428	CloseFile	C:\Users\acids\AppData\Local\Temp	SUCCESS	
0:10:...	Week5.exe	6428	CloseFile	C:\Users\acids\AppData\Local\Temp\...	SUCCESS	
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	NAME NOT FOUND	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	NAME NOT FOUND	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	NAME NOT FOUND	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	NAME NOT FOUND	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	NAME NOT FOUND	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	ACCESS DENIED	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	ACCESS DENIED	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Desired
0:10:...	Week5.exe	6428	QueryAttributeT...	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Attribute
0:10:...	Week5.exe	6428	QueryBasicInfor...	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Creation
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Temp	SUCCESS	Desired
0:10:...	Week5.exe	6428	SetRenameInfo...	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Replace
0:10:...	Week5.exe	6428	CloseFile	C:\Users\acids\AppData\Local\Temp	SUCCESS	
0:10:...	Week5.exe	6428	CloseFile	C:\Users\acids\AppData\Local\Temp\...	SUCCESS	
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	NAME NOT FOUND	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	NAME NOT FOUND	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	NAME NOT FOUND	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	NAME NOT FOUND	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	NAME NOT FOUND	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	ACCESS DENIED	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired
0:10:...	Week5.exe	6428	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	ACCESS DENIED	Desired
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Desired
0:10:...	Week5.exe	6428	QueryAttributeT...	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Attribute
0:10:...	Week5.exe	6428	QueryBasicInfor...	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Creation
0:10:...	Week5.exe	6428	CreateFile	C:\Users\acids\AppData\Local\Temp	SUCCESS	Desired
0:10:...	Week5.exe	6428	SetRenameInfo...	C:\Users\acids\AppData\Local\Micros...	SUCCESS	Replace
0:10:...	Week5.exe	6428	CloseFile	C:\Users\acids\AppData\Local\Temp	SUCCESS	



- [Network activity]
  - Connections to various foreign IP addresses (ANY.RUN)
- [File system changes]
  - From ProcMon: files created, renamed, opened and closed

Continued Monitoring

- [Persistent changes]
  - Encrypted files
- [Scheduled tasks]
  - Ransomware pop up only came up after running Week5.exe twice
- [Registry modifications]
  - Keys:394379
  - Values:675302
  - Compare:
    - Keys deleted: 26
    - Values added: 21
    - Values modified: 61
    - Total changes: 216

- [Additional payloads]
    - None found

3. Post-Execution Analysis

- System state changes:
    - [Permanent modifications]
        - Files renamed, created and encrypted
    - [Persistence mechanisms]
        - none
    - [Data exfiltration evidence]
        - none
- Network activity summary:
    - [Connection attempts]
    - ANY.RUN
        - Connection attempts to many foreign IP addresses
    - [Data transfers]
        - none
    - [Command & Control activity]
        - none

Impact Analysis

1. User Impact Assessment

Home Users

- [Potential impact] Very high impact, will encrypt all files
- [Risk level] Very high risk
- [Data compromise potential], All files will be encrypted leading to loss of availability

Business Users

- [Operational impact] Will bring all operations to a halt because affected systems will be inoperable
- [Data security concerns]: Data could be exfiltrated, loss of availability of data
- [Financial implications]: Loss of time, possibly loss of $300 per affected machine if ransom is paid, however even if ransom is paid there is no guarantee that files will be decrypted

Government Users

- [Security implications] Loss of control over files

- [Data sensitivity concerns] Sensitive data could be lost or damaged beyond repair
- [Operational disruption potential]: would cause loss of time, data, and resources

2. Mitigation Strategy

Immediate Response

- [Initial containment steps] Try to use decryptor if possible to regain access to files, inform all users about the infection to prevent further spreading.
- [System isolation procedures] Immediately disconnect from network
- [Data preservation methods]: Try to use decryptor. Backup encrypted files to a separate storage medium, if possible, to preserve them for potential future decryption attempts. Utilize any available backups to restore previous versions of affected files.

Long-term Prevention

- [Security control recommendations] Do not download suspicious programs, they could be trojans. Regularly update antivirus definitions and conduct security scans.
- [Policy modifications] Develop and enforce a strict software installation policy to ensure that only verified applications are installed. Conduct regular audits of installed software.
- [Training requirements]: Training to avoid suspicious links.

Conclusion

1. Analysis Reflection

- [Summary of findings]: The analysis of the Week5.exe file indicates it is a variant of the WannaCry ransomware, designed to encrypt user files and demand ransom in Bitcoin. Static analysis revealed several indicators of malicious behavior, including calls to API functions related to file encryption and memory allocation.
- [Unusual characteristics]: The file exhibited packed sections, unusual entropy scores, and suspicious strings indicating potential payload functionality. The dynamic analysis confirmed the execution of the malware resulted in immediate file encryption and ransom notifications.
- [Learning outcomes]: The analysis demonstrated the importance of both static and dynamic analysis in understanding malware behavior. Additionally, it reinforced the necessity of security measures and the rapid response required when dealing with ransomware threats.
- [Additional research needed]

2. Evidence Documentation

- [Screenshot descriptions and relevance]
- [Tool output documentation]: ProcMon, ProcessHacker, RegShot, Any.Run, Ghidra, Detect-It-Easy, x32dbg, HxD
- [Additional supporting materials]