WannaCry Encryptor Report

A report on the Encryptor executable within the WannaCry ransomware malware

Paul Michael Oates

2001642

CMP320: Advanced Ethical Hacking

2022/2023

Note that Information contained in this document is for educational purposes.

.

Abstract

Malicious software or malware is code that is designed to cause harm to computers without the consent of the owner. WannaCry ransomware consists of two components the Worm, that allows it to spread across a network and the Encryptor, the component that encrypts the files and demands the ransom. In today's world ransomware is highly profitable for threat actors and a frustration for businesses. The Sample One executable is the encryptor component of the WannaCry ransomware.

This report aims to install the provided Sample One on a virtual machine and execute it, and then analyse the malwares type and characteristics using both static and dynamic analysis. An evaluation of the components and functionality will identify the processes undertaken by the malware to cause harm to the end user. This analysis will also establish Sample One's Indicators of Compromise (IOC). The methodology was applied through tools such as VMware, Wireshark, IDA and Cutter to ensure a robust analysis was undertaken. This yielded the file types the ransomware does not encrypt, the encryption keys and how they are obscured, how the malware deletes the shadow files in order to maximise the damage as well as the Indicators of Compromise on an infected machine.

This ransomware proved highly effective against a wide range of Microsoft Windows Operating Systems. Sample One makes use of standard Windows functions from a 32 bit executable in order to maximise the damage it does across a variety of Windows Operating Systems. This report could be used to better understand how WannaCry encrypts an Operating System and helps the end user protect their Operating Systems by implementing the mitigations suggested.

.

Contents

.

1 INTRODUCTION

1.1 BACKGROUND

Malicious software or malware is code that is designed to cause harm to computers without the consent of the owner. Malware has been around since the first computer virus in 1974. Today malware is divided into categories by its characteristics and the method in which it can affect a device. Categories include (Crowdstrike.com, 2023):

- Virus – A virus is a piece of code that inserts itself into an application and executes when the app is run
- Worm - Spreads through a network by replicating itself
- Trojan - Disguises itself as desirable code
- Spyware - Collects user activity data without their knowledge
- Ransomware - software that encrypts files and folders and demands a payment typically in a Cryptocurrency such as Bitcoin to decrypt the files

One example of ransomware is WannaCry. This makes use of the Eternal Blue exploit to propagate itself across the network and encrypt files that it finds on the infected devices, demanding a ransom to release the encrypted files. (Hypr.com, nd)

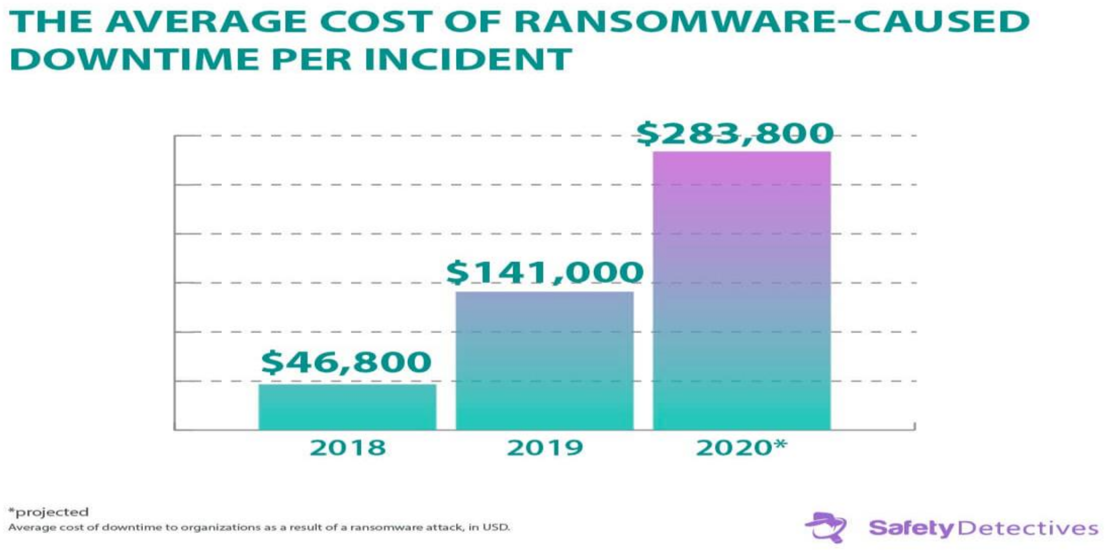


Figure 1-1 (Safetydetectives.com,nd)

Figure 1-1 shows the cost of the downtime to a business regarding a ransomware attack. This does not include the cost to the business to decrypt the files. “Ransomware is highly profitable business for criminals and nation states, for example the damage WannaCry did to the National Health Service in the UK was around $100 million and worldwide came to $4 billion USD." (Ditto.com, 2018)

In conclusion, malware's including ransomware can be damaging to businesses and industries and highly profitable for criminals.

1.2 AIM

The aim of the report is to:

- Install the provided Sample One malware on a virtual machine and execute
- Analyse the provided Sample One malware to identify the type and characteristics using both static and dynamic analysis
- Evaluate the malware components and functionality identifying the processes undertaken by the malware to cause harm to the end user
- Establish Sample One malware's Indicators of Compromise (IOC)
- Report on findings, including mitigation and prevention methods

1.3 METHODOLOGY

The Malware sample used will be Sample One. This was installed into A Microsoft Windows 10 Flare VMware Virtual Machine (VM). This supplies a secure sandboxed environment to analyse the malware allowing for both dynamic and static analysis to take place. The methodology undertaken to analyse the malware sample will be broken into two separate sections allowing for a thorough analysis of the malware sample given. The sections will be:

- Static Analysis
    - Online Research
    - Basic Information
    - String Analysis
    - Imports Analysis
- Dynamic Analysis
    - Executable Process
    - Network Traffic Analysis
    - Registry Analysis
    - Memory Analysis

Dynamic analysis has been completed using tools including:

- Process monitor
- Volatility
- Reg Shot
- Wireshark

Static analysis has been completed using tools including:

- Cutter
- Hash it Easy
- Virus Total
- 010 Editor
- CFF Explorer VIII
- Pestudio

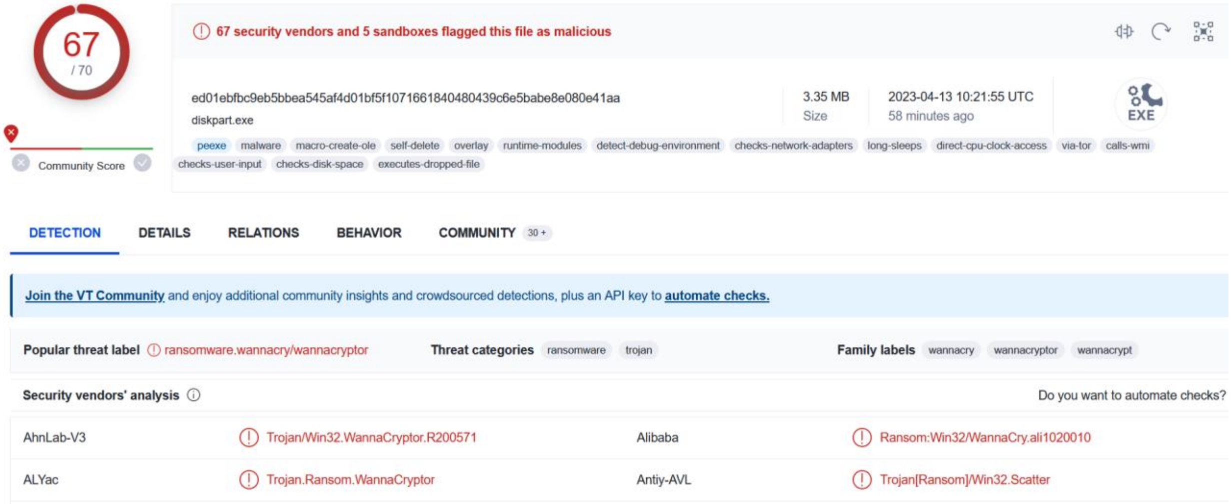
A full list of the tools used and where to download them can be found in references - Tools for Malware Analysis.

1.4 STATIC ANALYSIS

Initially the malware Sample One was unzipped and moved to the desktop folder allowing the sample to be analysed and executed.

1.4.1 Online Research

The file was initially hashed using MD5 and the signature was searched for in Virus Total.



67 security vendors and 5 sandboxes flagged this file as malicious

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
diskpart.exe

3.35 MB
Size

2023-04-13 10:21:55 UTC
58 minutes ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label ransomware.wannacry/wannacryptor Threat categories ransomware trojan Family labels wannacry wannacryptor wannacrypt

Security vendors' analysis Do you want to automate checks?

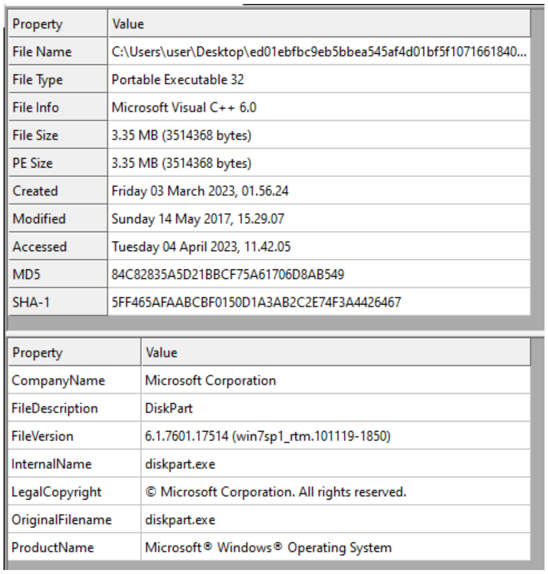
AhnLab-V3	Trojan/Win32.WannaCryptor.R200571	Alibaba	Ransom:Win32/WannaCry.ali1020010
ALYac	Trojan.Ransom.WannaCryptor	Antiy-AVL	Trojan[Ransom]/Win32.Scatter

Figure 1 Virus Total Scan

Figure 1 shows the Virus Total scan result identifying Sample One as malicious. Using vendor analysis Sample One was identified as the WannaCryptor ransomware.

1.4.2 Basic Information

CFF Explorer VIII was used to identify basic Information about Sample One.

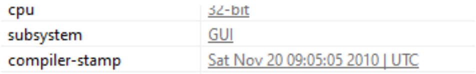


Property	Value
File Name	C:\Users\user\Desktop\ed01ebfbc9eb5bbea545af4d01bf5f1071661840...
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	3.35 MB (3514368 bytes)
PE Size	3.35 MB (3514368 bytes)
Created	Friday 03 March 2023, 01.56.24
Modified	Sunday 14 May 2017, 15.29.07
Accessed	Tuesday 04 April 2023, 11.42.05
MD5	84C82835A5D21BBCF75A61706D8AB549
SHA-1	5FF465AFAABCBF0150D1A3AB2C2E74F3A4426467

Property	Value
CompanyName	Microsoft Corporation
FileDescription	DiskPart
FileVersion	6.1.7601.17514 (win7sp1_rtm.101119-1850)
InternalName	diskpart.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	diskpart.exe
ProductName	Microsoft® Windows® Operating System

Figure 2 CFF Explorer

Figure 2 shows Sample One's basic information. Sample One had a description of "DiskPart" and an original name of "diskpart.exe" it is also a 32bit executable. As the file size and the PE size match, this indicates that the file is not likely packed.



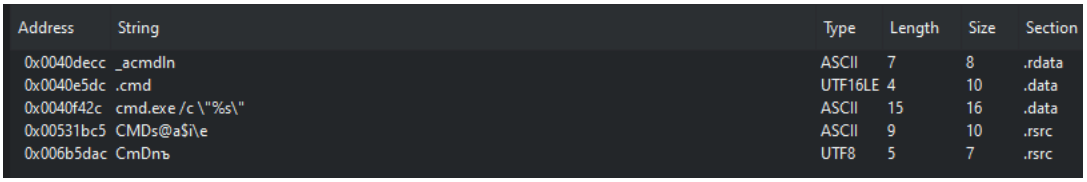
cpu	32-bit
subsystem	GUI
compiler-stamp	Sat Nov 20 09:05:05 2010 | UTC

Figure 3 PE-Studio

Figure 3 Identified the compile time of Sample One as Saturday November 20th, 2010, at 9:05am.

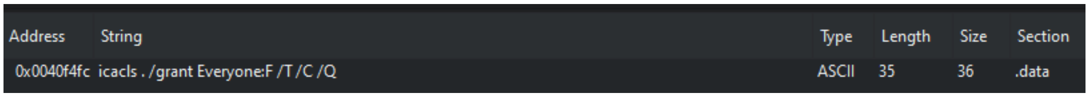
1.4.3 String Analysis

Next using a tool called Cutter, Sample One was searched for strings of interest:



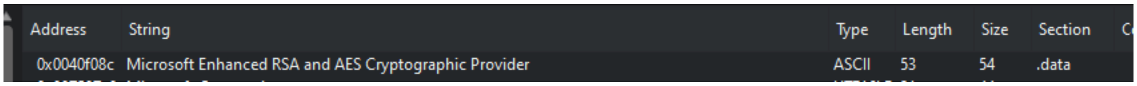
Address	String	Type	Length	Size	Section
0x0040decc	_acmdln	ASCII	7	8	.rdata
0x0040e5dc	.cmd	UTF16LE	4	10	.data
0x0040f42c	cmd.exe /c \"%s\"	ASCII	15	16	.data
0x00531bc5	CMDs@a$i\e	ASCII	9	10	.rsrc
0x006b5dac	CmDnъ	UTF8	5	7	.rsrc

Figure 4 "cmd" string search



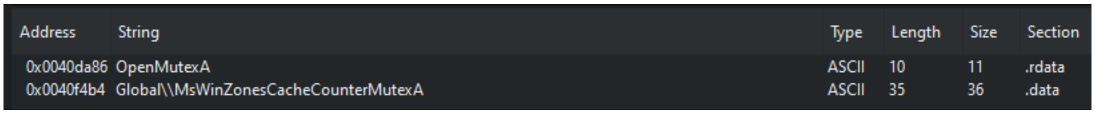
Address	String	Type	Length	Size	Section
0x0040f4fc	icacls . /grant Everyone:F /T /C /Q	ASCII	35	36	.data

Figure 5 "icals" search



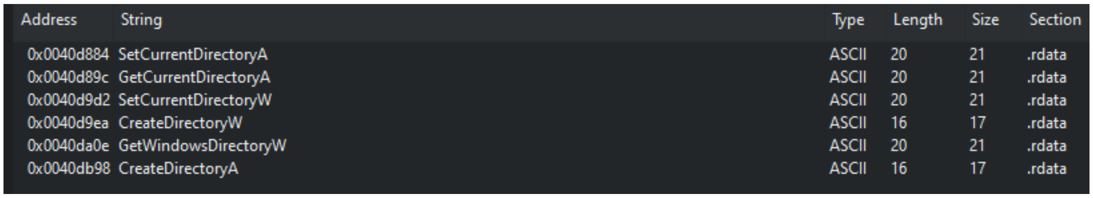
Address	String	Type	Length	Size	Section
0x0040f08c	Microsoft Enhanced RSA and AES Cryptographic Provider	ASCII	53	54	.data

Figure 6 RSA search



Address	String	Type	Length	Size	Section
0x0040da86	OpenMutexA	ASCII	10	11	.rdata
0x0040f4b4	Global\\MsWinZonesCacheCounterMutexA	ASCII	35	36	.data

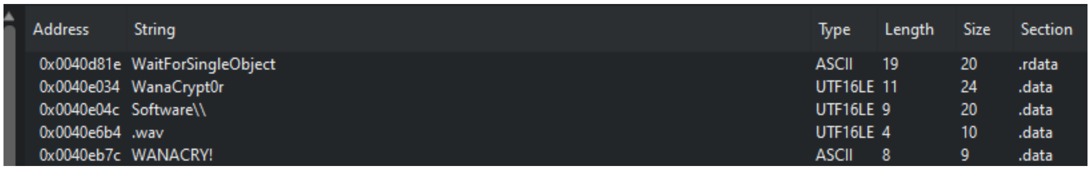
Figure 7 Mutex search



Address	String	Type	Length	Size	Section
0x0040d884	SetCurrentDirectoryA	ASCII	20	21	.rdata
0x0040d89c	GetCurrentDirectoryA	ASCII	20	21	.rdata
0x0040d9d2	SetCurrentDirectoryW	ASCII	20	21	.rdata
0x0040d9ea	CreateDirectoryW	ASCII	16	17	.rdata
0x0040da0e	GetWindowsDirectoryW	ASCII	20	21	.rdata
0x0040db98	CreateDirectoryA	ASCII	16	17	.rdata

Figure 8 Directory Search

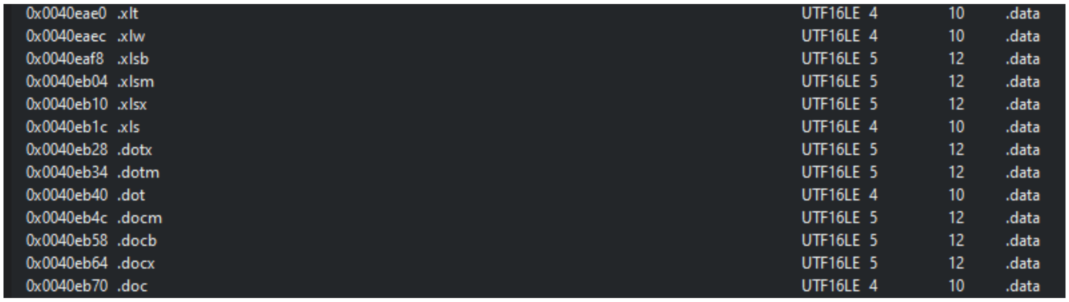
Figure 4 - 8 shows Sample One contains possibly malicious functions and services, including a directory search, mutexes, RSA and AES Utility, command prompt and “icacls” a tool for modifying file permissions.



Address	String	Type	Length	Size	Section
0x0040d81e	WaitForSingleObject	ASCII	19	20	.rdata
0x0040e034	WanaCrypt0r	UTF16LE	11	24	.data
0x0040e04c	Software\\	UTF16LE	9	20	.data
0x0040e6b4	.wav	UTF16LE	4	10	.data
0x0040eb7c	WANACRY!	ASCII	8	9	.data

Figure 9 “Wan” search

Figure 9 shows Sample One contains the phrase “WANACRY!” and “WanaCrypt0r” this identifies that Sample One is likely a part of the WannaCry ransomware.



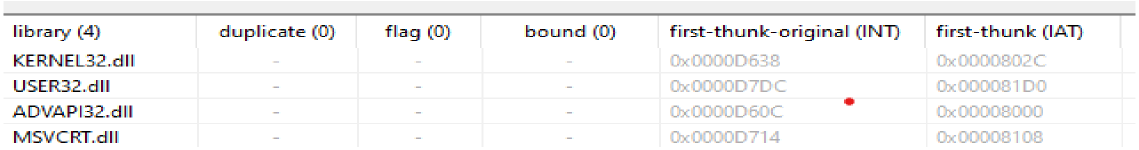
0x0040eae0	.xlt	UTF16LE	4	10	.data
0x0040eaec	.xlw	UTF16LE	4	10	.data
0x0040eaf8	.xlsb	UTF16LE	5	12	.data
0x0040eb04	.xlsm	UTF16LE	5	12	.data
0x0040eb10	.xlsx	UTF16LE	5	12	.data
0x0040eb1c	.xls	UTF16LE	4	10	.data
0x0040eb28	.dotx	UTF16LE	5	12	.data
0x0040eb34	.dotm	UTF16LE	5	12	.data
0x0040eb40	.dot	UTF16LE	4	10	.data
0x0040eb4c	.docm	UTF16LE	5	12	.data
0x0040eb58	.docb	UTF16LE	5	12	.data
0x0040eb64	.docx	UTF16LE	5	12	.data
0x0040eb70	.doc	UTF16LE	4	10	.data

Figure 10 "." string search

Figure 10 shows Sample One includes a list of some of the file type extensions, a full list of can be found in Appendix A “.” String Search.

1.4.4 Imports Analysis

Next “VirusTotal” and “pestudio” were used to identify the imports used by Sample One.



library (4)	duplicate (0)	flag (0)	bound (0)	first-thunk-original (INT)	first-thunk (IAT)
KERNEL32.dll	-	-	-	0x0000D638	0x0000802C
USER32.dll	-	-	-	0x0000D7DC	0x000081D0
ADVAPI32.dll	-	-	-	0x0000D60C	0x00008000
MSVCRT.dll	-	-	-	0x0000D714	0x00008108

Figure 11 “pestudio” Libraries

Figure 11 shows Sample One makes use of four libraries. By using “VirusTotal” and “pestudio” the following imports from the libraries were discovered: (Microsoft.com, nd)

KERNEL32.dll:

- VirtualAlloc – A function that allows a program to allocate a block of memory.
- VirtualProtect – A function which is used to change the access permissions of memory pages.
- GetFileAttributesW – A function which allows a program to retrieve information about a Directory or File
- GetFileSizeEx – A function that allows a program to retrieve the file size. Ex is for files larger than 64GB.
- GetFileSize - A function that allows a program to retrieve the file size up to 4GB.
- SetFileAttributesW – A function that allows a program to modify the attributes of a file or directory, such as its read-only, hidden, archive, or system status.

USER32.dll

- wsprintfA - A function in the that allows a program to format a string of text and store the result in a buffer.

ADVAPI32.dll

- CryptReleaseContext - A function that allows a program to release a cryptographic service provider.
- RegCreateKeyW - A function that allows a program to create a new registry key or open an existing one for modification or querying.
- RegSetValueExA - A function in the Windows API that allows a program to set the value of a registry key.
- RegQueryValueExA - A function in the Windows API that allows a program to retrieve the value of a registry key.
- RegCloseKey - A function in the Windows API that allows a program to close a previously opened registry key.
- OpenSCManagerA - A function in the Windows API that allows a program to open a handle to the service control manager.

MSVCRT.dll

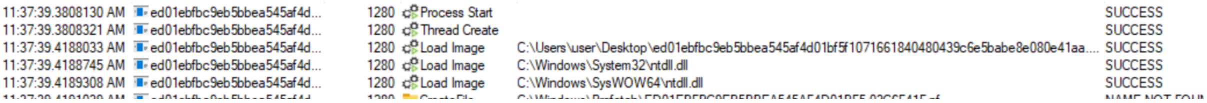
- rand/srand- Functions used for generating random numbers.
- fopen/fread/fwrite/fclose – Functions for opening , reading, writing, and closing files.
- sprintf/swprintf – functions used for sting formatting.
- exit/ExitProcess – Functions used for ending program and returning to the OS.
- _stricmp – Function for comparing strings without caring for case sensitivity.

1.5 DYNAMIC ANALYSIS

In order to gain a complete understanding of Sample One it was executed in a VMware Virtual Machine in order to understand its processes and behaviours.

1.5.1 Executable Process

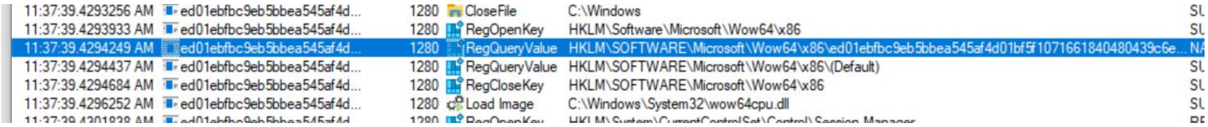
Process Monitor was used to log Sample One’s interactions with the system



```
11:37:39.3808130 AM  ed01ebfbc9eb5bbea545af4d...   1280  Process Start                                                                                              SUCCESS
11:37:39.3808321 AM  ed01ebfbc9eb5bbea545af4d...   1280  Thread Create                                                                                              SUCCESS
11:37:39.4188033 AM  ed01ebfbc9eb5bbea545af4d...   1280  Load Image     C:\Users\user\Desktop\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa....  SUCCESS
11:37:39.4188745 AM  ed01ebfbc9eb5bbea545af4d...   1280  Load Image     C:\Windows\System32\ntdll.dll                                                               SUCCESS
11:37:39.4189308 AM  ed01ebfbc9eb5bbea545af4d...   1280  Load Image     C:\Windows\SysWOW64\ntdll.dll                                                               SUCCESS
```

Figure 12 Process Monitor

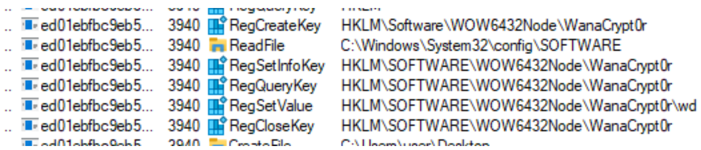
Figure 12 shows Sample One is initially ran calling the 32-bit emulator.



```
11:37:39.4293256 AM  ed01ebfbc9eb5bbea545af4d...   1280  CloseFile      C:\Windows                                                                          SU
11:37:39.4293933 AM  ed01ebfbc9eb5bbea545af4d...   1280  RegOpenKey     HKLM\Software\Microsoft\Wow64\x86                                                   SU
11:37:39.4294249 AM  ed01ebfbc9eb5bbea545af4d...   1280  RegQueryValue  HKLM\SOFTWARE\Microsoft\Wow64\x86\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e...  NA
11:37:39.4294437 AM  ed01ebfbc9eb5bbea545af4d...   1280  RegQueryValue  HKLM\SOFTWARE\Microsoft\Wow64\x86\(Default)                                         SU
11:37:39.4294684 AM  ed01ebfbc9eb5bbea545af4d...   1280  RegCloseKey    HKLM\SOFTWARE\Microsoft\Wow64\x86                                                   SU
11:37:39.4296252 AM  ed01ebfbc9eb5bbea545af4d...   1280  Load Image     C:\Windows\System32\wow64cpu.dll                                                    SU
```

Figure 13 Process Monitor

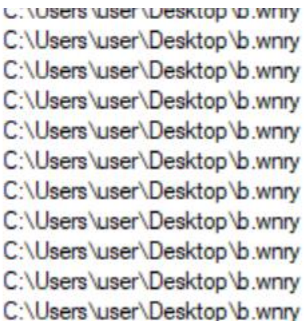
Figure 13 shows Sample One fails to fetch a Registry Key in the 32bit emulator.



```
..  ed01ebfbc9eb5...  3940  RegCreateKey   HKLM\Software\WOW6432Node\WanaCrypt0r
..  ed01ebfbc9eb5...  3940  ReadFile       C:\Windows\System32\config\SOFTWARE
..  ed01ebfbc9eb5...  3940  RegSetInfoKey  HKLM\SOFTWARE\WOW6432Node\WanaCrypt0r
..  ed01ebfbc9eb5...  3940  RegQueryKey    HKLM\SOFTWARE\WOW6432Node\WanaCrypt0r
..  ed01ebfbc9eb5...  3940  RegSetValue    HKLM\SOFTWARE\WOW6432Node\WanaCrypt0r\wd
..  ed01ebfbc9eb5...  3940  RegCloseKey    HKLM\SOFTWARE\WOW6432Node\WanaCrypt0r
```

Figure 14 Registry edit

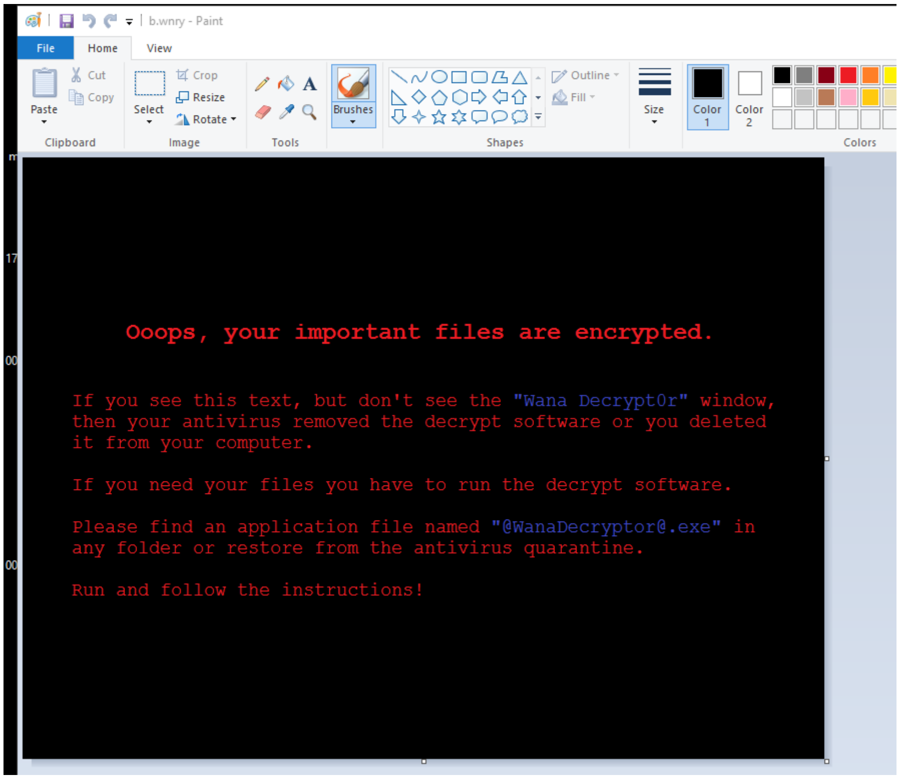
Figure 14 shows Sample One added WanaCrypt0r to the 32bit emulator.



```
C:\Users\user\Desktop\b.wnry
C:\Users\user\Desktop\b.wnry
C:\Users\user\Desktop\b.wnry
C:\Users\user\Desktop\b.wnry
C:\Users\user\Desktop\b.wnry
C:\Users\user\Desktop\b.wnry
C:\Users\user\Desktop\b.wnry
C:\Users\user\Desktop\b.wnry
C:\Users\user\Desktop\b.wnry
C:\Users\user\Desktop\b.wnry
C:\Users\user\Desktop\b.wnry
```

Figure 15 ”b.wnry”

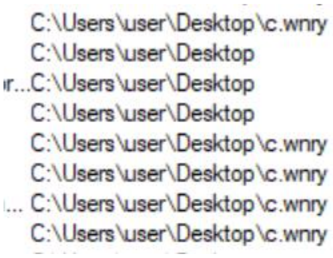
Figure 15 shows Sample One created the file “b.wnry” on the desktop.



```
Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.

Run and follow the instructions!
```

Figure 16 "b.wnry" contents

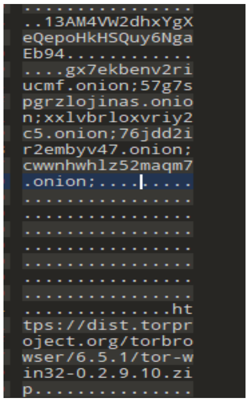
Figure 16 shows Sample One's ransom desktop background image in the 'b.wnry' file.



```
   C:\Users\user\Desktop\c.wnry
   C:\Users\user\Desktop
r...C:\Users\user\Desktop
   C:\Users\user\Desktop
   C:\Users\user\Desktop\c.wnry
   C:\Users\user\Desktop\c.wnry
... C:\Users\user\Desktop\c.wnry
   C:\Users\user\Desktop\c.wnry
```

Figure 17 "c.wrny" creation

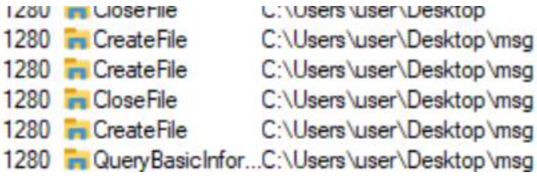
Figure 17 shows Sample One creates an additional file called "c.wnry" on the desktop



```
................
..13AM4VW2dhxYgX
eQepoHkHSQuy6Nga
Eb94............
....gx7ekbenv2ri
ucmf.onion;57g7s
pgrzlojinas.onio
n;xxlvbrloxvriy2
c5.onion;76jdd2i
r2embyv47.onion;
cwwnhwhlz52maqm7
.onion;.........
................
................
................
................
................
................
................
..............ht
tps://dist.torpr
oject.org/torbro
wser/6.5.1/tor-w
in32-0.2.9.10.zi
p...............
```

Figure 18 "c.wrny " in 010 Editor

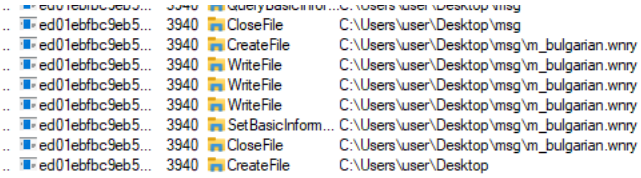
Figure 18 shows that Sample One "c.wrny" contained onion addresses and a Tor download link.



```
1280  CloseFile           C:\Users\user\Desktop
1280  CreateFile          C:\Users\user\Desktop\msg
1280  CreateFile          C:\Users\user\Desktop\msg
1280  CloseFile           C:\Users\user\Desktop\msg
1280  CreateFile          C:\Users\user\Desktop\msg
1280  QueryBasicInfor...  C:\Users\user\Desktop\msg
```

Figure 19 "/msg" directory

Figure 19 shows that Sample One created the "/msg" directory on the desktop where the ransom notes will go.



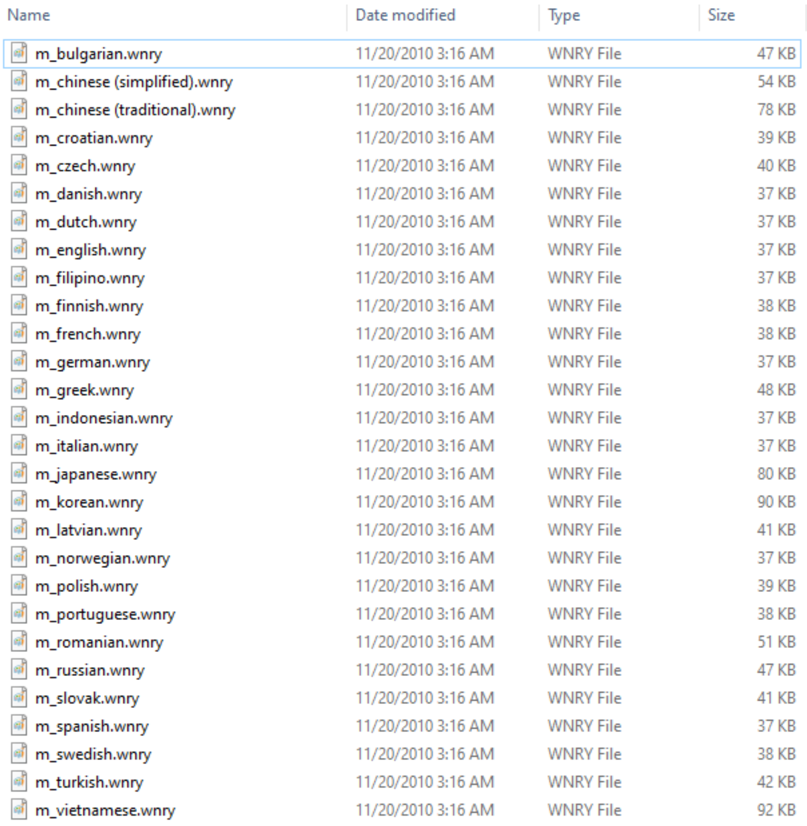
```
..  ed01ebfbc9eb5...  3940  QueryBasicInfor...  C:\Users\user\Desktop\msg
..  ed01ebfbc9eb5...  3940  CloseFile           C:\Users\user\Desktop\msg
..  ed01ebfbc9eb5...  3940  CreateFile          C:\Users\user\Desktop\msg\m_bulgarian.wnry
..  ed01ebfbc9eb5...  3940  WriteFile           C:\Users\user\Desktop\msg\m_bulgarian.wnry
..  ed01ebfbc9eb5...  3940  WriteFile           C:\Users\user\Desktop\msg\m_bulgarian.wnry
..  ed01ebfbc9eb5...  3940  WriteFile           C:\Users\user\Desktop\msg\m_bulgarian.wnry
..  ed01ebfbc9eb5...  3940  SetBasicInform...   C:\Users\user\Desktop\msg\m_bulgarian.wnry
..  ed01ebfbc9eb5...  3940  CloseFile           C:\Users\user\Desktop\msg\m_bulgarian.wnry
..  ed01ebfbc9eb5...  3940  CreateFile          C:\Users\user\Desktop
```

Figure 20 "bulgarian.wnry" creation

Figure 20 shows the creation of the "bulgarian.wnry" ransom message this ransom is also created in the following languages following a similar process.

Language	Filename
Bulgarian	m_bulgarian.wnry
Chinese	m_chinese (simplified).wnry
Chinese	m_chinese (traditional).wnry
Croatian	m_croatian.wnry
Czech	m_czech.wnry
Danish	m_danish.wnry
Dutch	m_dutch.wnry
English	m_english.wnry
Filipino	m_filipino.wnry
Finish	m_finnish.wnry

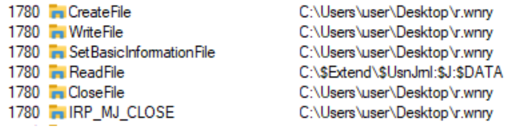
French	m_french.wnry
German	m_german.wnry
Greek	m_greek.wnry
Indonesian	m_indonesian.wnry
Italian	m_italian.wnry
Japanese	m_japanese.wnry
Korean	m_korean.wnry
Latvian	m_latvian.wnry
Norwegian	m_norwegian.wnry
Polish	m_polish.wnry
Portuguese	m_portuguese.wnry
Romanian	m_romanian.wnry
Russian	m_russian.wnry
Slovak	m_slovak.wnry
Spanish	m_spanish.wnry
Turkish	m_turkish.wnry
Vietnamese	m_vietnamese.wnry



Name	Date modified	Type	Size
m_bulgarian.wnry	11/20/2010 3:16 AM	WNRY File	47 KB
m_chinese (simplified).wnry	11/20/2010 3:16 AM	WNRY File	54 KB
m_chinese (traditional).wnry	11/20/2010 3:16 AM	WNRY File	78 KB
m_croatian.wnry	11/20/2010 3:16 AM	WNRY File	39 KB
m_czech.wnry	11/20/2010 3:16 AM	WNRY File	40 KB
m_danish.wnry	11/20/2010 3:16 AM	WNRY File	37 KB
m_dutch.wnry	11/20/2010 3:16 AM	WNRY File	37 KB
m_english.wnry	11/20/2010 3:16 AM	WNRY File	37 KB
m_filipino.wnry	11/20/2010 3:16 AM	WNRY File	37 KB
m_finnish.wnry	11/20/2010 3:16 AM	WNRY File	38 KB
m_french.wnry	11/20/2010 3:16 AM	WNRY File	38 KB
m_german.wnry	11/20/2010 3:16 AM	WNRY File	37 KB
m_greek.wnry	11/20/2010 3:16 AM	WNRY File	48 KB
m_indonesian.wnry	11/20/2010 3:16 AM	WNRY File	37 KB
m_italian.wnry	11/20/2010 3:16 AM	WNRY File	37 KB
m_japanese.wnry	11/20/2010 3:16 AM	WNRY File	80 KB
m_korean.wnry	11/20/2010 3:16 AM	WNRY File	90 KB
m_latvian.wnry	11/20/2010 3:16 AM	WNRY File	41 KB
m_norwegian.wnry	11/20/2010 3:16 AM	WNRY File	37 KB
m_polish.wnry	11/20/2010 3:16 AM	WNRY File	39 KB
m_portuguese.wnry	11/20/2010 3:16 AM	WNRY File	38 KB
m_romanian.wnry	11/20/2010 3:16 AM	WNRY File	51 KB
m_russian.wnry	11/20/2010 3:16 AM	WNRY File	47 KB
m_slovak.wnry	11/20/2010 3:16 AM	WNRY File	41 KB
m_spanish.wnry	11/20/2010 3:16 AM	WNRY File	37 KB
m_swedish.wnry	11/20/2010 3:16 AM	WNRY File	38 KB
m_turkish.wnry	11/20/2010 3:16 AM	WNRY File	42 KB
m_vietnamese.wnry	11/20/2010 3:16 AM	WNRY File	92 KB

Figure 21 /msg directory

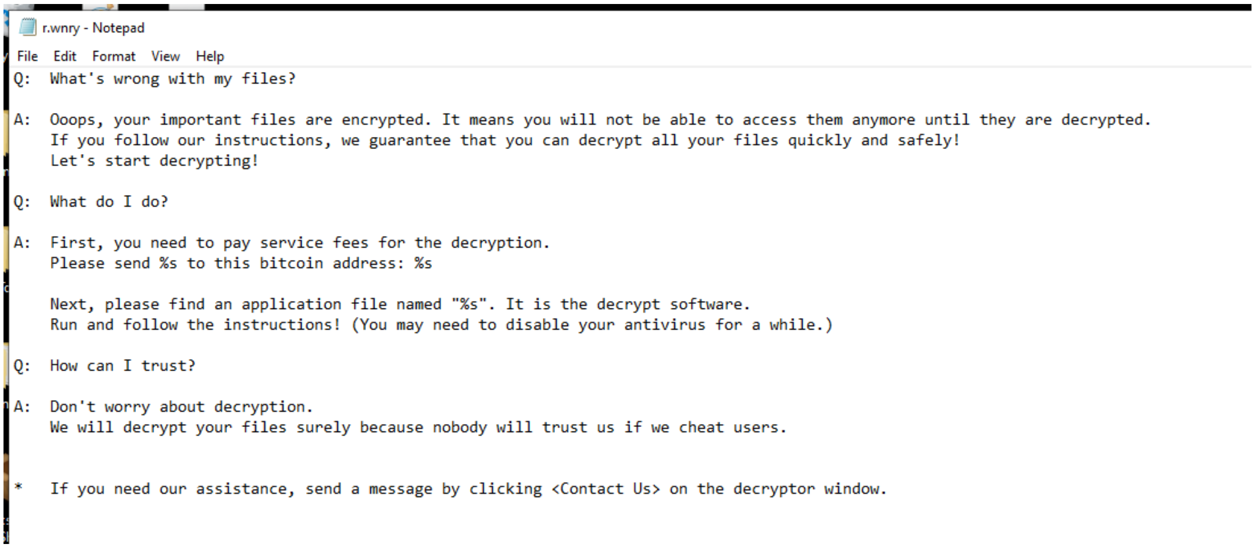
Figure 21 shows Sample One creates a message directory which Identifies the various language the ransom note was wrote in.



```
1780  CreateFile                  C:\Users\user\Desktop\r.wnry
1780  WriteFile                   C:\Users\user\Desktop\r.wnry
1780  SetBasicInformationFile     C:\Users\user\Desktop\r.wnry
1780  ReadFile                    C:\$Extend\$UsnJrnl:$J:$DATA
1780  CloseFile                   C:\Users\user\Desktop\r.wnry
1780  IRP_MJ_CLOSE                C:\Users\user\Desktop\r.wnry
```

Figure 22 "r.wnry"

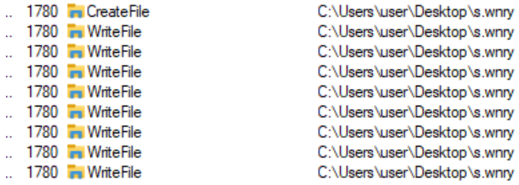
Figure 22 shows Sample One then created and wrote to the "r.wnry" file on the desktop



```
Q:  What's wrong with my files?

A:  Ooops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted.
    If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely!
    Let's start decrypting!

Q:  What do I do?

A:  First, you need to pay service fees for the decryption.
    Please send %s to this bitcoin address: %s

    Next, please find an application file named "%s". It is the decrypt software.
    Run and follow the instructions! (You may need to disable your antivirus for a while.)

Q:  How can I trust?

A:  Don't worry about decryption.
    We will decrypt your files surely because nobody will trust us if we cheat users.


*   If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.
```

Figure 23 "r.wnry" ransom note

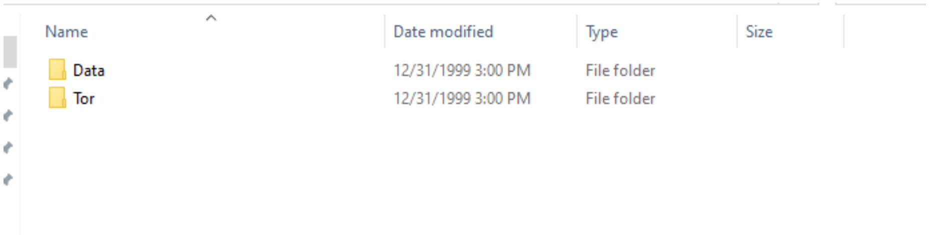
Figure 23 shows Sample Ones "r.wnry" ransom text.



```
1780  CreateFile    C:\Users\user\Desktop\s.wnry
1780  WriteFile     C:\Users\user\Desktop\s.wnry
1780  WriteFile     C:\Users\user\Desktop\s.wnry
1780  WriteFile     C:\Users\user\Desktop\s.wnry
1780  WriteFile     C:\Users\user\Desktop\s.wnry
1780  WriteFile     C:\Users\user\Desktop\s.wnry
1780  WriteFile     C:\Users\user\Desktop\s.wnry
1780  WriteFile     C:\Users\user\Desktop\s.wnry
1780  WriteFile     C:\Users\user\Desktop\s.wnry
```

Figure 24 "s.wnry" creation

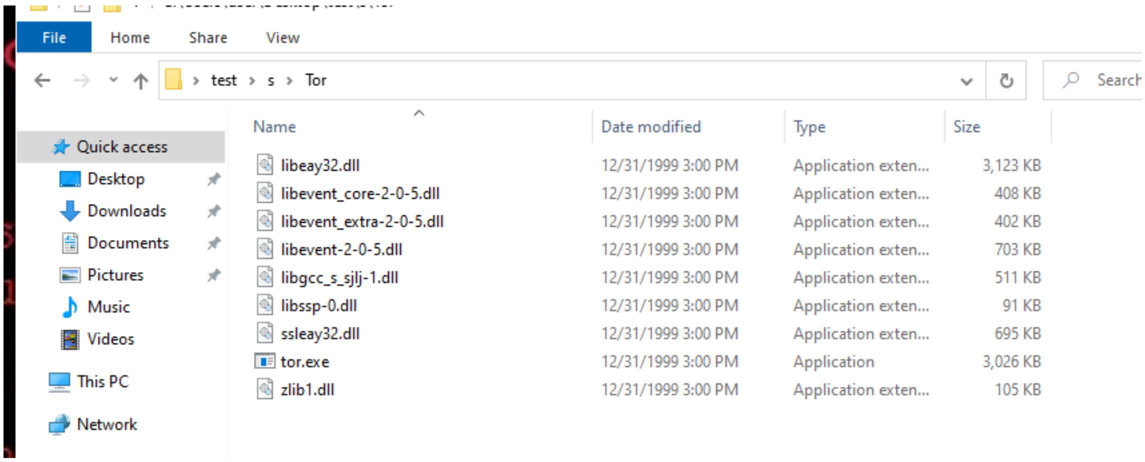
Figure 24 identifies the creation of the "s.wnry" file on the desktop



Name	Date modified	Type	Size
Data	12/31/1999 3:00 PM	File folder	
Tor	12/31/1999 3:00 PM	File folder	

Figure 25 "s.wnry" extraction

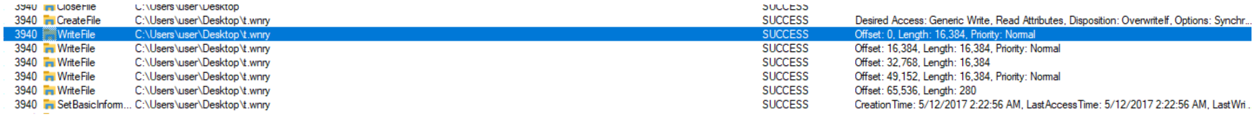
Figure 25 shows Sample One created “s.wnry” file . The file when unzipped contains two directories’ “Data” and “Tor”. Nothing is contained within the Data directory.



Name	Date modified	Type	Size
libeay32.dll	12/31/1999 3:00 PM	Application exten...	3,123 KB
libevent_core-2-0-5.dll	12/31/1999 3:00 PM	Application exten...	408 KB
libevent_extra-2-0-5.dll	12/31/1999 3:00 PM	Application exten...	402 KB
libevent-2-0-5.dll	12/31/1999 3:00 PM	Application exten...	703 KB
libgcc_s_sjlj-1.dll	12/31/1999 3:00 PM	Application exten...	511 KB
libssp-0.dll	12/31/1999 3:00 PM	Application exten...	91 KB
ssleay32.dll	12/31/1999 3:00 PM	Application exten...	695 KB
tor.exe	12/31/1999 3:00 PM	Application	3,026 KB
zlib1.dll	12/31/1999 3:00 PM	Application exten...	105 KB

Figure 26 Tor Directory

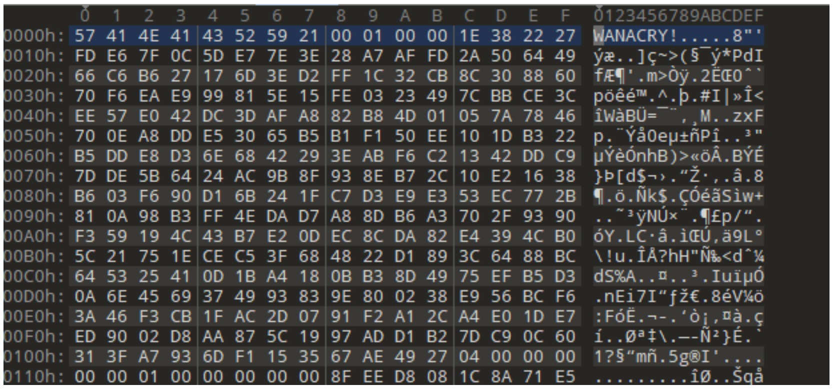
Figure 26 shows the contents of the Tor directory. This contains the install executable and relevant DLLs for the Tor browser.



```
3940  CloseFile       C:\Users\user\Desktop          SUCCESS
3940  CreateFile      C:\Users\user\Desktop\t.wnry   SUCCESS   Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: Synchr...
3940  WriteFile       C:\Users\user\Desktop\t.wnry   SUCCESS   Offset: 0, Length: 16,384, Priority: Normal
3940  WriteFile       C:\Users\user\Desktop\t.wnry   SUCCESS   Offset: 16,384, Length: 16,384, Priority: Normal
3940  WriteFile       C:\Users\user\Desktop\t.wnry   SUCCESS   Offset: 32,768, Length: 16,384
3940  WriteFile       C:\Users\user\Desktop\t.wnry   SUCCESS   Offset: 49,152, Length: 16,384, Priority: Normal
3940  WriteFile       C:\Users\user\Desktop\t.wnry   SUCCESS   Offset: 65,536, Length: 280
3940  SetBasicInform... C:\Users\user\Desktop\t.wnry SUCCESS   CreationTime: 5/12/2017 2:22:56 AM, LastAccessTime: 5/12/2017 2:22:56 AM, LastWri...
```

Figure 27 "t.wnry" creation

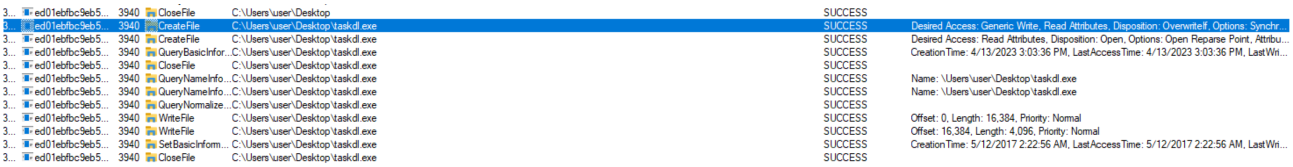
Figure 27 shows Sample One created “t.wnry” file.



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 57 41 4E 41 43 52 59 21 00 01 00 00 1E 38 22 27  WANACRY!.....8"'
0010h: FD E6 7F 0C 5D E7 7E 3E 28 A7 AF FD 2A 50 64 49  ýæ..]ç~>(§¯ý*PdI
0020h: 66 C6 B6 27 17 6D 3E D2 FF 1C 32 CB 8C 30 88 60  fÆ¶'.m>Òÿ.2ËŒ0ˆ`
0030h: 70 F6 EA E9 99 81 5E 15 FE 03 23 49 7C BB CE 3C  pöêé™.^.þ.#I|»Î<
0040h: EE 57 E0 42 DC 3D AF A8 82 B8 4D 01 05 7A 78 46  îWàBÜ=¯¨‚¸M..zxF
0050h: 70 0E A8 DD E5 30 65 B5 B1 F1 50 EE 10 1D B3 22  p.¨Ýå0eµ±ñPî..³"
0060h: B5 DD E8 D3 6E 68 42 29 3E AB F6 C2 13 42 DD C9  µÝèÓnhB)>«öÂ.BÝÉ
0070h: 7D DE 5B 64 24 AC 9B 8F 93 8E B7 2C 10 E2 16 38  }Þ[d$¬›.“Ž·,.â.8
0080h: B6 03 F6 90 D1 6B 24 1F C7 D3 E9 E3 53 EC 77 2B  ¶.ö.Ñk$.ÇÓéãSìw+
0090h: 81 0A 98 B3 FF 4E DA D7 A8 8D B6 A3 70 2F 93 90  ..˜³ÿNÚ×¨.¶£p/“.
00A0h: F3 59 19 4C 43 B7 E2 0D EC 8C DA 82 E4 39 4C B0  óY.LC·â.ìŒÚ‚ä9L°
00B0h: 5C 21 75 1E CE C5 3F 68 48 22 D1 89 3C 64 88 BC  \!u.ÎÅ?hH"Ñ‰<dˆ¼
00C0h: 64 53 25 41 0D 1B A4 18 0B B3 8D 49 75 EF B5 D3  dS%A..¤..³.IuïµÓ
00D0h: 0A 6E 45 69 37 49 93 83 9E 80 02 38 E9 56 BC F6  .nEi7I“ƒž€.8éV¼ö
00E0h: 3A 46 F3 CB 1F AC 2D 07 91 F2 A1 2C A4 E0 1D E7  :FóË.¬-.‘ò¡,¤à.ç
00F0h: ED 90 02 D8 AA 87 5C 19 97 AD D1 B2 7D C9 0C 60  í..Øª‡\.—Ñ²}É.`
0100h: 31 3F A7 93 6D F1 15 35 67 AE 49 27 04 00 00 00  1?§“mñ.5g®I'....
0110h: 00 00 01 00 00 00 00 00 8F EE D8 08 1C 8A 71 E5  .........îØ..Šqå
```

Figure 28 Encrypted tool

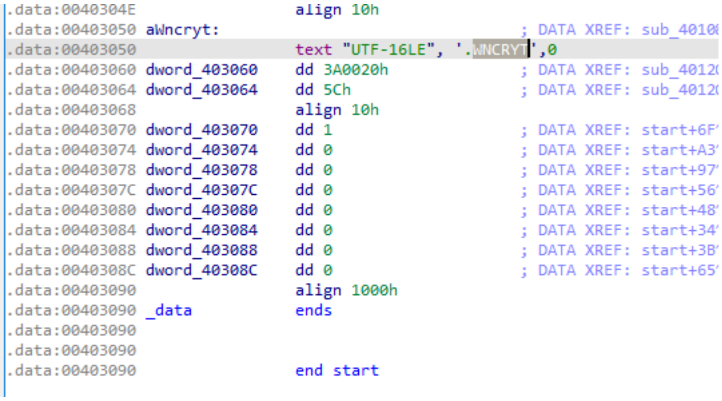
Figure 28 shows “t.wnry” in 010 Editor the data begins with “WANACRY!” which identifies the file as being encrypted.



```
3... ed01ebfbc9eb5... 3940 CloseFile          C:\Users\user\Desktop              SUCCESS
3... ed01ebfbc9eb5... 3940 CreateFile         C:\Users\user\Desktop\taskdl.exe   SUCCESS  Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: Synchr...
3... ed01ebfbc9eb5... 3940 CreateFile         C:\Users\user\Desktop\taskdl.exe   SUCCESS  Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attribu...
3... ed01ebfbc9eb5... 3940 QueryBasicInfor... C:\Users\user\Desktop\taskdl.exe   SUCCESS  CreationTime: 4/13/2023 3:03:36 PM, LastAccessTime: 4/13/2023 3:03:36 PM, LastWri...
3... ed01ebfbc9eb5... 3940 CloseFile          C:\Users\user\Desktop\taskdl.exe   SUCCESS
3... ed01ebfbc9eb5... 3940 QueryNameInfo...   C:\Users\user\Desktop\taskdl.exe   SUCCESS  Name: \Users\user\Desktop\taskdl.exe
3... ed01ebfbc9eb5... 3940 QueryNameInfo...   C:\Users\user\Desktop\taskdl.exe   SUCCESS  Name: \Users\user\Desktop\taskdl.exe
3... ed01ebfbc9eb5... 3940 QueryNormalize...  C:\Users\user\Desktop\taskdl.exe   SUCCESS
3... ed01ebfbc9eb5... 3940 WriteFile          C:\Users\user\Desktop\taskdl.exe   SUCCESS  Offset: 0, Length: 16,384, Priority: Normal
3... ed01ebfbc9eb5... 3940 WriteFile          C:\Users\user\Desktop\taskdl.exe   SUCCESS  Offset: 16,384, Length: 4,096, Priority: Normal
3... ed01ebfbc9eb5... 3940 SetBasicInform...  C:\Users\user\Desktop\taskdl.exe   SUCCESS  CreationTime: 5/12/2017 2:22:56 AM, LastAccessTime: 5/12/2017 2:22:56 AM, LastWri...
3... ed01ebfbc9eb5... 3940 CloseFile          C:\Users\user\Desktop\taskdl.exe   SUCCESS
```

Figure 29 taskdl.exe

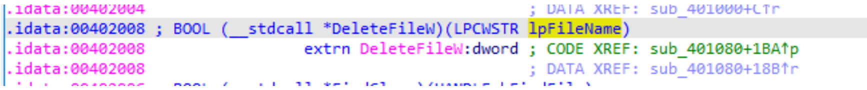
Figure 29 shows the creation of the file “taskdl.exe” on the desktop.



```
.data:0040304E                 align 10h
.data:00403050 aWncryt:                                 ; DATA XREF: sub_4010(
.data:00403050                 text "UTF-16LE", '.WNCRYT',0
.data:00403060 dword_403060    dd 3A0020h               ; DATA XREF: sub_4012(
.data:00403064 dword_403064    dd 5Ch                   ; DATA XREF: sub_4012(
.data:00403068                 align 10h
.data:00403070 dword_403070    dd 1                     ; DATA XREF: start+6F'
.data:00403074 dword_403074    dd 0                     ; DATA XREF: start+A3'
.data:00403078 dword_403078    dd 0                     ; DATA XREF: start+97'
.data:0040307C dword_40307C    dd 0                     ; DATA XREF: start+56'
.data:00403080 dword_403080    dd 0                     ; DATA XREF: start+48'
.data:00403084 dword_403084    dd 0                     ; DATA XREF: start+34'
.data:00403088 dword_403088    dd 0                     ; DATA XREF: start+3B'
.data:0040308C dword_40308C    dd 0                     ; DATA XREF: start+65'
.data:00403090                 align 1000h
.data:00403090 _data           ends
.data:00403090
.data:00403090
.data:00403090                 end start
```

Figure 30 ".WNCRYT"

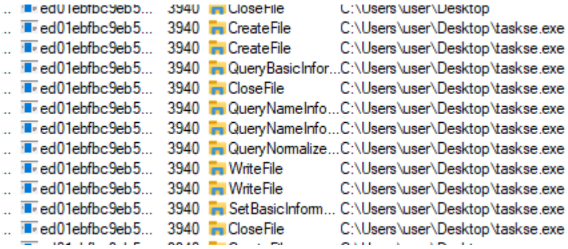
Figure 30 shows the disassembled “taskdl.exe” it includes the “.WNCRYT “file extension



```
.idata:00402004                                 ; DATA XREF: sub_401000+C↑r
.idata:00402008 ; BOOL (__stdcall *DeleteFileW)(LPCWSTR lpFileName)
.idata:00402008                 extrn DeleteFileW:dword ; CODE XREF: sub_401080+1BA↑p
.idata:00402008                                 ; DATA XREF: sub_401080+18B↑r
```

Figure 31 DeleteFileW

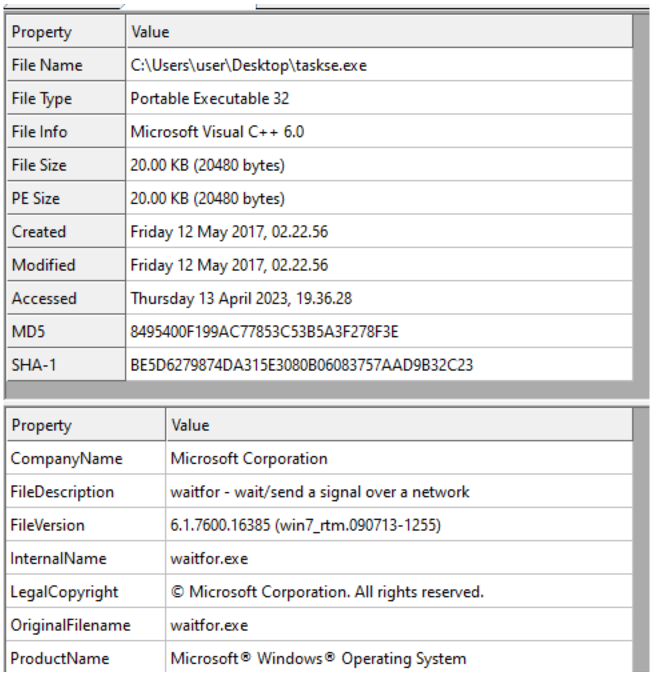
Figure 31 shows DeleteFileW pointer in IDA this executable may delete files.



```
.. ed01ebfbc9eb5... 3940 CloseFile          C:\Users\user\Desktop
.. ed01ebfbc9eb5... 3940 CreateFile         C:\Users\user\Desktop\taskse.exe
.. ed01ebfbc9eb5... 3940 CreateFile         C:\Users\user\Desktop\taskse.exe
.. ed01ebfbc9eb5... 3940 QueryBasicInfor... C:\Users\user\Desktop\taskse.exe
.. ed01ebfbc9eb5... 3940 CloseFile          C:\Users\user\Desktop\taskse.exe
.. ed01ebfbc9eb5... 3940 QueryNameInfo...   C:\Users\user\Desktop\taskse.exe
.. ed01ebfbc9eb5... 3940 QueryNameInfo...   C:\Users\user\Desktop\taskse.exe
.. ed01ebfbc9eb5... 3940 QueryNormalize...  C:\Users\user\Desktop\taskse.exe
.. ed01ebfbc9eb5... 3940 WriteFile          C:\Users\user\Desktop\taskse.exe
.. ed01ebfbc9eb5... 3940 WriteFile          C:\Users\user\Desktop\taskse.exe
.. ed01ebfbc9eb5... 3940 SetBasicInform...  C:\Users\user\Desktop\taskse.exe
.. ed01ebfbc9eb5... 3940 CloseFile          C:\Users\user\Desktop\taskse.exe
```

Figure 32 taskse.exe

Figure 32 shows the next process that the Sample One malware generates is the “taskse.exe”on the desktop.

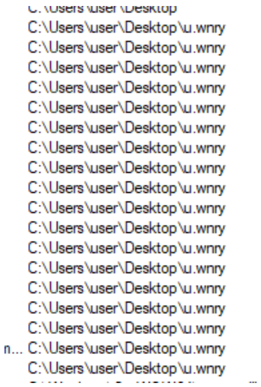


Property	Value
File Name	C:\Users\user\Desktop\taskse.exe
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	20.00 KB (20480 bytes)
PE Size	20.00 KB (20480 bytes)
Created	Friday 12 May 2017, 02.22.56
Modified	Friday 12 May 2017, 02.22.56
Accessed	Thursday 13 April 2023, 19.36.28
MD5	8495400F199AC77853C53B5A3F278F3E
SHA-1	BE5D6279874DA315E3080B06083757AAD9B32C23

Property	Value
CompanyName	Microsoft Corporation
FileDescription	waitfor - wait/send a signal over a network
FileVersion	6.1.7600.16385 (win7_rtm.090713-1255)
InternalName	waitfor.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	waitfor.exe
ProductName	Microsoft® Windows® Operating System

Figure 33 CFF Explorer

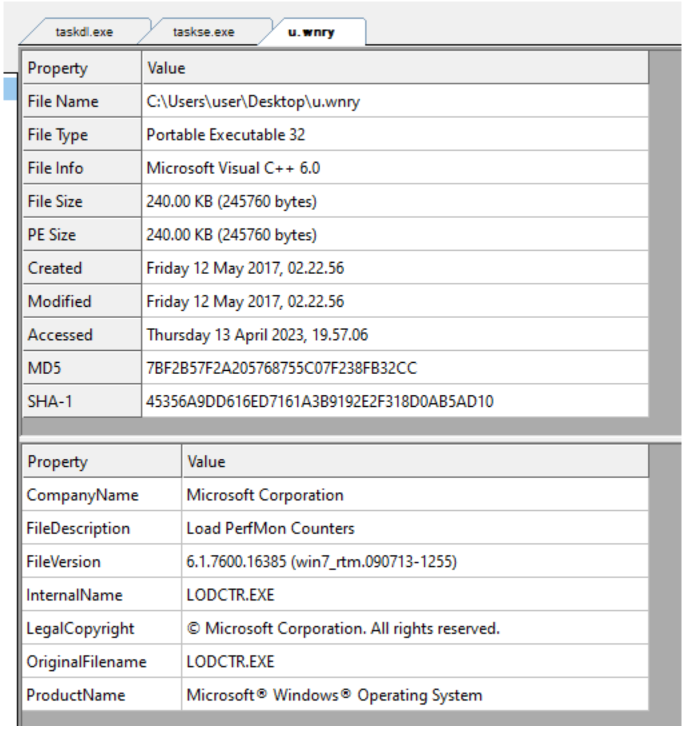
Figure 33 shows the “taskse.exe” was originally called “waitfor.exe” with a description of “waitfor – wait/send a signal over a network” which suggests this may be part of the decryption tool.



```
    C:\Users\user\Desktop
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
n... C:\Users\user\Desktop\u.wnry
    C:\Users\user\Desktop\u.wnry
```

Figure 34 "u.wnry" file creation

Figure 34 shows Sample One created “u.wnry” on the desktop.

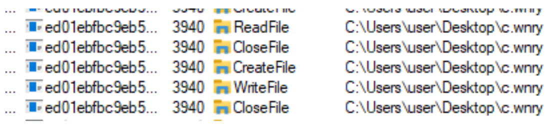


Property	Value
File Name	C:\Users\user\Desktop\u.wnry
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	240.00 KB (245760 bytes)
PE Size	240.00 KB (245760 bytes)
Created	Friday 12 May 2017, 02.22.56
Modified	Friday 12 May 2017, 02.22.56
Accessed	Thursday 13 April 2023, 19.57.06
MD5	7BF2B57F2A205768755C07F238FB32CC
SHA-1	45356A9DD616ED7161A3B9192E2F318D0AB5AD10

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Load PerfMon Counters
FileVersion	6.1.7600.16385 (win7_rtm.090713-1255)
InternalName	LODCTR.EXE
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	LODCTR.EXE
ProductName	Microsoft® Windows® Operating System

Figure 35 CFF Explorer showing "u.wnry"

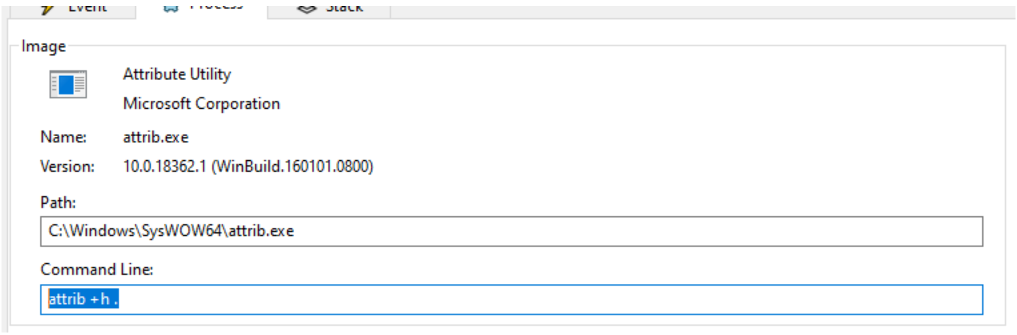
Figure 35 shows the "u.wnry" was originally called "LODCTR.exe" with a description of "Load PerfMon Counter".



```
... ed01ebfbc9eb5... 3940 ReadFile    C:\Users\user\Desktop\c.wnry
... ed01ebfbc9eb5... 3940 CloseFile   C:\Users\user\Desktop\c.wnry
... ed01ebfbc9eb5... 3940 CreateFile  C:\Users\user\Desktop\c.wnry
... ed01ebfbc9eb5... 3940 WriteFile   C:\Users\user\Desktop\c.wnry
... ed01ebfbc9eb5... 3940 CloseFile   C:\Users\user\Desktop\c.wnry
```

Figure 36 "c.wnry"

Figure 36 shows "c.wnry" being written to and read from on the desktop.



Attribute Utility
Microsoft Corporation

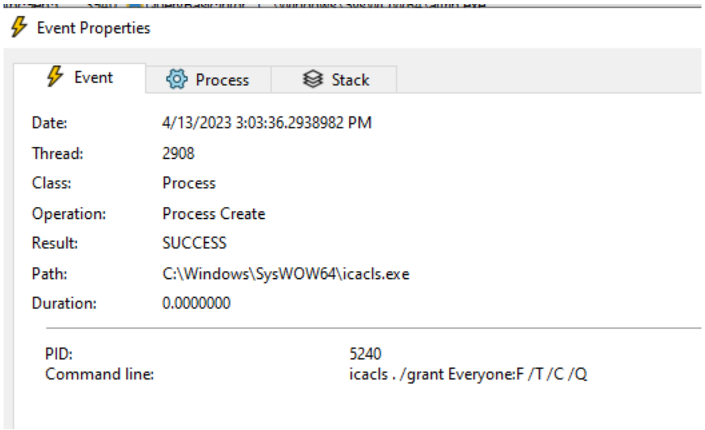
Name: attrib.exe
Version: 10.0.18362.1 (WinBuild.160101.0800)

Path:
C:\Windows\SysWOW64\attrib.exe

Command Line:
attrib +h .

Figure 37

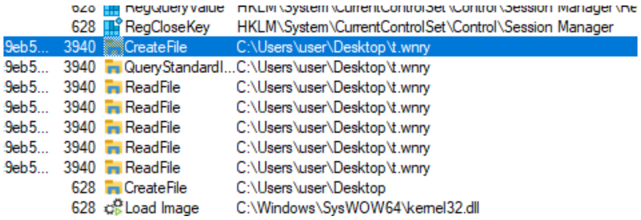
Figure 37 shows Sample One setting the files in the current directory to hidden. The directory was "C:\Users\user\Desktop\".



```
Date:          4/13/2023 3:03:36.2938982 PM
Thread:        2908
Class:         Process
Operation:     Process Create
Result:        SUCCESS
Path:          C:\Windows\SysWOW64\icacls.exe
Duration:      0.0000000

PID:                         5240
Command line:                icacls . /grant Everyone:F /T /C /Q
```

Figure 38 "icalcs" command

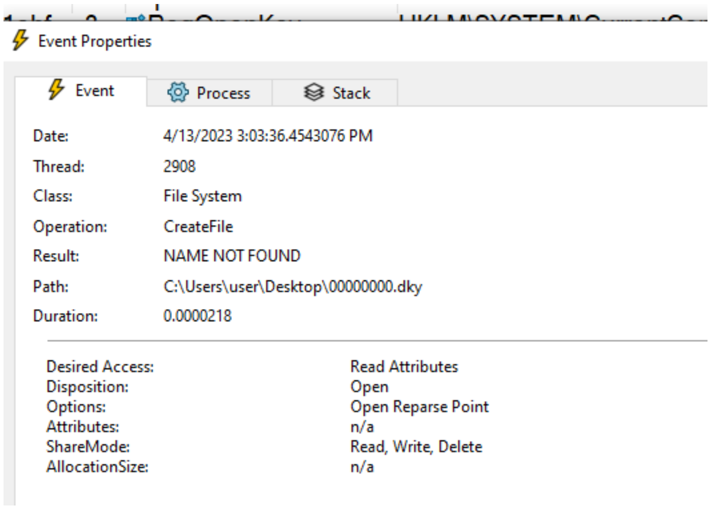
Figure 38 shows Sample One executed the "icalcs" command altering permissions to allow for everyone to modify files and folders.



```
          628  RegQueryValue   HKLM\System\CurrentControlSet\Control\Session Manager\Re
          628  RegCloseKey     HKLM\System\CurrentControlSet\Control\Session Manager
9eb5...  3940  CreateFile      C:\Users\user\Desktop\t.wnry
9eb5...  3940  QueryStandardI...C:\Users\user\Desktop\t.wnry
9eb5...  3940  ReadFile        C:\Users\user\Desktop\t.wnry
9eb5...  3940  ReadFile        C:\Users\user\Desktop\t.wnry
9eb5...  3940  ReadFile        C:\Users\user\Desktop\t.wnry
9eb5...  3940  ReadFile        C:\Users\user\Desktop\t.wnry
9eb5...  3940  ReadFile        C:\Users\user\Desktop\t.wnry
          628  CreateFile      C:\Users\user\Desktop
          628  Load Image      C:\Windows\SysWOW64\kernel32.dll
```

Figure 39 t.wnry

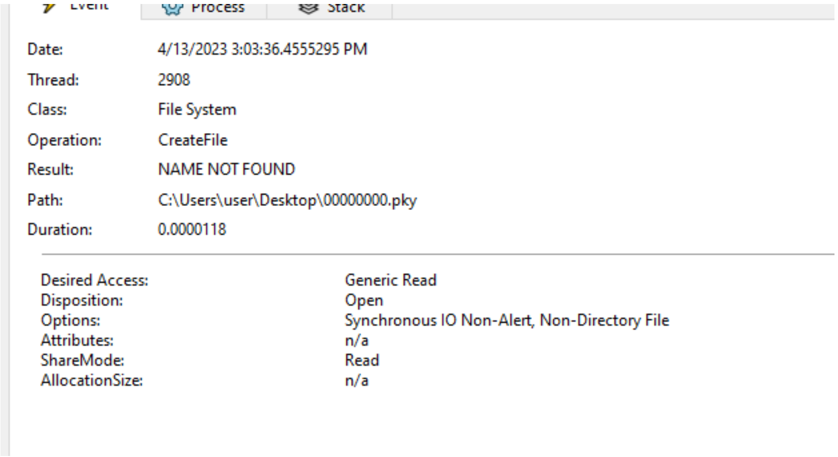
Figure 39 shows Sample One reading information from "t.wnry" on the desktop



```
Date:          4/13/2023 3:03:36.4543076 PM
Thread:        2908
Class:         File System
Operation:     CreateFile
Result:        NAME NOT FOUND
Path:          C:\Users\user\Desktop\00000000.dky
Duration:      0.0000218

Desired Access:              Read Attributes
Disposition:                 Open
Options:                     Open Reparse Point
Attributes:                  n/a
ShareMode:                   Read, Write, Delete
AllocationSize:              n/a
```

Figure 40 Process Monitor event

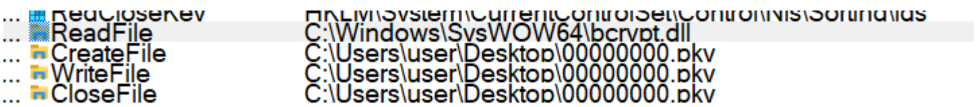
Figure 40 shows Sample One failing to fetch a key called "00000000.dky" from the desktop



```
Date:         4/13/2023 3:03:36.4555295 PM
Thread:       2908
Class:        File System
Operation:    CreateFile
Result:       NAME NOT FOUND
Path:         C:\Users\user\Desktop\00000000.pky
Duration:     0.0000118

  Desired Access:          Generic Read
  Disposition:             Open
  Options:                 Synchronous IO Non-Alert, Non-Directory File
  Attributes:              n/a
  ShareMode:               Read
  AllocationSize:          n/a
```

Figure 41 ".pky" key fail

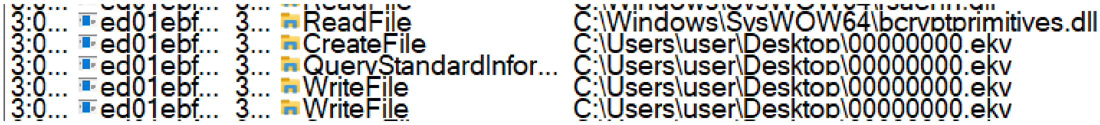
Figure 41 shows Sample One failing to fetch a key called "00000000.pky" from the desktop.



```
... RegCloseKey    HKLM\System\CurrentControlSet\Control\Nls\Sorting\Ids
... ReadFile       C:\Windows\SysWOW64\bcrypt.dll
... CreateFile     C:\Users\user\Desktop\00000000.pky
... WriteFile      C:\Users\user\Desktop\00000000.pky
... CloseFile      C:\Users\user\Desktop\00000000.pky
```

Figure 42 ".pky" creation

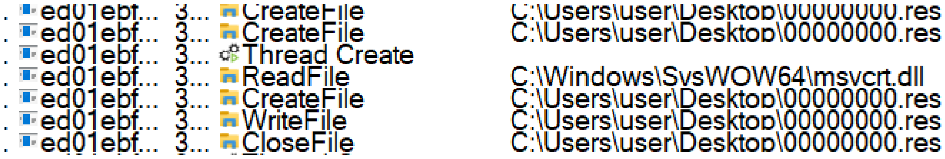
Figure 42 shows Sample One creating "00000000.pky" an encryption key on the desktop after failing to find it. Initially 276 bytes are added to it.



```
3:0... ed01ebf... 3... ReadFile             C:\Windows\SysWOW64\bcryptprimitives.dll
3:0... ed01ebf... 3... CreateFile           C:\Users\user\Desktop\00000000.eky
3:0... ed01ebf... 3... QueryStandardInfor... C:\Users\user\Desktop\00000000.eky
3:0... ed01ebf... 3... WriteFile            C:\Users\user\Desktop\00000000.eky
3:0... ed01ebf... 3... WriteFile            C:\Users\user\Desktop\00000000.eky
```

Figure 43 ".eky" creation

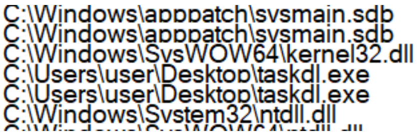
Figure 43 shows another encryption key being created called "00000000.eky" on the desktop



```
. ed01ebf... 3... CreateFile     C:\Users\user\Desktop\00000000.res
. ed01ebf... 3... CreateFile     C:\Users\user\Desktop\00000000.res
. ed01ebf... 3... Thread Create
. ed01ebf... 3... ReadFile       C:\Windows\SysWOW64\msvcrt.dll
. ed01ebf... 3... CreateFile     C:\Users\user\Desktop\00000000.res
. ed01ebf... 3... WriteFile      C:\Users\user\Desktop\00000000.res
. ed01ebf... 3... CloseFile      C:\Users\user\Desktop\00000000.res
```

Figure 44 ".res" creation

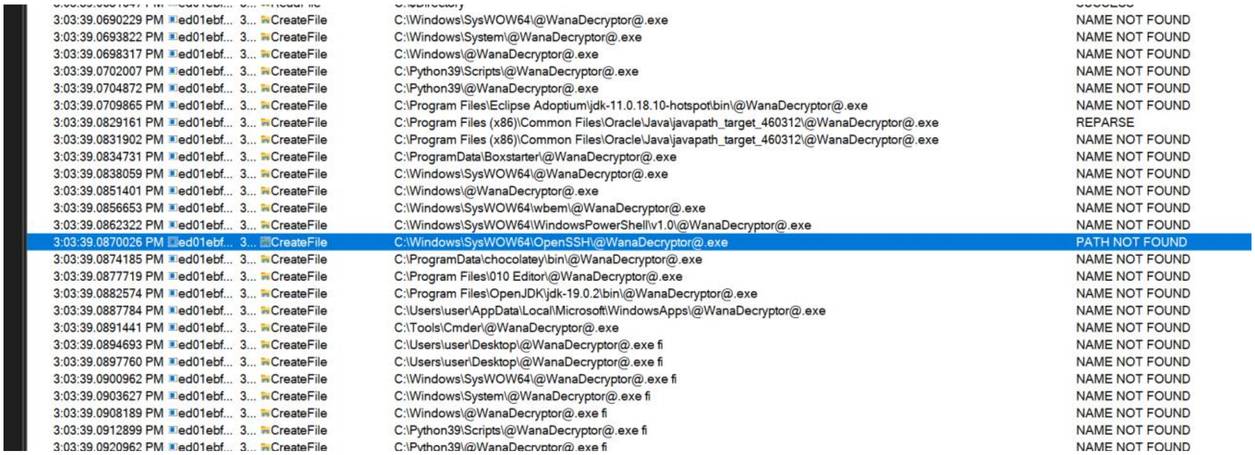
Figure 44 shows another encryption key called "00000000.res" added to the desktop with 176 bytes being added.



```
C:\Windows\apppatch\sysmain.sdb
C:\Windows\apppatch\sysmain.sdb
C:\Windows\SysWOW64\kernel32.dll
C:\Users\user\Desktop\taskdl.exe
C:\Users\user\Desktop\taskdl.exe
C:\Windows\System32\ntdll.dll
```

Figure 45 "taskdl.exe"

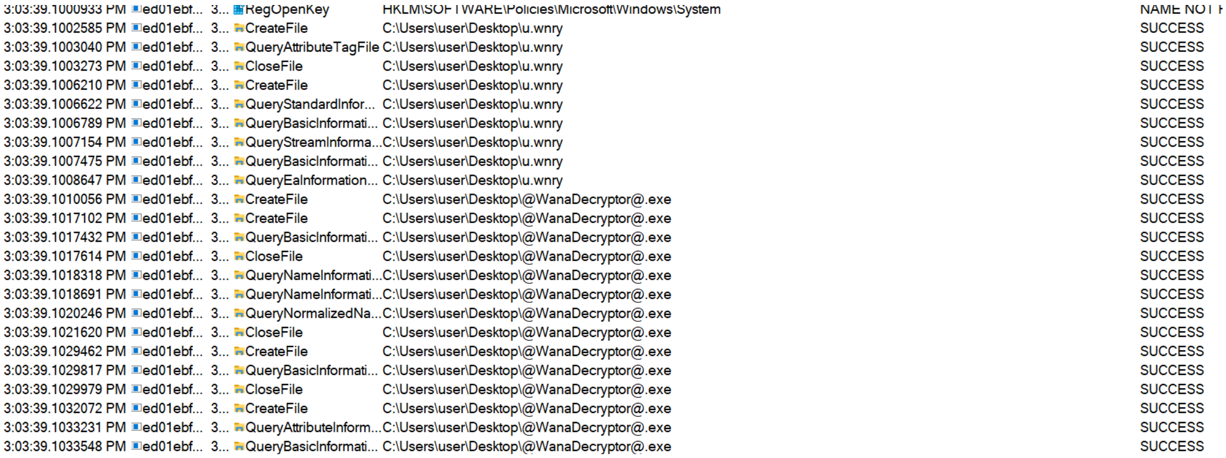
Figure 45 shows Sample One calling "taskdl.exe".



```
3:03:39.0690229 PM  ed01ebf...  3...  CreateFile  C:\Windows\SysWOW64\@WanaDecryptor@.exe                                                   NAME NOT FOUND
3:03:39.0693822 PM  ed01ebf...  3...  CreateFile  C:\Windows\System\@WanaDecryptor@.exe                                                     NAME NOT FOUND
3:03:39.0698317 PM  ed01ebf...  3...  CreateFile  C:\Windows\@WanaDecryptor@.exe                                                            NAME NOT FOUND
3:03:39.0702007 PM  ed01ebf...  3...  CreateFile  C:\Python39\Scripts\@WanaDecryptor@.exe                                                   NAME NOT FOUND
3:03:39.0704872 PM  ed01ebf...  3...  CreateFile  C:\Python39\@WanaDecryptor@.exe                                                           NAME NOT FOUND
3:03:39.0709865 PM  ed01ebf...  3...  CreateFile  C:\Program Files\Eclipse Adoptium\jdk-11.0.18.10-hotspot\bin\@WanaDecryptor@.exe           NAME NOT FOUND
3:03:39.0829161 PM  ed01ebf...  3...  CreateFile  C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_460312\@WanaDecryptor@.exe REPARSE
3:03:39.0831902 PM  ed01ebf...  3...  CreateFile  C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_460312\@WanaDecryptor@.exe NAME NOT FOUND
3:03:39.0834731 PM  ed01ebf...  3...  CreateFile  C:\ProgramData\Boxstarter\@WanaDecryptor@.exe                                             NAME NOT FOUND
3:03:39.0838059 PM  ed01ebf...  3...  CreateFile  C:\Windows\SysWOW64\@WanaDecryptor@.exe                                                   NAME NOT FOUND
3:03:39.0851401 PM  ed01ebf...  3...  CreateFile  C:\Windows\@WanaDecryptor@.exe                                                            NAME NOT FOUND
3:03:39.0856653 PM  ed01ebf...  3...  CreateFile  C:\Windows\SysWOW64\wbem\@WanaDecryptor@.exe                                              NAME NOT FOUND
3:03:39.0862322 PM  ed01ebf...  3...  CreateFile  C:\Windows\SysWOW64\WindowsPowerShell\v1.0\@WanaDecryptor@.exe                            NAME NOT FOUND
3:03:39.0870026 PM  ed01ebf...  3...  CreateFile  C:\Windows\SysWOW64\OpenSSH\@WanaDecryptor@.exe                                           PATH NOT FOUND
3:03:39.0874185 PM  ed01ebf...  3...  CreateFile  C:\ProgramData\chocolatey\bin\@WanaDecryptor@.exe                                         NAME NOT FOUND
3:03:39.0877719 PM  ed01ebf...  3...  CreateFile  C:\Program Files\010 Editor\@WanaDecryptor@.exe                                           NAME NOT FOUND
3:03:39.0882574 PM  ed01ebf...  3...  CreateFile  C:\Program Files\OpenJDK\jdk-19.0.2\bin\@WanaDecryptor@.exe                               NAME NOT FOUND
3:03:39.0887784 PM  ed01ebf...  3...  CreateFile  C:\Users\user\AppData\Local\Microsoft\WindowsApps\@WanaDecryptor@.exe                     NAME NOT FOUND
3:03:39.0891441 PM  ed01ebf...  3...  CreateFile  C:\Tools\Cmder\@WanaDecryptor@.exe                                                        NAME NOT FOUND
3:03:39.0894693 PM  ed01ebf...  3...  CreateFile  C:\Users\user\Desktop\@WanaDecryptor@.exe fi                                              NAME NOT FOUND
3:03:39.0897760 PM  ed01ebf...  3...  CreateFile  C:\Users\user\Desktop\@WanaDecryptor@.exe fi                                              NAME NOT FOUND
3:03:39.0900962 PM  ed01ebf...  3...  CreateFile  C:\Windows\SysWOW64\@WanaDecryptor@.exe fi                                                NAME NOT FOUND
3:03:39.0903627 PM  ed01ebf...  3...  CreateFile  C:\Windows\System\@WanaDecryptor@.exe fi                                                  NAME NOT FOUND
3:03:39.0908189 PM  ed01ebf...  3...  CreateFile  C:\Windows\@WanaDecryptor@.exe fi                                                         NAME NOT FOUND
3:03:39.0912899 PM  ed01ebf...  3...  CreateFile  C:\Python39\Scripts\@WanaDecryptor@.exe fi                                                NAME NOT FOUND
3:03:39.0920962 PM  ed01ebf...  3...  CreateFile  C:\Python39\@WanaDecryptor@.exe fi                                                        NAME NOT FOUND
```

Figure 46 "@WanaDecryptor@.exe"

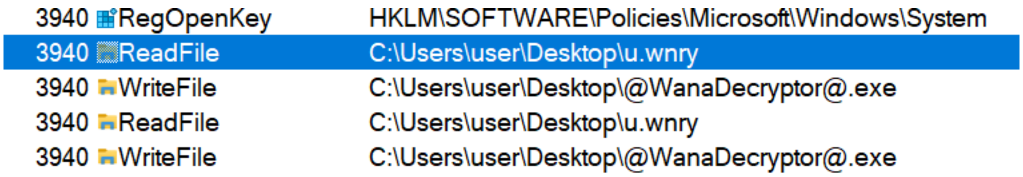
Figure 46 shows Sample One failing to create files in various directories on the "C:\" drive, including the "@WannaDecryptor@.exe" executable file.



```
3:03:39.1000933 PM  ed01ebf...  3...  RegOpenKey             HKLM\SOFTWARE\Policies\Microsoft\Windows\System  NAME NOT F
3:03:39.1002585 PM  ed01ebf...  3...  CreateFile             C:\Users\user\Desktop\u.wnry                     SUCCESS
3:03:39.1003040 PM  ed01ebf...  3...  QueryAttributeTagFile  C:\Users\user\Desktop\u.wnry                     SUCCESS
3:03:39.1003273 PM  ed01ebf...  3...  CloseFile              C:\Users\user\Desktop\u.wnry                     SUCCESS
3:03:39.1006210 PM  ed01ebf...  3...  CreateFile             C:\Users\user\Desktop\u.wnry                     SUCCESS
3:03:39.1006622 PM  ed01ebf...  3...  QueryStandardInfor...  C:\Users\user\Desktop\u.wnry                     SUCCESS
3:03:39.1006789 PM  ed01ebf...  3...  QueryBasicInformati... C:\Users\user\Desktop\u.wnry                     SUCCESS
3:03:39.1007154 PM  ed01ebf...  3...  QueryStreamInforma...  C:\Users\user\Desktop\u.wnry                     SUCCESS
3:03:39.1007475 PM  ed01ebf...  3...  QueryBasicInformati... C:\Users\user\Desktop\u.wnry                     SUCCESS
3:03:39.1008647 PM  ed01ebf...  3...  QueryEaInformation...  C:\Users\user\Desktop\u.wnry                     SUCCESS
3:03:39.1010056 PM  ed01ebf...  3...  CreateFile             C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1017102 PM  ed01ebf...  3...  CreateFile             C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1017432 PM  ed01ebf...  3...  QueryBasicInformati... C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1017614 PM  ed01ebf...  3...  CloseFile              C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1018318 PM  ed01ebf...  3...  QueryNameInformati...  C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1018691 PM  ed01ebf...  3...  QueryNameInformati...  C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1020246 PM  ed01ebf...  3...  QueryNormalizedNa...   C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1021620 PM  ed01ebf...  3...  CloseFile              C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1029462 PM  ed01ebf...  3...  CreateFile             C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1029817 PM  ed01ebf...  3...  QueryBasicInformati... C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1029979 PM  ed01ebf...  3...  CloseFile              C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1032072 PM  ed01ebf...  3...  CreateFile             C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1033231 PM  ed01ebf...  3...  QueryAttributeInform...C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
3:03:39.1033548 PM  ed01ebf...  3...  QueryBasicInformati... C:\Users\user\Desktop\@WanaDecryptor@.exe        SUCCESS
```

Figure 47 Process monitor

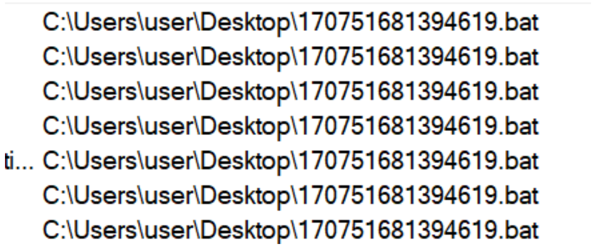
Figure 47 shows Sample One creating "@WannaDecryptor@.exe" file in the desktop directory.



```
3940 RegOpenKey    HKLM\SOFTWARE\Policies\Microsoft\Windows\System
3940 ReadFile      C:\Users\user\Desktop\u.wnry
3940 WriteFile     C:\Users\user\Desktop\@WanaDecryptor@.exe
3940 ReadFile      C:\Users\user\Desktop\u.wnry
3940 WriteFile     C:\Users\user\Desktop\@WanaDecryptor@.exe
```

Figure 48 "u.wnry" reading

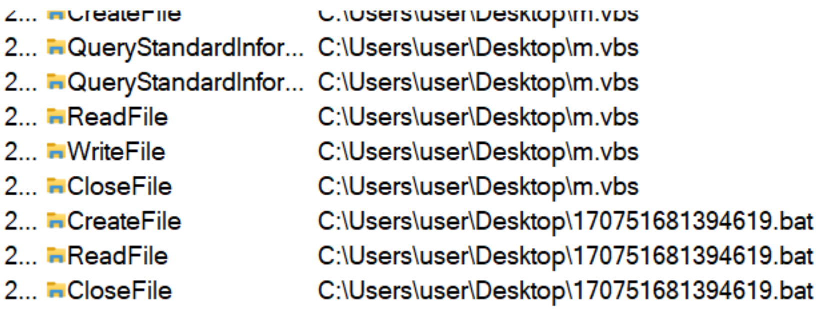
Figure 48 shows Sample one reading information from "u.wnry" and writing it to "@WannaDecryptor@.exe".



```
    C:\Users\user\Desktop\170751681394619.bat
    C:\Users\user\Desktop\170751681394619.bat
    C:\Users\user\Desktop\170751681394619.bat
    C:\Users\user\Desktop\170751681394619.bat
ti... C:\Users\user\Desktop\170751681394619.bat
    C:\Users\user\Desktop\170751681394619.bat
    C:\Users\user\Desktop\170751681394619.bat
```

Figure 49 ".bat" script

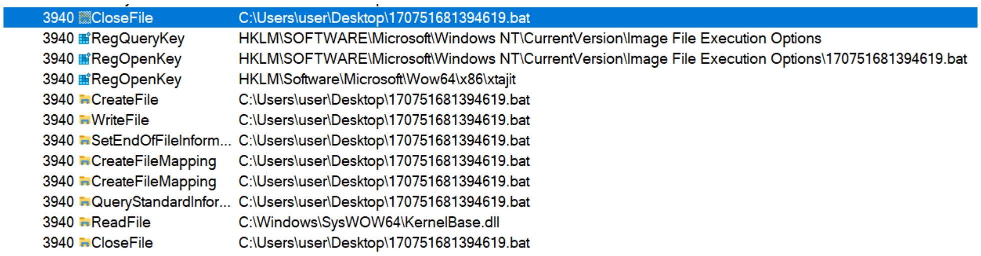
Figure 49 shows Sample One creating a ".bat" script in the desktop directory.



```
2... CreateFile              C:\Users\user\Desktop\m.vbs
2... QueryStandardInfor...   C:\Users\user\Desktop\m.vbs
2... QueryStandardInfor...   C:\Users\user\Desktop\m.vbs
2... ReadFile                C:\Users\user\Desktop\m.vbs
2... WriteFile               C:\Users\user\Desktop\m.vbs
2... CloseFile               C:\Users\user\Desktop\m.vbs
2... CreateFile              C:\Users\user\Desktop\170751681394619.bat
2... ReadFile                C:\Users\user\Desktop\170751681394619.bat
2... CloseFile               C:\Users\user\Desktop\170751681394619.bat
```

Figure 50 "m.vbs" script

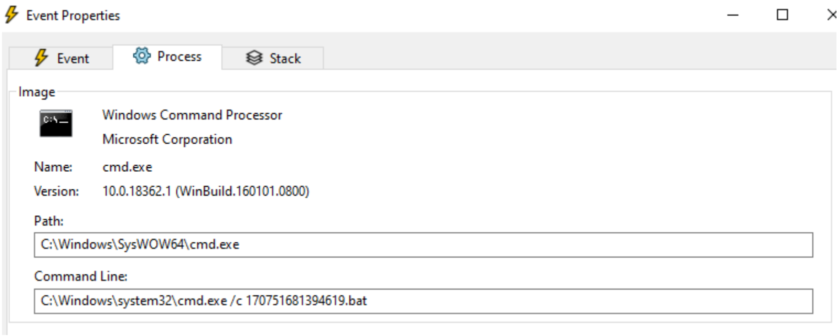
Figure 50 shows Sample One creating the "m.vbs" script.



```
3940 CloseFile               C:\Users\user\Desktop\170751681394619.bat
3940 RegQueryKey             HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
3940 RegOpenKey              HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\170751681394619.bat
3940 RegOpenKey              HKLM\Software\Microsoft\Wow64\x86\xtajit
3940 CreateFile              C:\Users\user\Desktop\170751681394619.bat
3940 WriteFile               C:\Users\user\Desktop\170751681394619.bat
3940 SetEndOfFileInform...   C:\Users\user\Desktop\170751681394619.bat
3940 CreateFileMapping       C:\Users\user\Desktop\170751681394619.bat
3940 CreateFileMapping       C:\Users\user\Desktop\170751681394619.bat
3940 QueryStandardInfor...   C:\Users\user\Desktop\170751681394619.bat
3940 ReadFile                C:\Windows\SysWOW64\KernelBase.dll
3940 CloseFile               C:\Users\user\Desktop\170751681394619.bat
```

Figure 51 Registry edit

Figure 51 shows the ".bat" file being given permissions by adding the value to the Registry.



Event Properties

Image

Windows Command Processor
Microsoft Corporation

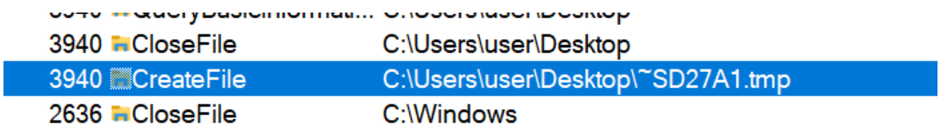
Name: cmd.exe
Version: 10.0.18362.1 (WinBuild.160101.0800)

Path:
```
C:\Windows\SysWOW64\cmd.exe
```

Command Line:
```
C:\Windows\system32\cmd.exe /c 170751681394619.bat
```

Figure 52 cmd.exe ".bat" execution

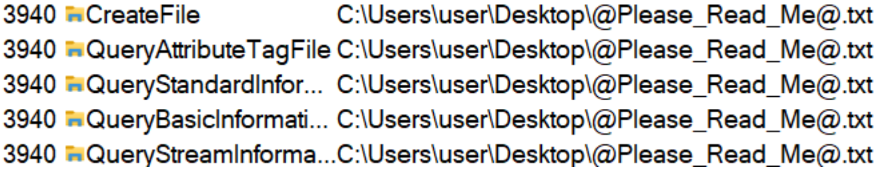
Figure 52 shows Sample One executing the ".bat" script with the "/c" option which ensures that the Command Prompt window closes automatically after the ".bat" file has finished executing.



```
3940 QueryBasicInformati... C:\Users\user\Desktop
3940 CloseFile              C:\Users\user\Desktop
3940 CreateFile             C:\Users\user\Desktop\~SD27A1.tmp
2636 CloseFile              C:\Windows
```

Figure 53 "~SD27A1.tmp"

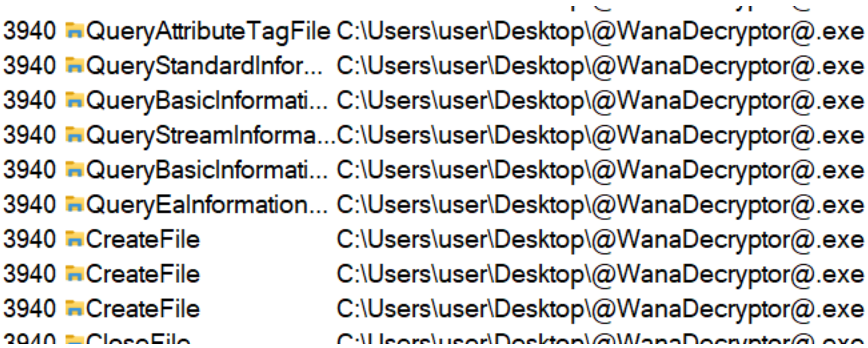
Figure 53 shows Sample One creates a temporary file on the desktop.



```
3940 CreateFile             C:\Users\user\Desktop\@Please_Read_Me@.txt
3940 QueryAttributeTagFile C:\Users\user\Desktop\@Please_Read_Me@.txt
3940 QueryStandardInfor...  C:\Users\user\Desktop\@Please_Read_Me@.txt
3940 QueryBasicInformati... C:\Users\user\Desktop\@Please_Read_Me@.txt
3940 QueryStreamInforma...C:\Users\user\Desktop\@Please_Read_Me@.txt
```

Figure 54 "@Please_Read_me@.txt"

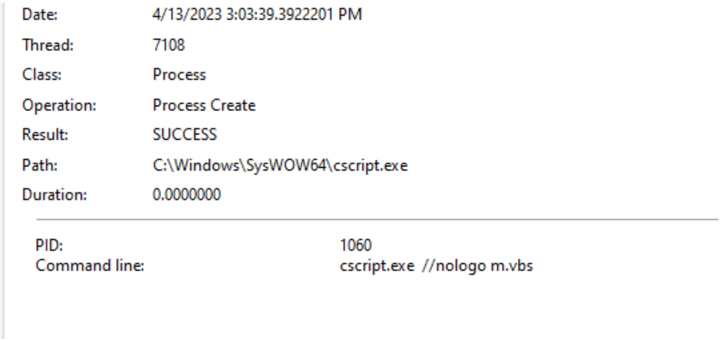
Figure 54 shows Sample One then creates the ransom note "@Please_Read_Me@.txt".



```
3940 QueryAttributeTagFile C:\Users\user\Desktop\@WanaDecryptor@.exe
3940 QueryStandardInfor...  C:\Users\user\Desktop\@WanaDecryptor@.exe
3940 QueryBasicInformati... C:\Users\user\Desktop\@WanaDecryptor@.exe
3940 QueryStreamInforma...C:\Users\user\Desktop\@WanaDecryptor@.exe
3940 QueryBasicInformati... C:\Users\user\Desktop\@WanaDecryptor@.exe
3940 QueryEaInformation...  C:\Users\user\Desktop\@WanaDecryptor@.exe
3940 CreateFile             C:\Users\user\Desktop\@WanaDecryptor@.exe
3940 CreateFile             C:\Users\user\Desktop\@WanaDecryptor@.exe
3940 CreateFile             C:\Users\user\Desktop\@WanaDecryptor@.exe
3940 CloseFile              C:\Users\user\Desktop\@WanaDecryptor@.exe
```

Figure 55 "@WannaDecryptor@.exe"

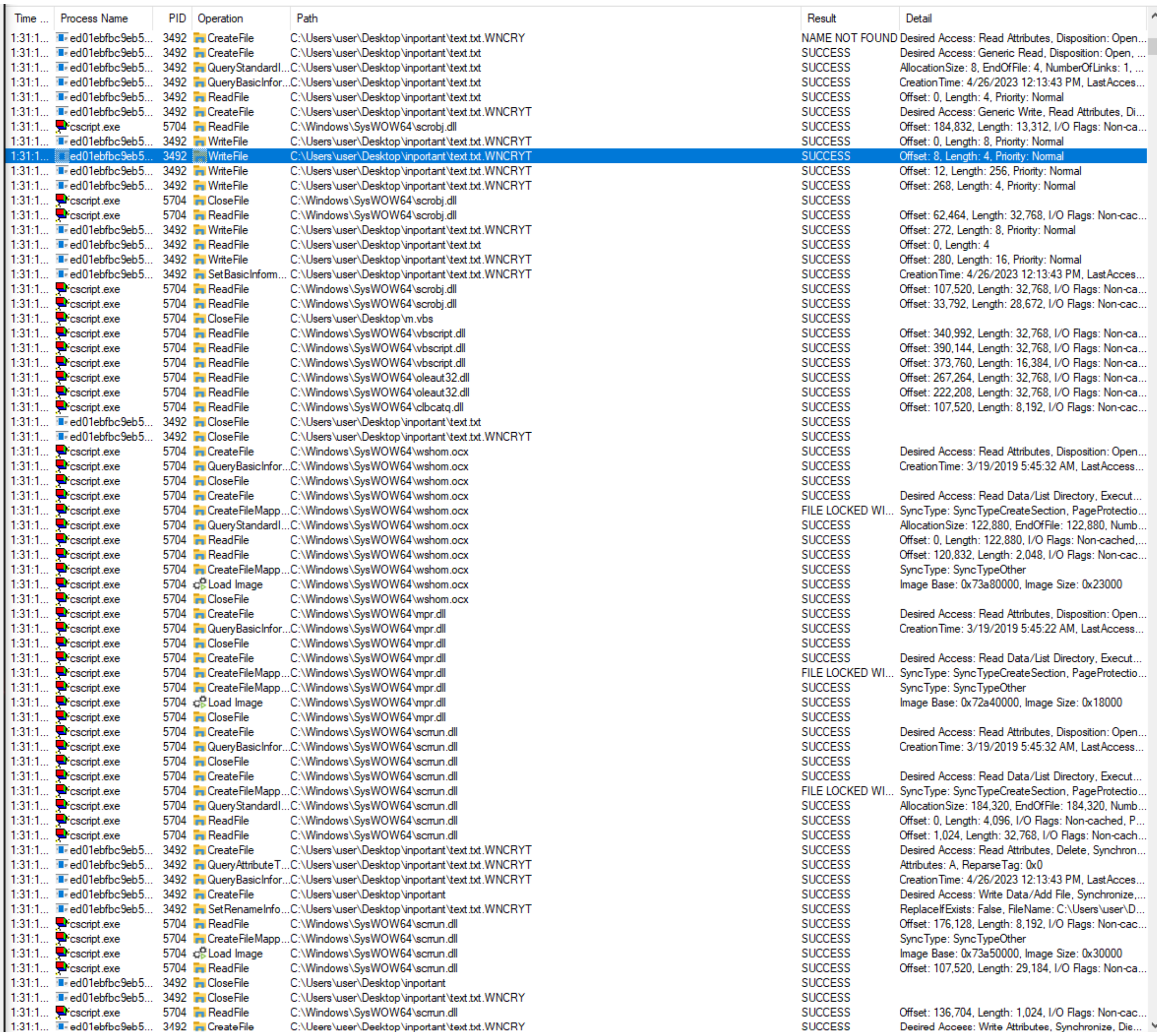
Figure 55 shows Sample One finally creates the"@WannaDecryptor@.exe" on the desktop.



```
Date:           4/13/2023 3:03:39.3922201 PM
Thread:         7108
Class:          Process
Operation:      Process Create
Result:         SUCCESS
Path:           C:\Windows\SysWOW64\cscript.exe
Duration:       0.0000000

  PID:                                  1060
  Command line:                         cscript.exe  //nologo m.vbs
```

Figure 56 cscript.exe

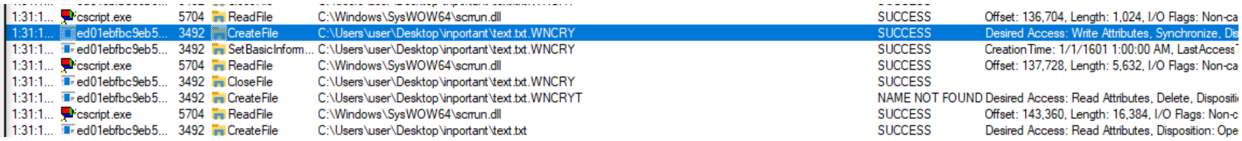
Figure 56 shows Sample One running the “m.vbs” script the “//nologo” option is run to prevent the user from being alerted.



Time ...	Process Name	PID	Operation	Path	Result	Detail
1:31:1...	ed01ebfbc9eb5...	3492	CreateFile	C:\Users\user\Desktop\inportant\text.txt.WNCRY	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open...
1:31:1...	ed01ebfbc9eb5...	3492	CreateFile	C:\Users\user\Desktop\inportant\text.txt	SUCCESS	Desired Access: Generic Read, Disposition: Open, ...
1:31:1...	ed01ebfbc9eb5...	3492	QueryStandardI...	C:\Users\user\Desktop\inportant\text.txt	SUCCESS	AllocationSize: 8, EndOfFile: 4, NumberOfLinks: 1, ...
1:31:1...	ed01ebfbc9eb5...	3492	QueryBasicInfor...	C:\Users\user\Desktop\inportant\text.txt	SUCCESS	CreationTime: 4/26/2023 12:13:43 PM, LastAcces...
1:31:1...	ed01ebfbc9eb5...	3492	ReadFile	C:\Users\user\Desktop\inportant\text.txt	SUCCESS	Offset: 0, Length: 4, Priority: Normal
1:31:1...	ed01ebfbc9eb5...	3492	CreateFile	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	Desired Access: Generic Write, Read Attributes, Di...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrobj.dll	SUCCESS	Offset: 184,832, Length: 13,312, I/O Flags: Non-ca...
1:31:1...	ed01ebfbc9eb5...	3492	WriteFile	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	Offset: 0, Length: 8, Priority: Normal
1:31:1...	ed01ebfbc9eb5...	3492	WriteFile	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	Offset: 8, Length: 4, Priority: Normal
1:31:1...	ed01ebfbc9eb5...	3492	WriteFile	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	Offset: 12, Length: 256, Priority: Normal
1:31:1...	ed01ebfbc9eb5...	3492	WriteFile	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	Offset: 268, Length: 4, Priority: Normal
1:31:1...	cscript.exe	5704	CloseFile	C:\Windows\SysWOW64\scrobj.dll	SUCCESS	
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrobj.dll	SUCCESS	Offset: 62,464, Length: 32,768, I/O Flags: Non-cac...
1:31:1...	ed01ebfbc9eb5...	3492	WriteFile	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	Offset: 272, Length: 8, Priority: Normal
1:31:1...	ed01ebfbc9eb5...	3492	ReadFile	C:\Users\user\Desktop\inportant\text.txt	SUCCESS	Offset: 0, Length: 4
1:31:1...	ed01ebfbc9eb5...	3492	WriteFile	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	Offset: 280, Length: 16, Priority: Normal
1:31:1...	ed01ebfbc9eb5...	3492	SetBasicInform...	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	CreationTime: 4/26/2023 12:13:43 PM, LastAcces...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrobj.dll	SUCCESS	Offset: 107,520, Length: 32,768, I/O Flags: Non-ca...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrobj.dll	SUCCESS	Offset: 33,792, Length: 28,672, I/O Flags: Non-cac...
1:31:1...	cscript.exe	5704	CloseFile	C:\Users\user\Desktop\m.vbs	SUCCESS	
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\vbscript.dll	SUCCESS	Offset: 340,992, Length: 32,768, I/O Flags: Non-ca...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\vbscript.dll	SUCCESS	Offset: 390,144, Length: 32,768, I/O Flags: Non-ca...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\vbscript.dll	SUCCESS	Offset: 373,760, Length: 16,384, I/O Flags: Non-ca...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Offset: 267,264, Length: 32,768, I/O Flags: Non-ca...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Offset: 222,208, Length: 32,768, I/O Flags: Non-ca...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\clbcatq.dll	SUCCESS	Offset: 107,520, Length: 8,192, I/O Flags: Non-cac...
1:31:1...	ed01ebfbc9eb5...	3492	CloseFile	C:\Users\user\Desktop\inportant\text.txt	SUCCESS	
1:31:1...	ed01ebfbc9eb5...	3492	CloseFile	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	
1:31:1...	cscript.exe	5704	CreateFile	C:\Windows\SysWOW64\wshom.ocx	SUCCESS	Desired Access: Read Attributes, Disposition: Open...
1:31:1...	cscript.exe	5704	QueryBasicInfor...	C:\Windows\SysWOW64\wshom.ocx	SUCCESS	CreationTime: 3/19/2019 5:45:32 AM, LastAccess...
1:31:1...	cscript.exe	5704	CloseFile	C:\Windows\SysWOW64\wshom.ocx	SUCCESS	
1:31:1...	cscript.exe	5704	CreateFile	C:\Windows\SysWOW64\wshom.ocx	SUCCESS	Desired Access: Read Data/List Directory, Execut...
1:31:1...	cscript.exe	5704	CreateFileMapp...	C:\Windows\SysWOW64\wshom.ocx	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtectio...
1:31:1...	cscript.exe	5704	QueryStandardI...	C:\Windows\SysWOW64\wshom.ocx	SUCCESS	AllocationSize: 122,880, EndOfFile: 122,880, Numb...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\wshom.ocx	SUCCESS	Offset: 0, Length: 122,880, I/O Flags: Non-cached,...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\wshom.ocx	SUCCESS	Offset: 120,832, Length: 2,048, I/O Flags: Non-cac...
1:31:1...	cscript.exe	5704	CreateFileMapp...	C:\Windows\SysWOW64\wshom.ocx	SUCCESS	SyncType: SyncTypeOther
1:31:1...	cscript.exe	5704	Load Image	C:\Windows\SysWOW64\wshom.ocx	SUCCESS	Image Base: 0x73a80000, Image Size: 0x23000
1:31:1...	cscript.exe	5704	CloseFile	C:\Windows\SysWOW64\wshom.ocx	SUCCESS	
1:31:1...	cscript.exe	5704	CreateFile	C:\Windows\SysWOW64\mpr.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open...
1:31:1...	cscript.exe	5704	QueryBasicInfor...	C:\Windows\SysWOW64\mpr.dll	SUCCESS	CreationTime: 3/19/2019 5:45:22 AM, LastAccess...
1:31:1...	cscript.exe	5704	CloseFile	C:\Windows\SysWOW64\mpr.dll	SUCCESS	
1:31:1...	cscript.exe	5704	CreateFile	C:\Windows\SysWOW64\mpr.dll	SUCCESS	Desired Access: Read Data/List Directory, Execut...
1:31:1...	cscript.exe	5704	CreateFileMapp...	C:\Windows\SysWOW64\mpr.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtectio...
1:31:1...	cscript.exe	5704	CreateFileMapp...	C:\Windows\SysWOW64\mpr.dll	SUCCESS	SyncType: SyncTypeOther
1:31:1...	cscript.exe	5704	Load Image	C:\Windows\SysWOW64\mpr.dll	SUCCESS	Image Base: 0x72a40000, Image Size: 0x18000
1:31:1...	cscript.exe	5704	CloseFile	C:\Windows\SysWOW64\mpr.dll	SUCCESS	
1:31:1...	cscript.exe	5704	CreateFile	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open...
1:31:1...	cscript.exe	5704	QueryBasicInfor...	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	CreationTime: 3/19/2019 5:45:32 AM, LastAccess...
1:31:1...	cscript.exe	5704	CloseFile	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	
1:31:1...	cscript.exe	5704	CreateFile	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	Desired Access: Read Data/List Directory, Execut...
1:31:1...	cscript.exe	5704	CreateFileMapp...	C:\Windows\SysWOW64\scrrun.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtectio...
1:31:1...	cscript.exe	5704	QueryStandardI...	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	AllocationSize: 184,320, EndOfFile: 184,320, Numb...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	Offset: 0, Length: 4,096, I/O Flags: Non-cached, P...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	Offset: 1,024, Length: 32,768, I/O Flags: Non-cach...
1:31:1...	ed01ebfbc9eb5...	3492	CreateFile	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	Desired Access: Read Attributes, Delete, Synchron...
1:31:1...	ed01ebfbc9eb5...	3492	QueryAttributeT...	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	Attributes: A, ReparseTag: 0x0
1:31:1...	ed01ebfbc9eb5...	3492	QueryBasicInfor...	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	CreationTime: 4/26/2023 12:13:43 PM, LastAcces...
1:31:1...	ed01ebfbc9eb5...	3492	CreateFile	C:\Users\user\Desktop\inportant	SUCCESS	Desired Access: Write Data/Add File, Synchronize,...
1:31:1...	ed01ebfbc9eb5...	3492	SetRenameInfo...	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	SUCCESS	ReplaceIfExists: False, FileName: C:\Users\user\D...
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	Offset: 176,128, Length: 8,192, I/O Flags: Non-cac...
1:31:1...	cscript.exe	5704	CreateFileMapp...	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	SyncType: SyncTypeOther
1:31:1...	cscript.exe	5704	Load Image	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	Image Base: 0x73a50000, Image Size: 0x30000
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	Offset: 107,520, Length: 29,184, I/O Flags: Non-ca...
1:31:1...	ed01ebfbc9eb5...	3492	CloseFile	C:\Users\user\Desktop\inportant	SUCCESS	
1:31:1...	ed01ebfbc9eb5...	3492	CloseFile	C:\Users\user\Desktop\inportant\text.txt.WNCRY	SUCCESS	
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	Offset: 136,704, Length: 1,024, I/O Flags: Non-cac...
1:31:1...	ed01ebfbc9eb5...	3492	CreateFile	C:\Users\user\Desktop\inportant\text.txt.WNCRY	SUCCESS	Desired Access: Write Attributes, Synchronize, Dis...

Figure 57 “test .txt” encryption

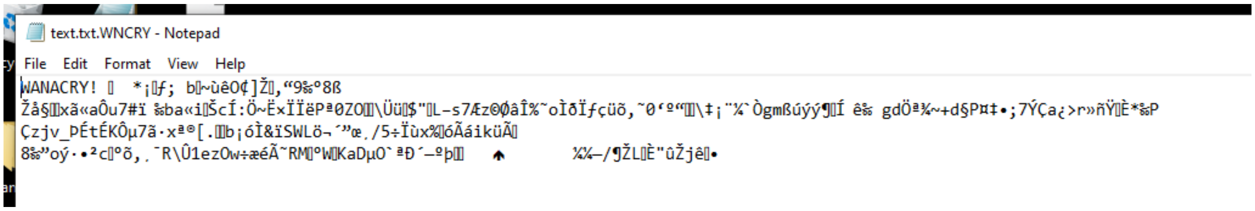
Figure 57 shows Sample One checking to see if the “test.txt.WNCRY” file doesn’t already exist. It proceeds to encrypt the file with the “.WNCRYT” extension and when complete copies the data to the “. WNCRY” extension.



1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	Offset: 136,704, Length: 1,024, I/O Flags: Non-ca
1:31:1...	ed01ebfbc9eb5...	3492	CreateFile	C:\Users\user\Desktop\inportant\text.txt.WNCRY	SUCCESS	Desired Access: Write Attributes, Synchronize, Dis
1:31:1...	ed01ebfbc9eb5...	3492	SetBasicInform...	C:\Users\user\Desktop\inportant\text.txt.WNCRY	SUCCESS	CreationTime: 1/1/1601 1:00:00 AM, LastAccess
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	Offset: 137,728, Length: 5,632, I/O Flags: Non-ca
1:31:1...	ed01ebfbc9eb5...	3492	CloseFile	C:\Users\user\Desktop\inportant\text.txt.WNCRY	SUCCESS	
1:31:1...	ed01ebfbc9eb5...	3492	CreateFile	C:\Users\user\Desktop\inportant\text.txt.WNCRYT	NAME NOT FOUND	Desired Access: Read Attributes, Delete, Disposit
1:31:1...	cscript.exe	5704	ReadFile	C:\Windows\SysWOW64\scrrun.dll	SUCCESS	Offset: 143,360, Length: 16,384, I/O Flags: Non-c
1:31:1...	ed01ebfbc9eb5...	3492	CreateFile	C:\Users\user\Desktop\inportant\text.txt	SUCCESS	Desired Access: Read Attributes, Disposition: Ope

Figure 58 ".WNCRYT" check

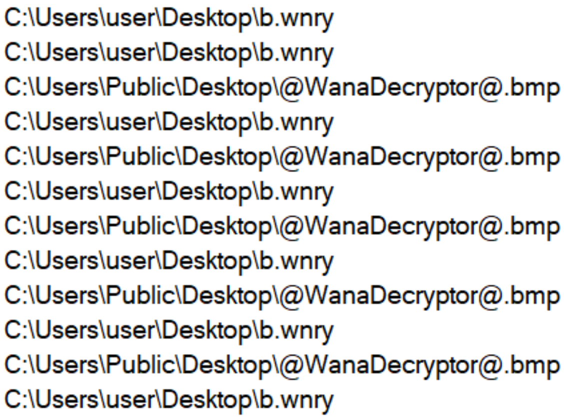
Figure 58 shows Sample one then closes the encrypted file and checks if the “.WNCRYT” extension is deleted.



```
WANACRY! 	 *¡f; b~ùêO¢]Ž,“9‰º8ß
Žå§xã«aÔu7#ï ‰ba«iŠcÍ:Ö~Ë×ÏÏëPª0ZO\Üü$"L-s7Æz©ØâÎ%˜oÌðÏƒçüõ,˜0‘º“\‡¡¨¼`ÒgmßúýýÍ ê‰ gdÖª¾~+d§P¤‡•;7ÝÇa¿>r»ñŸÈ*‰P
Çzjv_ÞÉtÉKÔµ7ã·xª®[.b¡óÌ&ïSWLö¬´”œ¸/5÷Ïùx%óÃáikü Ã
8‰”oý·•²cºõ,¸¯R\Û1ezOw÷æéÃ˜RMºWKaDµO`ªÐ´—ºþ          ¼¼—/¶ŽLÈ"ûŽjê•
```

Figure 59 “test.txt.WNCRY”

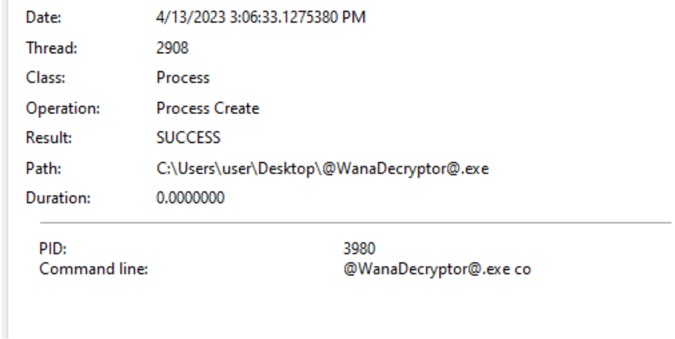
Figure 59 shows Sample One encrypted the contents of the file “test.txt”. Each file begins with “WANACRY!” and continues with the encrypted data.



```
C:\Users\user\Desktop\b.wnry
C:\Users\user\Desktop\b.wnry
C:\Users\Public\Desktop\@WanaDecryptor@.bmp
C:\Users\user\Desktop\b.wnry
C:\Users\Public\Desktop\@WanaDecryptor@.bmp
C:\Users\user\Desktop\b.wnry
C:\Users\Public\Desktop\@WanaDecryptor@.bmp
C:\Users\user\Desktop\b.wnry
C:\Users\Public\Desktop\@WanaDecryptor@.bmp
C:\Users\user\Desktop\b.wnry
C:\Users\Public\Desktop\@WanaDecryptor@.bmp
C:\Users\user\Desktop\b.wnry
```

Figure 60 “@WanaDecryptor@.bmp”

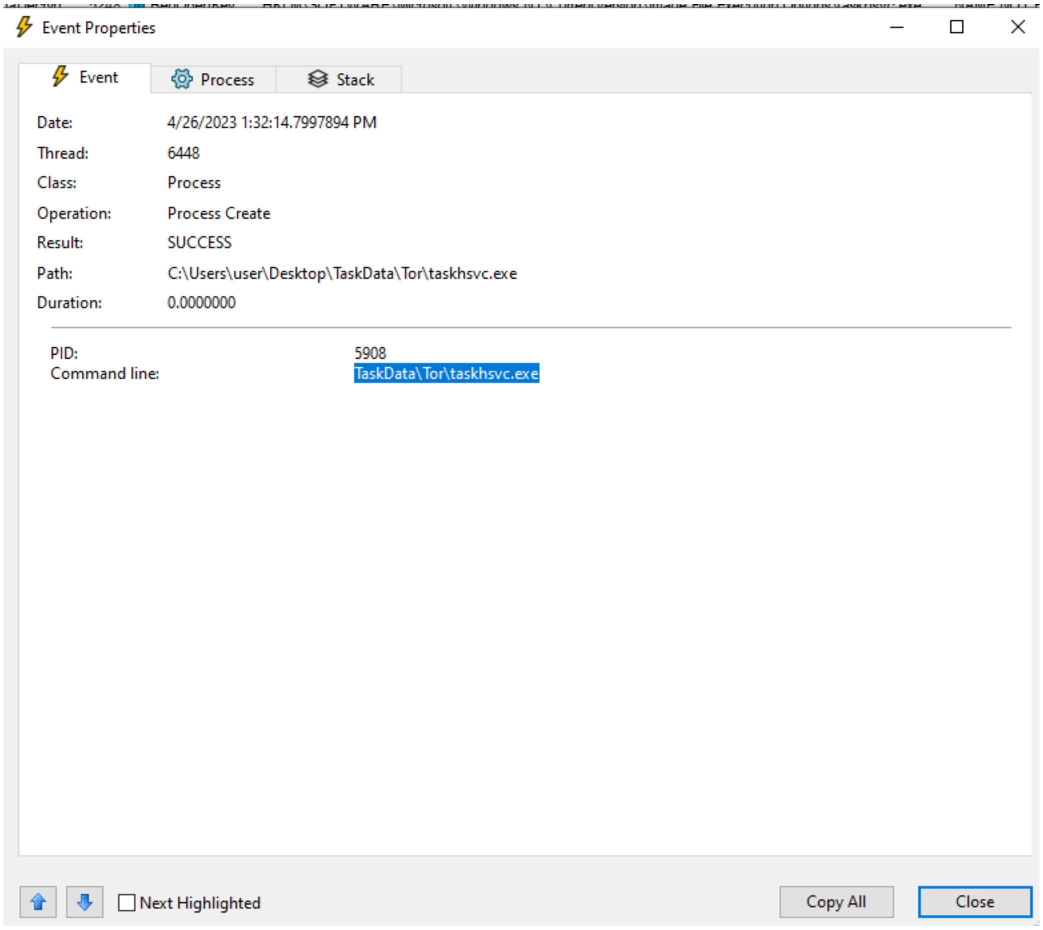
Figure 60 shows Sample One copying the background image to the “.bmp” file on the desktop.



Date:	4/13/2023 3:06:33.1275380 PM
Thread:	2908
Class:	Process
Operation:	Process Create
Result:	SUCCESS
Path:	C:\Users\user\Desktop\@WanaDecryptor@.exe
Duration:	0.0000000
PID:	3980
Command line:	@WanaDecryptor@.exe co

Figure 61 “@WanaDecryptor@.exe co”

Figure 61 shows Sample One being executed with the “co” switch.

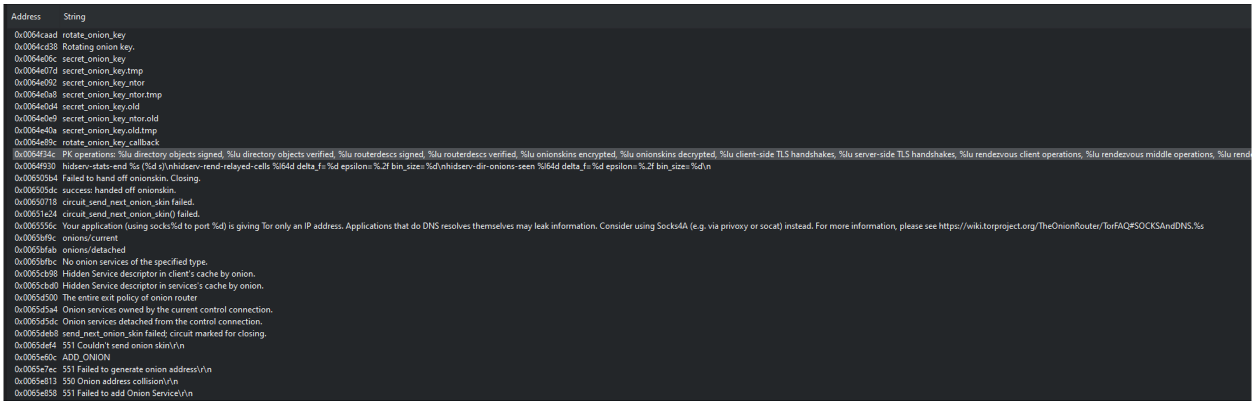


Date: 4/26/2023 1:32:14.7997894 PM
Thread: 6448
Class: Process
Operation: Process Create
Result: SUCCESS
Path: C:\Users\user\Desktop\TaskData\Tor\taskhsvc.exe
Duration: 0.0000000

PID: 5908
Command line: TaskData\Tor\taskhsvc.exe

Figure 62 "tasksvc.exe"

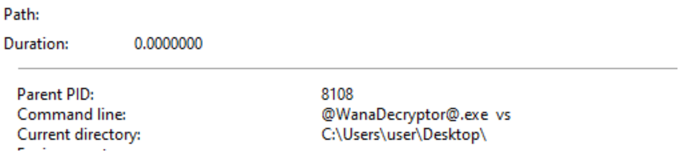
Figure 62 shows Sample One executing the "tasksvc.exe" file after the "co" switch was ran.



```
Address     String
0x0064caad  rotate_onion_key
0x0064cd38  Rotating onion key.
0x0064e06c  secret_onion_key
0x0064e07d  secret_onion_key.tmp
0x0064e092  secret_onion_key_ntor
0x0064e0a8  secret_onion_key_ntor.tmp
0x0064e0d4  secret_onion_key.old
0x0064e0e9  secret_onion_key_ntor.old
0x0064e40a  secret_onion_key.old.tmp
0x0064e89c  rotate_onion_key_callback
0x0064f34c  PK operations: %lu directory objects signed, %lu directory objects verified, %lu routerdescs signed, %lu routerdescs verified, %lu onionskins encrypted, %lu onionskins decrypted, %lu client-side TLS handshakes, %lu server-side TLS handshakes, %lu rendezvous client operations, %lu rendezvous middle operations, %lu rende
0x0064f930  hidserv-stats-end %s (%d s)\nhidserv-rend-relayed-cells %l64d delta_f=%d epsilon=%.2f bin_size=%d\nhidserv-dir-onions-seen %l64d delta_f=%d epsilon=%.2f bin_size=%d\n
0x006505b4  Failed to hand off onionskin. Closing.
0x006505dc  success: handed off onionskin.
0x00650718  circuit_send_next_onion_skin failed.
0x00651e24  circuit_send_next_onion_skin() failed.
0x0065556c  Your application (using socks%d to port %d) is giving Tor only an IP address. Applications that do DNS resolves themselves may leak information. Consider using Socks4A (e.g. via privoxy or socat) instead. For more information, please see https://wiki.torproject.org/TheOnionRouter/TorFAQ#SOCKSAndDNS.%s
0x0065bf9c  onions/current
0x0065bfab  onions/detached
0x0065bfbc  No onion services of the specified type.
0x0065cb98  Hidden Service descriptor in client's cache by onion.
0x0065cbd0  Hidden Service descriptor in services's cache by onion.
0x0065d500  The entire exit policy of onion router
0x0065d5a4  Onion services owned by the current control connection.
0x0065d5dc  Onion services detached from the control connection.
0x0065deb8  send_next_onion_skin failed; circuit marked for closing.
0x0065def4  551 Couldn't send onion skin\r\n
0x0065e60c  ADD_ONION
0x0065e7ec  551 Failed to generate onion address\r\n
0x0065e813  550 Onion address collision\r\n
0x0065e858  551 Failed to add Onion Service\r\n
```

Figure 63 Cutter Strings analysis

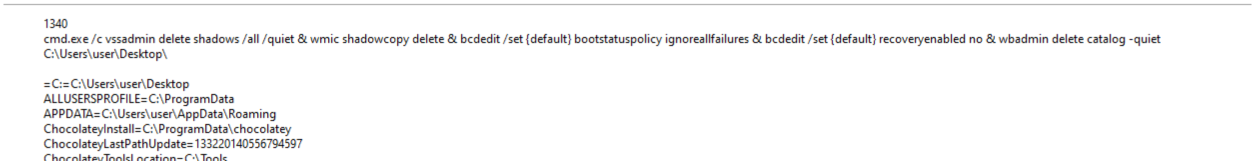
Figure 63 shows "tasksvc.exe" makes use of the onion network by using functions and phrases such as "rotate_onion_key" and "secrect_onion_key". Due to the VM not having any access to the internet process monitor does not see any connections. Sample One is likely attempting to make a connection to the C2 component of the malware.



```
Path:
Duration:          0.0000000

  Parent PID:                        8108
  Command line:                      @WanaDecryptor@.exe  vs
  Current directory:                 C:\Users\user\Desktop\
```

Figure 64 “@WanaDecryptor@.exe vs”

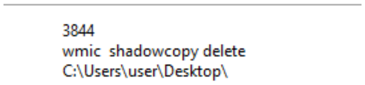
Figure 64 shows Sample One executed the “@WanaDecryptor@.exe” with the “vs” switch.



```
1340
cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
C:\Users\user\Desktop\

=C:=C:\Users\user\Desktop
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\user\AppData\Roaming
ChocolateyInstall=C:\ProgramData\chocolatey
ChocolateyLastPathUpdate=133220140556794597
ChocolateyToolsLocation=C:\Tools
```

Figure 65 “delete shadow files”

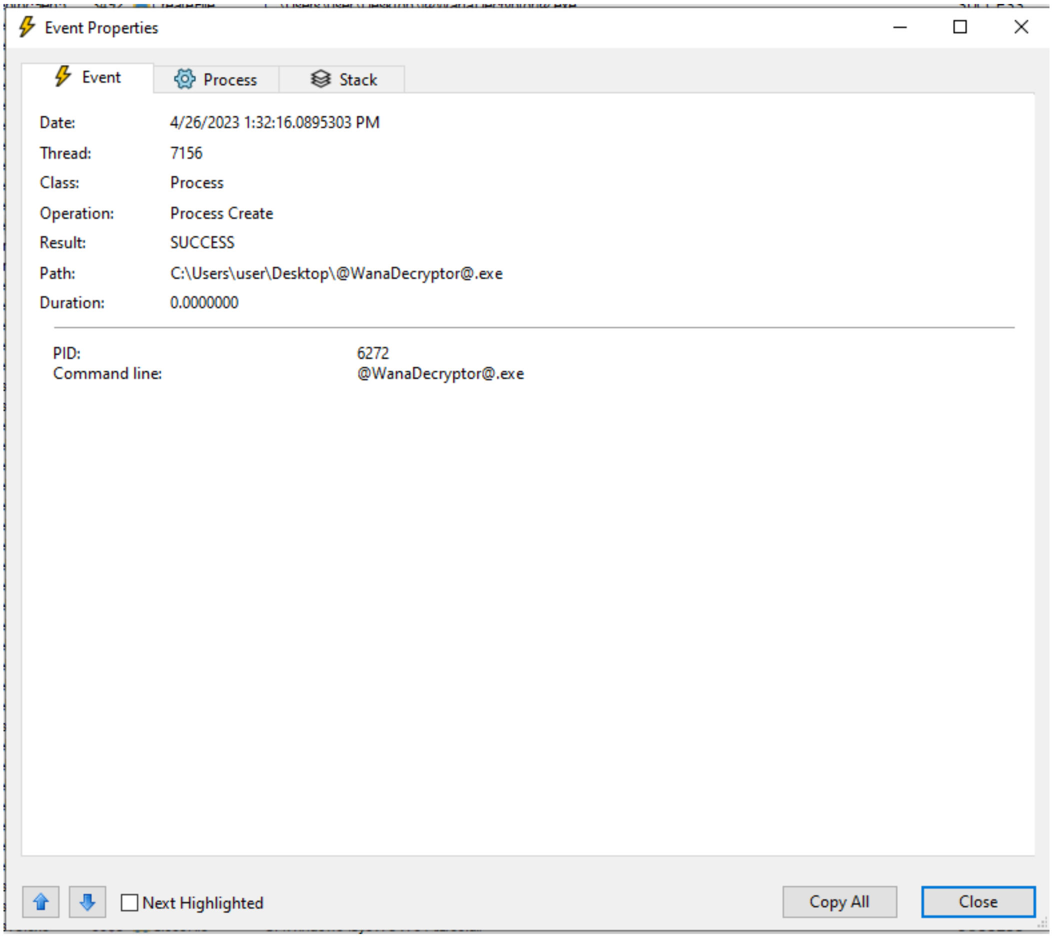
Figure 65 shows Sample One deleting all shadow files on the system this makes it impossible to recover from a local backup.



```
3844
wmic  shadowcopy delete
C:\Users\user\Desktop\
```

Figure 66 wmic

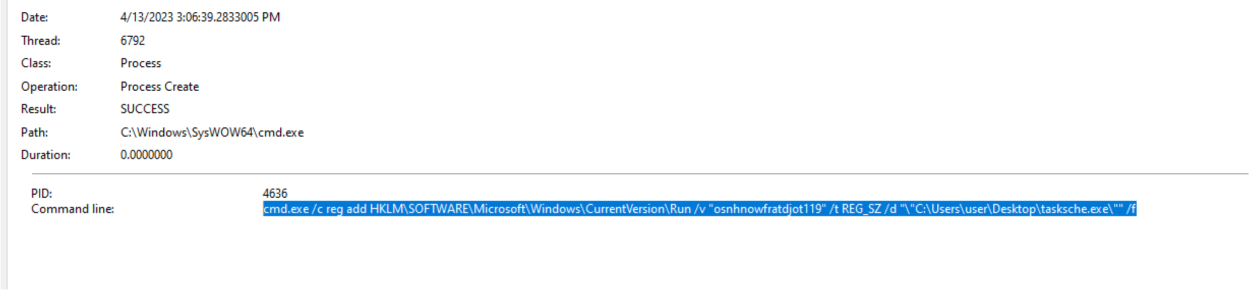
Figure 66 shows the “wmic” further deleting shadow files.



```
Date:        4/26/2023 1:32:16.0895303 PM
Thread:      7156
Class:       Process
Operation:   Process Create
Result:      SUCCESS
Path:        C:\Users\user\Desktop\@WanaDecryptor@.exe
Duration:    0.0000000

PID:                     6272
Command line:            @WanaDecryptor@.exe
```

Figure 67 "@WannaDecryptor@.exe"

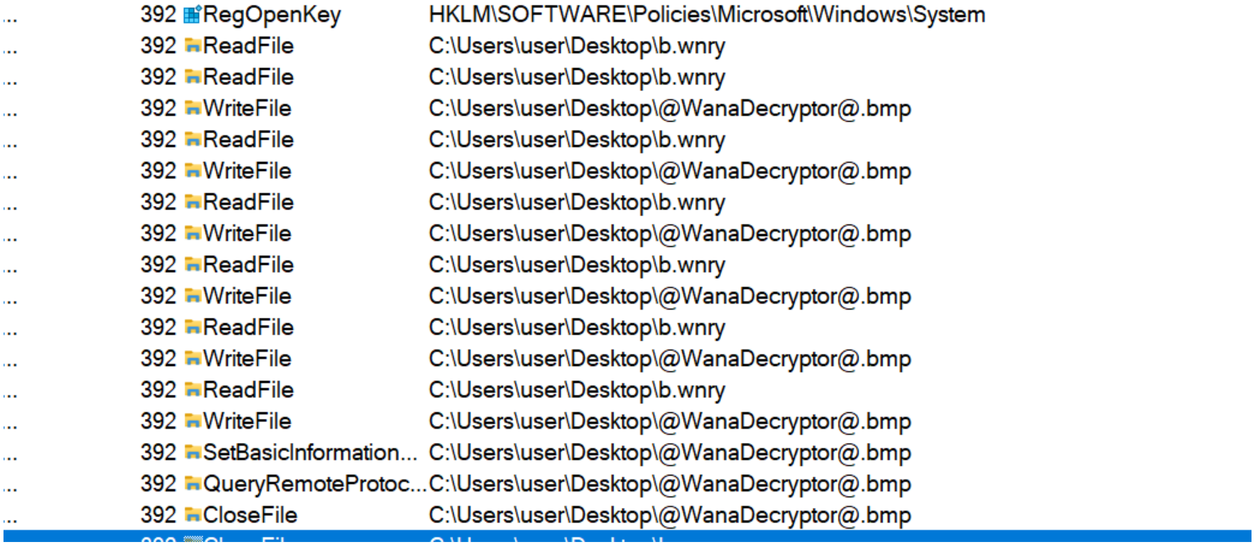
Figure 67 shows "@WannaDecryptor@.exe" is finally ran without any switches.



```
Date:        4/13/2023 3:06:39.2833005 PM
Thread:      6792
Class:       Process
Operation:   Process Create
Result:      SUCCESS
Path:        C:\Windows\SysWOW64\cmd.exe
Duration:    0.0000000

PID:                     4636
Command line:            cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "osnhnowfratdjot119" /t REG_SZ /d "\"C:\Users\user\Desktop\tasksche.exe\"" /f
```

Figure 68 Tasksche.exe

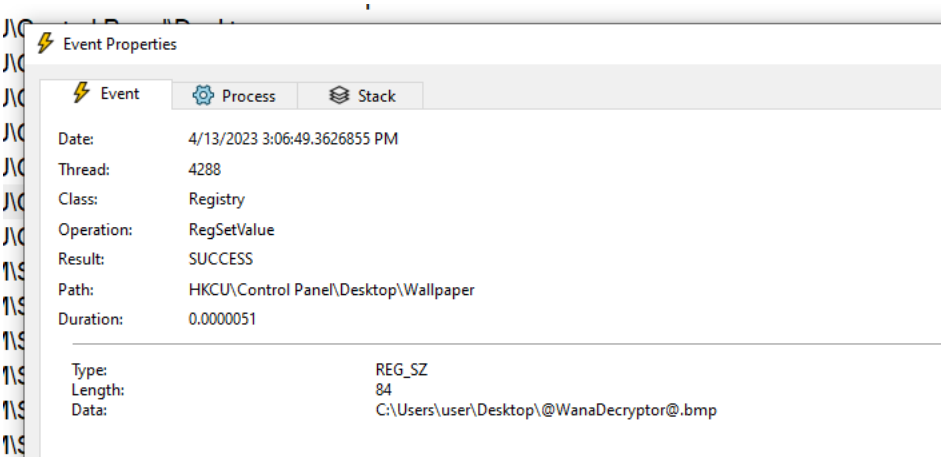
Figure 68 shows Sample One adding the program "C:\Users\user\Desktop\tasksche.exe" to the registry. This will be launched automatically when the computer starts up.



```
...   392 RegOpenKey              HKLM\SOFTWARE\Policies\Microsoft\Windows\System
...   392 ReadFile                C:\Users\user\Desktop\b.wnry
...   392 ReadFile                C:\Users\user\Desktop\b.wnry
...   392 WriteFile               C:\Users\user\Desktop\@WanaDecryptor@.bmp
...   392 ReadFile                C:\Users\user\Desktop\b.wnry
...   392 WriteFile               C:\Users\user\Desktop\@WanaDecryptor@.bmp
...   392 ReadFile                C:\Users\user\Desktop\b.wnry
...   392 WriteFile               C:\Users\user\Desktop\@WanaDecryptor@.bmp
...   392 ReadFile                C:\Users\user\Desktop\b.wnry
...   392 WriteFile               C:\Users\user\Desktop\@WanaDecryptor@.bmp
...   392 ReadFile                C:\Users\user\Desktop\b.wnry
...   392 WriteFile               C:\Users\user\Desktop\@WanaDecryptor@.bmp
...   392 ReadFile                C:\Users\user\Desktop\b.wnry
...   392 WriteFile               C:\Users\user\Desktop\@WanaDecryptor@.bmp
...   392 SetBasicInformation...  C:\Users\user\Desktop\@WanaDecryptor@.bmp
...   392 QueryRemoteProtoc...    C:\Users\user\Desktop\@WanaDecryptor@.bmp
...   392 CloseFile               C:\Users\user\Desktop\@WanaDecryptor@.bmp
```

Figure 69 "@WannaDecryptor@.bmp"

Figure 69 shows Sample One reading information from "b.wrny" and writing to "@WannaDecryptor@.bmp"

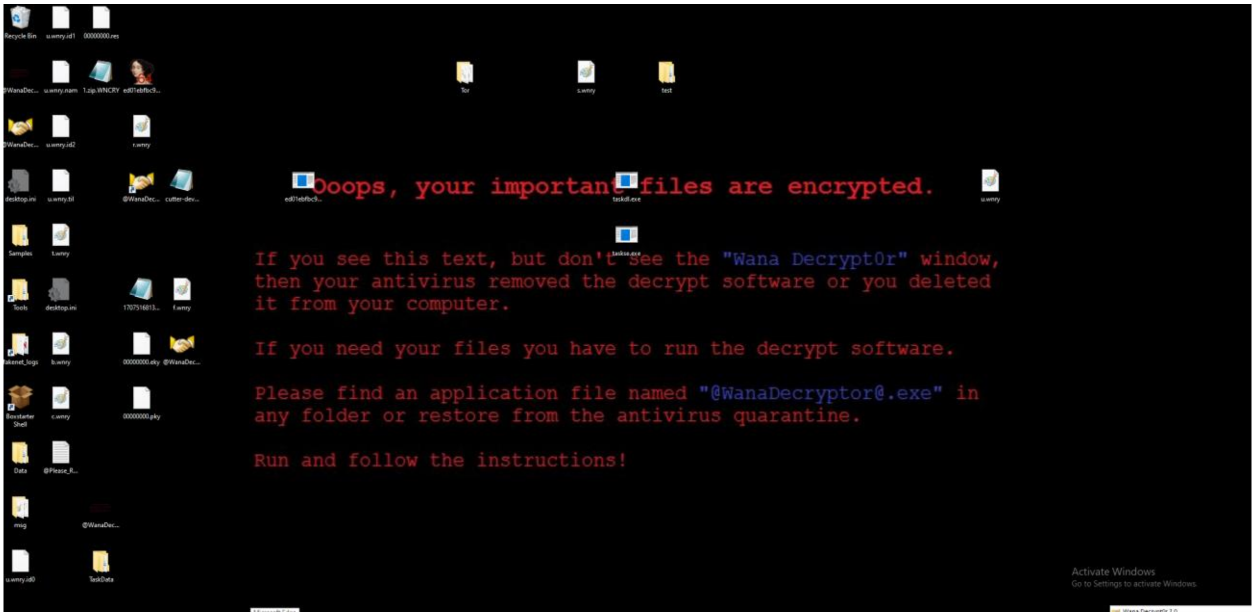


Date:	4/13/2023 3:06:49.3626855 PM
Thread:	4288
Class:	Registry
Operation:	RegSetValue
Result:	SUCCESS
Path:	HKCU\Control Panel\Desktop\Wallpaper
Duration:	0.0000051

Type:	REG_SZ
Length:	84
Data:	C:\Users\user\Desktop\@WanaDecryptor@.bmp

Figure 70 Wallpaper Registry change

Figure 70 shows Sample One changing the windows desktop background to the ransom bitmap.



Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.

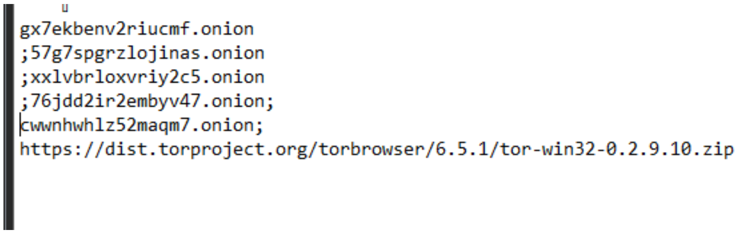
Run and follow the instructions!

Figure 71 Ransom image

Figure 71 shows the Windows desktop background now set to the ransom bitmap.

1.5.2 Network Traffic Analysis

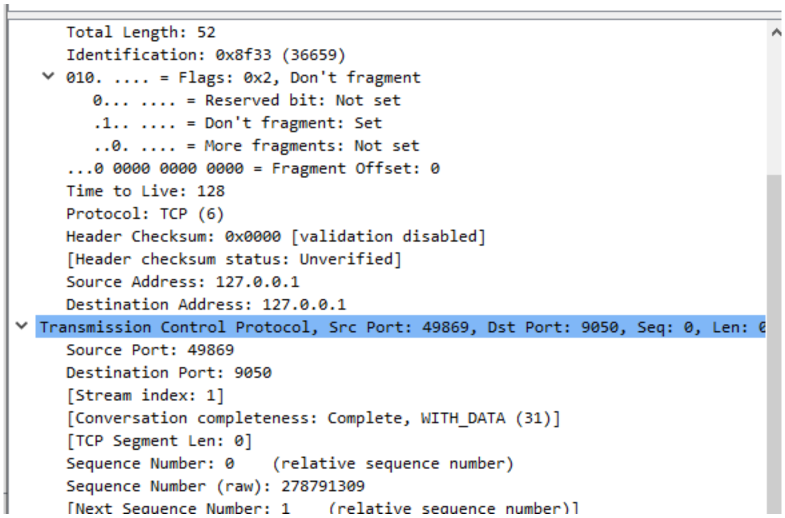
The VM was reverted to the previous snapshot, a host only network adapter was added and Sample One was then executed and the network traffic was then analysed to understand what connections the malware attempts to make.



```
gx7ekbenv2riucmf.onion
;57g7spgrzlojinas.onion
;xxlvbrloxvriy2c5.onion
;76jdd2ir2embyv47.onion;
cwwnhwhlz52maqm7.onion;
https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip
```

Figure 72 "c.wnry" contents

Figure 72 shows the contents of "c.wnry" containing ".onion" addresses. This is likely the hops Sample One makes.

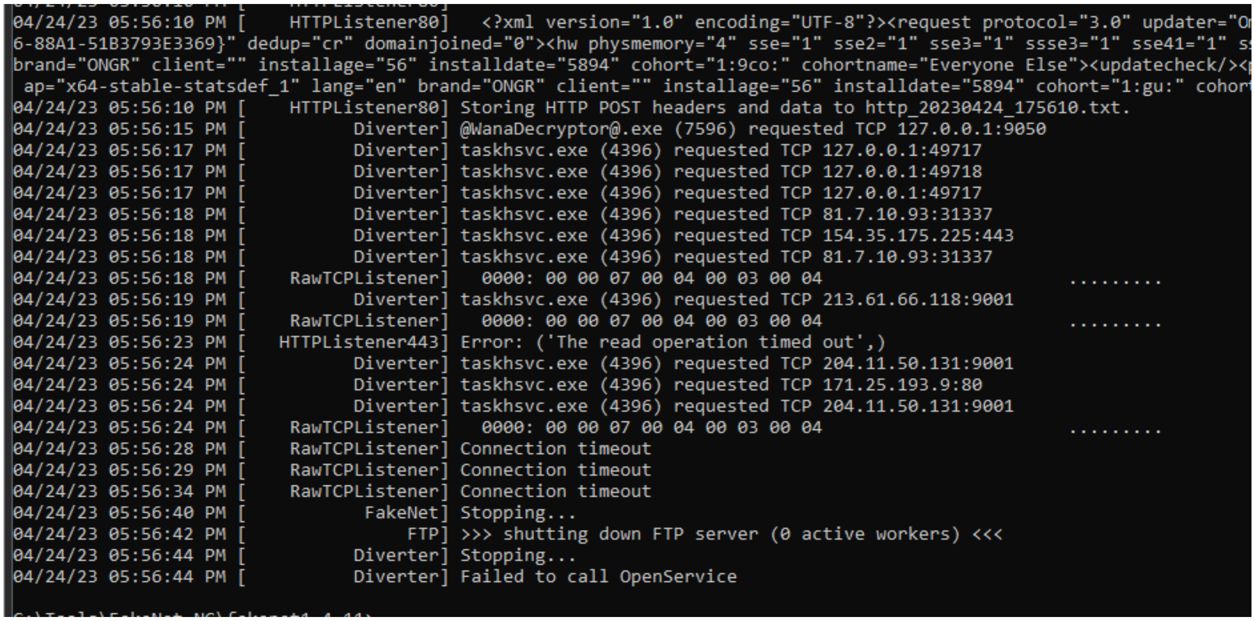


```
    Total Length: 52
    Identification: 0x8f33 (36659)
  ˅ 010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 127.0.0.1
    Destination Address: 127.0.0.1
˅ Transmission Control Protocol, Src Port: 49869, Dst Port: 9050, Seq: 0, Len: 0
    Source Port: 49869
    Destination Port: 9050
    [Stream index: 1]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 278791309
    [Next Sequence Number: 1    (relative sequence number)]
```

Figure 73 Wireshark capture

Figure 73 shows the "@WannaDecryptor@.exe" attempting to access port 9050 when the check payment button is clicked. This is a known port used by the Tor network.

Next Fakenet-NG was ran to analyse the network traffic .



```
04/24/23 05:56:10 PM [    HTTPListener80]   <?xml version="1.0" encoding="UTF-8"?><request protocol="3.0" updater="O
6-88A1-51B3793E3369}" dedup="cr" domainjoined="0"><hw physmemory="4" sse="1" sse2="1" sse3="1" ssse3="1" sse41="1" s
brand="ONGR" client="" installage="56" installdate="5894" cohort="1:9co:" cohortname="Everyone Else"><updatecheck/><
 ap="x64-stable-statsdef_1" lang="en" brand="ONGR" client="" installage="56" installdate="5894" cohort="1:gu:" cohor
04/24/23 05:56:10 PM [    HTTPListener80] Storing HTTP POST headers and data to http_20230424_175610.txt.
04/24/23 05:56:15 PM [          Diverter] @WanaDecryptor@.exe (7596) requested TCP 127.0.0.1:9050
04/24/23 05:56:17 PM [          Diverter] taskhsvc.exe (4396) requested TCP 127.0.0.1:49717
04/24/23 05:56:17 PM [          Diverter] taskhsvc.exe (4396) requested TCP 127.0.0.1:49718
04/24/23 05:56:17 PM [          Diverter] taskhsvc.exe (4396) requested TCP 127.0.0.1:49717
04/24/23 05:56:18 PM [          Diverter] taskhsvc.exe (4396) requested TCP 81.7.10.93:31337
04/24/23 05:56:18 PM [          Diverter] taskhsvc.exe (4396) requested TCP 154.35.175.225:443
04/24/23 05:56:18 PM [          Diverter] taskhsvc.exe (4396) requested TCP 81.7.10.93:31337
04/24/23 05:56:18 PM [    RawTCPListener]   0000: 00 00 07 00 04 00 03 00 04                        .........
04/24/23 05:56:19 PM [          Diverter] taskhsvc.exe (4396) requested TCP 213.61.66.118:9001
04/24/23 05:56:19 PM [    RawTCPListener]   0000: 00 00 07 00 04 00 03 00 04                        .........
04/24/23 05:56:23 PM [   HTTPListener443] Error: ('The read operation timed out',)
04/24/23 05:56:24 PM [          Diverter] taskhsvc.exe (4396) requested TCP 204.11.50.131:9001
04/24/23 05:56:24 PM [          Diverter] taskhsvc.exe (4396) requested TCP 171.25.193.9:80
04/24/23 05:56:24 PM [          Diverter] taskhsvc.exe (4396) requested TCP 204.11.50.131:9001
04/24/23 05:56:24 PM [    RawTCPListener]   0000: 00 00 07 00 04 00 03 00 04                        .........
04/24/23 05:56:28 PM [    RawTCPListener] Connection timeout
04/24/23 05:56:29 PM [    RawTCPListener] Connection timeout
04/24/23 05:56:34 PM [    RawTCPListener] Connection timeout
04/24/23 05:56:40 PM [           FakeNet] Stopping...
04/24/23 05:56:42 PM [               FTP] >>> shutting down FTP server (0 active workers) <<<
04/24/23 05:56:44 PM [          Diverter] Stopping...
04/24/23 05:56:44 PM [          Diverter] Failed to call OpenService
```

Figure 74 Fakenet

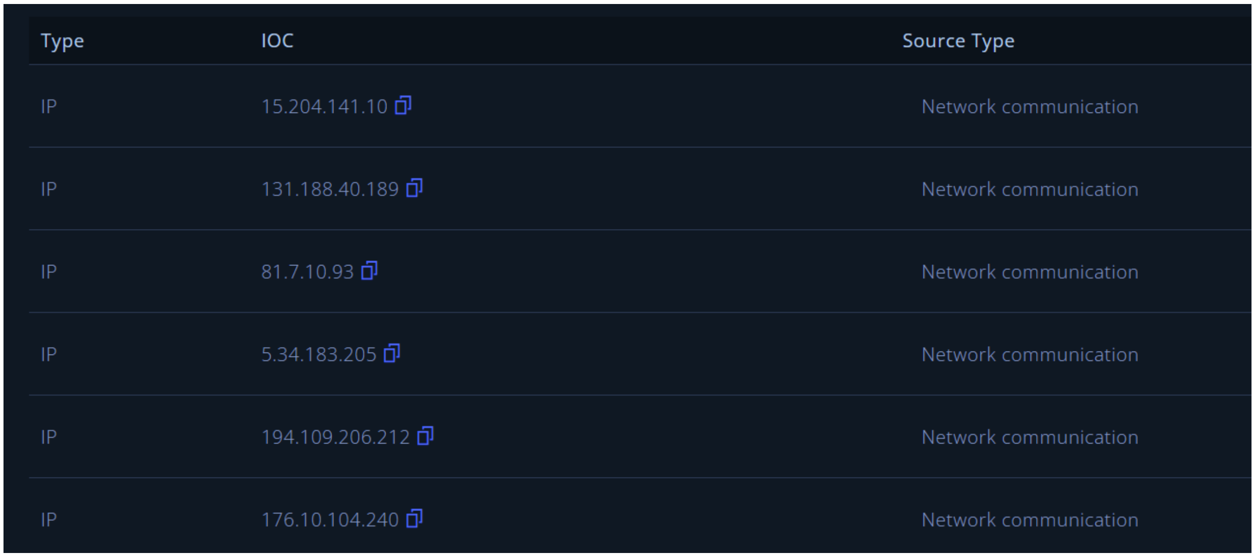
Figure 74 shows Sample One requesting the following IP addresses:

- 81.7.10.93 - Germany
- 154.35.175.225 - United States
- 213.61.66.118 - Germany
- 204.11.50.131 - Canada
- 171.25.193.9 - Sweden

The following ports are used by Sample One

- 9050 – Tor
- 443 -HTTPS
- 49717 – Unknown
- 49718-Unkonwn
- 31337 – spells Elite (used by viruses)
- 9001 – Tor
- 80 – HTTP

Finally Sample One was executed using InterAnalyze an online sandbox.



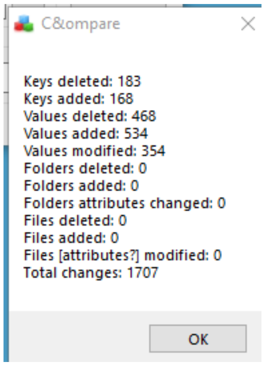
Type	IOC	Source Type
IP	15.204.141.10	Network communication
IP	131.188.40.189	Network communication
IP	81.7.10.93	Network communication
IP	5.34.183.205	Network communication
IP	194.109.206.212	Network communication
IP	176.10.104.240	Network communication

Figure 75 InterAnalyze IP IOC

Figure 75 shows the IP addresses that Sample One makes use of.

1.5.3 Registry Analysis

Registry analysis was undertook in order to analyse what Sample One changes in the Windows Registry. Initially Reg-Shot a tool for Comparing Registries was used.



```
Keys deleted: 183
Keys added: 168
Values deleted: 468
Values added: 534
Values modified: 354
Folders deleted: 0
Folders added: 0
Folders attributes changed: 0
Files deleted: 0
Files added: 0
Files [attributes?] modified: 0
Total changes: 1707
```

Figure 76 Reg-Shot

Figure 76 shows Sample One accessing 1707 registry values. Some of interest include:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "osnhnowfratdjot119" /t REG_SZ/d "\"C:\Users\user\Desktop\tasksche.exe\"" /f

This is added so the “tasksche.exe” is ran on startup

- HKLM\Software\WOW6432Node\WanaCrypt0r
- HKLM\SOFTWARE\WOW6432Node\WanaCrypt0r

This adds the WannaCryptor to the 32 bit emulator

- HKLM\SOFTWARE\WOW6432Node\WanaCrypt0r\wd

This adds the working directory to the WanaCrypt0r key

Finally InterAnalyze was ran to Identify what Registry Keys were written to by Sample One:

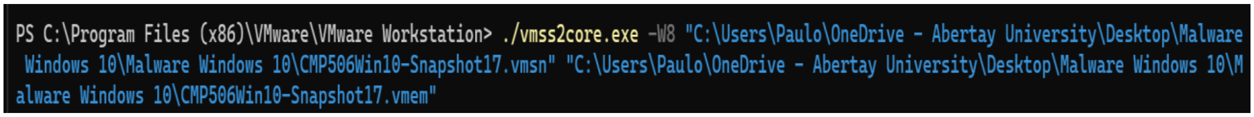
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces
- HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA#
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\zvxr\NccQngn\Ybpny\Grzc\@JnanQrpelcgbe@.rkr
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider
- HKEY_LOCAL_MACHINE\Software\WanaCrypt0r

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{ED50FC29-B964-48A9-AFB3-15EBB9B97F36} {ADD8BA80-002B-11D0-8F0F-00C04FD7D062} 0xFFFF
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\WanaCrypt0r\wd
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime

InterAnalyze identified a total of 15 registry keys were written by Sample One.

1.5.4 Memory Analysis

Next Memory analysis was undertaken against Sample One using “wm2core.exe” and “Volatility Workbench”. The Memory analysis was undertaken after the malware was executed.



```
PS C:\Program Files (x86)\VMware\VMware Workstation> ./vmss2core.exe -W8 "C:\Users\Paulo\OneDrive - Abertay University\Desktop\Malware
 Windows 10\Malware Windows 10\CMP506Win10-Snapshot17.vmsn" "C:\Users\Paulo\OneDrive - Abertay University\Desktop\Malware Windows 10\M
alware Windows 10\CMP506Win10-Snapshot17.vmem"
```

Figure 77 ./vmss2core.exe

Figure 77 shows the command run to build the “memory.dmp” a file which contains the RAM contents after the malware was executed. This will now be referred to as “The Memory Capture”.

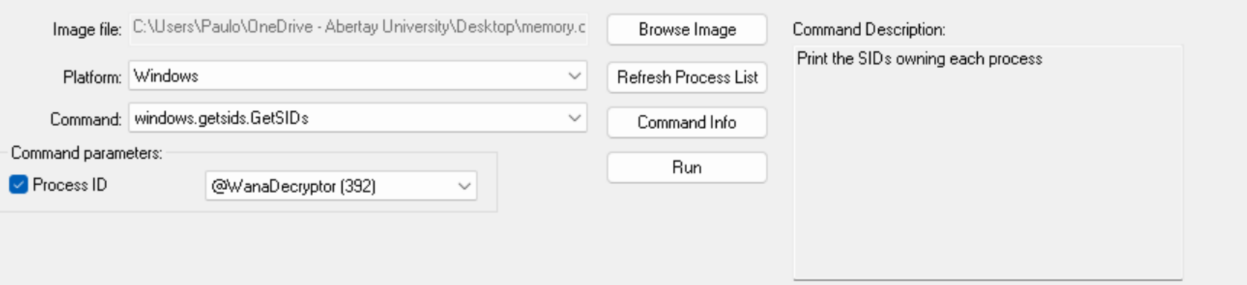


Image file: C:\Users\Paulo\OneDrive - Abertay University\Desktop\memory.c

Platform: Windows

Command: windows.getsids.GetSIDs

Command parameters:

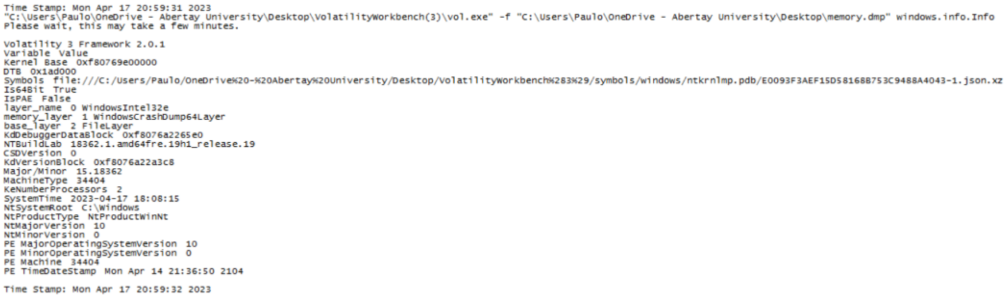
☑ Process ID @WanaDecryptor (392)

Command Description:

Print the SIDs owning each process

Figure 78 Volatility GUI

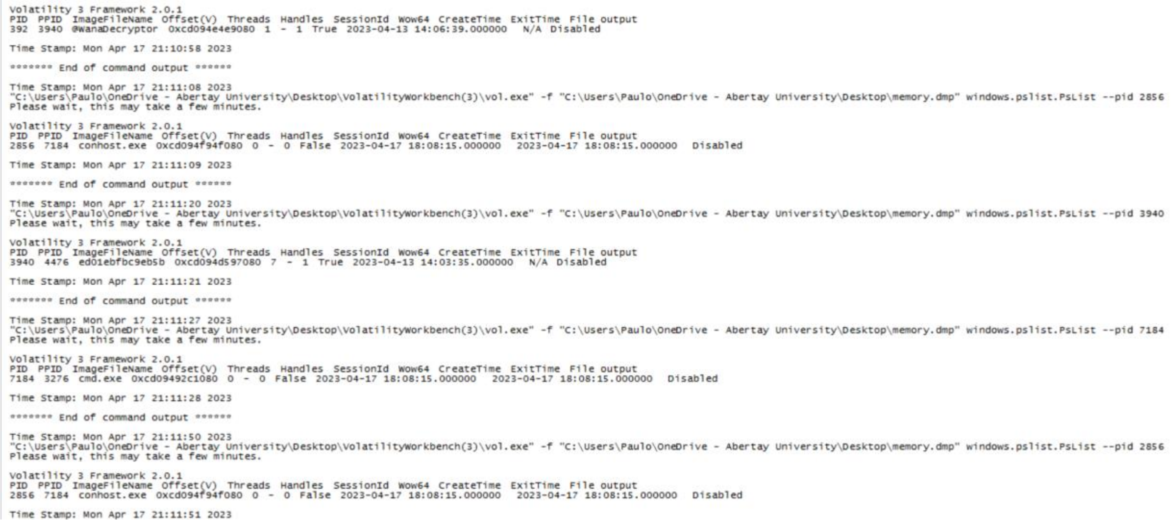
Figure 78 shows The Memory Capture in Volatility Workbench allowing for analysis.



```
Time Stamp: Mon Apr 17 20:59:31 2023
"C:\Users\Paulo\OneDrive - Abertay University\Desktop\VolatilityWorkbench(3)\vol.exe" -f "C:\Users\Paulo\OneDrive - Abertay University\Desktop\memory.dmp" windows.info.Info
Please wait, this may take a few minutes.

Volatility 3 Framework 2.0.1
Variable  Value
Kernel Base  0xf80769e00000
DTB  0x1ad000
Symbols  file:///C:/Users/Paulo/OneDrive%20-%20Abertay%20University/Desktop/VolatilityWorkbench%283%29/symbols/windows/ntkrnlmp.pdb/E0093F3AEF15D58168B753C9488A4043-1.json.xz
Is64Bit  True
IsPAE  False
layer_name  0 WindowsIntel32e
memory_layer  1 WindowsCrashDump64Layer
base_layer  2 FileLayer
KdDebuggerDataBlock  0xf8076a2265e0
NTBuildLab  18362.1.amd64fre.19h1_release.19
CSDVersion  0
KdVersionBlock  0xf8076a22a3c8
Major/Minor  15.18362
MachineType  34404
KeNumberProcessors  2
SystemTime  2023-04-17 18:08:15
NtSystemRoot  C:\Windows
NtProductType  NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine  34404
PE TimeDateStamp  Mon Apr 14 21:36:50 2104

Time Stamp: Mon Apr 17 20:59:32 2023
```

Figure 79 Volatility GUI basic info

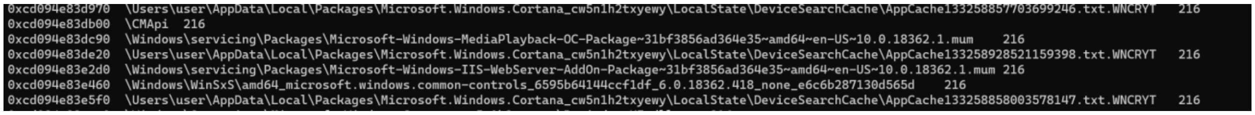
Figure 79 shows the basic information of The Memory Capture.



```
Volatility 3 Framework 2.0.1
PID  PPID  ImageFileName  Offset(V)  Threads  Handles  SessionId  Wow64  CreateTime  ExitTime  File output
392  3940  @WanaDecryptor  0xcd094e4e9080  1  -  1  True  2023-04-13 14:06:39.000000   N/A  Disabled

Time Stamp: Mon Apr 17 21:10:58 2023

******* End of command output ******

Time Stamp: Mon Apr 17 21:11:08 2023
"C:\Users\Paulo\OneDrive - Abertay University\Desktop\VolatilityWorkbench(3)\vol.exe" -f "C:\Users\Paulo\OneDrive - Abertay University\Desktop\memory.dmp" windows.pslist.PsList --pid 2856
Please wait, this may take a few minutes.

Volatility 3 Framework 2.0.1
PID  PPID  ImageFileName  Offset(V)  Threads  Handles  SessionId  Wow64  CreateTime  ExitTime  File output
2856  7184  conhost.exe  0xcd094f94f080  0  -  0  False  2023-04-17 18:08:15.000000   2023-04-17 18:08:15.000000   Disabled

Time Stamp: Mon Apr 17 21:11:09 2023

******* End of command output ******

Time Stamp: Mon Apr 17 21:11:20 2023
"C:\Users\Paulo\OneDrive - Abertay University\Desktop\VolatilityWorkbench(3)\vol.exe" -f "C:\Users\Paulo\OneDrive - Abertay University\Desktop\memory.dmp" windows.pslist.PsList --pid 3940
Please wait, this may take a few minutes.

Volatility 3 Framework 2.0.1
PID  PPID  ImageFileName  Offset(V)  Threads  Handles  SessionId  Wow64  CreateTime  ExitTime  File output
3940  4476  ed01ebfbc9eb5b  0xcd094d597080  7  -  1  True  2023-04-13 14:03:35.000000   N/A  Disabled

Time Stamp: Mon Apr 17 21:11:21 2023

******* End of command output ******

Time Stamp: Mon Apr 17 21:11:27 2023
"C:\Users\Paulo\OneDrive - Abertay University\Desktop\VolatilityWorkbench(3)\vol.exe" -f "C:\Users\Paulo\OneDrive - Abertay University\Desktop\memory.dmp" windows.pslist.PsList --pid 7184
Please wait, this may take a few minutes.

Volatility 3 Framework 2.0.1
PID  PPID  ImageFileName  Offset(V)  Threads  Handles  SessionId  Wow64  CreateTime  ExitTime  File output
7184  3276  cmd.exe  0xcd09492c1080  0  -  0  False  2023-04-17 18:08:15.000000   2023-04-17 18:08:15.000000   Disabled

Time Stamp: Mon Apr 17 21:11:28 2023

******* End of command output ******

Time Stamp: Mon Apr 17 21:11:50 2023
"C:\Users\Paulo\OneDrive - Abertay University\Desktop\VolatilityWorkbench(3)\vol.exe" -f "C:\Users\Paulo\OneDrive - Abertay University\Desktop\memory.dmp" windows.pslist.PsList --pid 2856
Please wait, this may take a few minutes.

Volatility 3 Framework 2.0.1
PID  PPID  ImageFileName  Offset(V)  Threads  Handles  SessionId  Wow64  CreateTime  ExitTime  File output
2856  7184  conhost.exe  0xcd094f94f080  0  -  0  False  2023-04-17 18:08:15.000000   2023-04-17 18:08:15.000000   Disabled

Time Stamp: Mon Apr 17 21:11:51 2023
```

Figure 80 Volatility PSlist

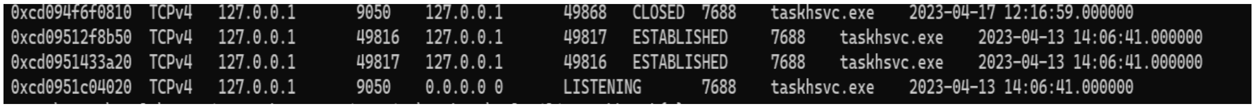
Figure 80 shows The Memory Capture's PSlist processes. The PSlist includes "conhost.exe", "cmd.exe" and "@WannaDecryptor@.exe" used by Sample One, a full scan can be found in Appendix B Volatility.



```
0xcd094e83d970  \Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258857703699246.txt.WNCRYT   216
0xcd094e83db00  \CMApi  216
0xcd094e83dc90  \Windows\servicing\Packages\Microsoft-Windows-MediaPlayback-OC-Package~31bf3856ad364e35~amd64~en-US~10.0.18362.1.mum    216
0xcd094e83de20  \Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258928521159398.txt.WNCRYT   216
0xcd094e83e2d0  \Windows\servicing\Packages\Microsoft-Windows-IIS-WebServer-AddOn-Package~31bf3856ad364e35~amd64~en-US~10.0.18362.1.mum 216
0xcd094e83e460  \Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.18362.418_none_e6c6b287130d565d    216
0xcd094e83e5f0  \Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258858003578147.txt.WNCRYT   216
```

Figure 81 Volatility Filescan

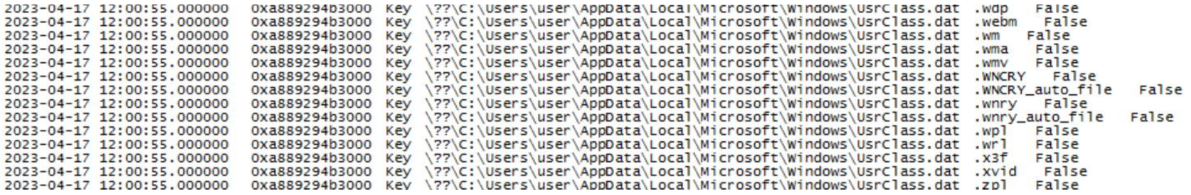
Figure 81 shows the Filescan plugin ran from the command line. It identifies the .WNCRYT extension used to encrypt files by Sample One.



```
0xcd094f6f0810  TCPv4   127.0.0.1       9050    127.0.0.1       49868  CLOSED  7688    taskhsvc.exe    2023-04-17 12:16:59.000000
0xcd09512f8b50  TCPv4   127.0.0.1       49816   127.0.0.1       49817  ESTABLISHED     7688    taskhsvc.exe    2023-04-13 14:06:41.000000
0xcd0951433a20  TCPv4   127.0.0.1       49817   127.0.0.1       49816  ESTABLISHED     7688    taskhsvc.exe    2023-04-13 14:06:41.000000
0xcd0951c04020  TCPv4   127.0.0.1       9050    0.0.0.0 0       LISTENING       7688    taskhsvc.exe    2023-04-13 14:06:41.000000
```

Figure 82 Volatility netscan

Figure 82 shows The Memory Capture ran with the "netscan" switch identifying "tasksvc.exe" listening for something on port 9050 a port used by the Tor network. The full Scan can be found in Appendix B Volatility.



```
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wdp   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .webm   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wm   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wma   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wmv   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .WNCRY   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .WNCRY_auto_file   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wnry   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wnry_auto_file   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wpl   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wrl   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .x3f   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .xvid   False
2023-04-17 12:00:55.000000   0xa889294b3000  Key  \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .zpl   False
```

Figure 83 Volatility Registry Keys

Figure 83 shows The Memory Capture Volatility identifying the ".wnry" extension used by the configuration files. The full Scan can be found in Appendix B Volatility.

2 DISCUSSION

2.1 GENERAL DISCUSSION

Sample One makes use of advanced malware techniques and an advanced understanding of The Microsoft Windows Operating System to cause maximum damage to the target. The malware is written as an 32bit executable as this is cross compatible with both x86 and x64 Windows operating systems. Furthermore, using generic operating system commands such as “cmd.exe” and “icals” enables Sample One to function across the majority of Microsoft Systems including Windows 10, XP and 7.

Sample One demands its ransom in Bitcoin and makes use of Onion routing to make it difficult to trace who is ultimately responsible for the attack. However due to the public ledger that Bitcoin uses and a handful of bitcoin exchanges e.g. places where the money can be withdrawn to real currency, the money can be easily traced if spent. The bitcoin wallet in question can be found at https://www.blockchain.com/explorer/addresses/btc/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 and currently has $9,911 in its account, however has received over $600,000 of payments (blockchain, nd). This highlights this malwares profitability and effectiveness.

Sample One furthers its effectiveness through displaying the ransom note in English, a widely spoken and understood language, as well as having the ransom note translated into many major languages spoken throughout the world. This increases the malwares readability to target a worldwide audience making it easy for people to understand the ransom request.

The malware makes use of AES and RSA encryption in order to encrypt the file contents and keys. The malware does not encrypt the “.dll”, “.exe”, ”.ink”, “.sys” or “.wnry” files and selected directories, this is in order to allow the end user to pay the ransom Sample One demands from the impacted system.

Moreover, Sample One utilises the “icals” command to alter file permissions on the computer. The command used was “./grant Everyone:F /T /C /Q”. This enables the program to bypass file permissions and have access all files. This allows access to other user accounts on the and encrypt their files also.

When encrypting the files Sample One initially checks to see if the file is already encrypted. During file encryption Sample One creates a temporary file following the form “FILENAME . FILE TYPE . WNCRYT“ e.g. “test.txt.wncryt”. Once encryption is complete the data from the “.WNCRYT ” file is then copied to a new file using the form “FILENAME . FILE TYPE . WNCRY“ e.g. “test.txt.wncry”. The “.WNCRYT” file is then deleted.

Another part of Sample One’s effectiveness is the encryption keys and obfuscation techniques Sample One utilised: (cyber-sectech.fandom.com, 2017)
“WannaCry encrypts files by loading a key from the 00000000.pky file. If the key does not exist, it will try to import and generate a public RSA-2048 key, which it will store in the 00000000.pky file. The corresponding private key that will be used to decrypt the victim's files is then generated and stored on the 00000000.eky file. This private key will then be stored to the 00000000.eky file and encrypted.”

Sample One hides its processes by using switches such as the "/c", "/Quiet" and "nologo", in order to not alert the user until the files are encrypted.

Sample One prior to encrypting files in each targeted directory creates two files "@Please_Read_Me@.txt" a message alerting that your files are encrypted and a shortcut to "@WannaDecryptor@.exe". This is the executable that displays the ransomware image and the countdown clock. This makes it clear that the computer has been compromised.

Sample One executes "@WannaDecryptor@.exe" three times. The first time the "@WannaDecryptor@.exe" is executed the "co" switch is used in an attempt to make a connection to the C2 component of the ransomware through the "tasksvc.exe" file. The second time the "@WannaDecryptor@.exe" is executed the "vs" switch is used to delete the shadow files on the system making it impossible to back up from the last save point. The final execution of the "@WannaDecryptor@.exe" no switches are used and this displays the ransomware image.

Sample One makes uses of AES (Advanced Encryption Standard) in order to encrypt files on the users system using a RSA-2048 key. This makes it highly unlikely to decrypt the data without paying the ransom, making this malware particularly effective.

2.2 The Indicators Of Compromise (IOC)

- File System IOC's
    - The .WNCRY extension of encrypted files.
    - "@Please_Read_Me@.txt" and "@WannaDecryptor@.exe" in every encrypted directory.
    - "b.wnry", "c.wnry", "t.wnry"
- The Registry keys IOC's
    - HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Run\: ""C:\Users\user\Desktop\tasksche.exe""
    - HKCU\Software\WanaCrypt0r
    - HKCU\Software\WanaCrypt0r\wd
- Network IOC's
    - gx7ekbenv2riucmf.onion
    - 57g7spgrzlojinas.onion
    - xxlvbrloxvriy2c5.onion
    - 76jdd2ir2embyv47.onion
    - cwwnhwhlz52maqm7.onion
    - 81.7.10.93
    - 154.35.175.225
    - 213.61.66.118
    - 204.11.50.131
    - 171.25.193.9
- Process names IOC's

    - "tasksche.exe"
    - "@WannaDecryptor@.exe"
    - "@WannaDecryptor@.exe.lnk"
- Command IOC's
    - cmd.exe /c start /b vssadmin.exe Delete Shadows /All /Quiet
    - wmic shadowcopy delete
    - icacls . /grant Everyone:F /T /C /Q
    - cscript nologo m.vbs
    - @WannaDecryptor@.exe vs
    - @WannaDecryptor@.exe co

2.3 Mitigation and Prevention

To mitigate against ransomware such as Sample One, certain procedures and software should be implemented.

One method to do this is to keep software up to date this guarantees that known vulnerabilities that Sample One and other malware exploits are "patched". Keeping systems up to date is the best way to keep devices secure. The specific patch that Microsoft released after WannaCry can be found here.

https://answers.microsoft.com/en-us/windows/forum/all/wanna-cry-ransomware-update-5212017-fix/5afdb045-8f36-4f55-a992-53398d21ed07

By backing up to an offsite or offline location, information can be restored from a specific backup point. If a business or individual had information backed up in software such as One Drive by Microsoft, or an offline backup, this attack would be but an inconvenience. All that would need to be done is a restore from the last save. However, an online backup is likely to be a key target of a threat actor. More information can be found here.

[Offline Backup]

https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

[Online Backup]

https://support.microsoft.com/en-gb/office/ransomware-detection-and-recovering-your-files-0d90ec50-6bfd-40f4-acc7-b8c12c73637f

Another tool which can prevent ransomware is antivirus software. Having an up to date anti-virus software makes it difficult for threat actors to exploit known vulnerabilities in software as they will likely be patched by the anti-virus software. Anti-virus software is also likely to have information regarding known ransomware and other viruses and is able to sandbox these threats. One of the most popular anti-virus suites is the already included Microsoft Defender. A ranking of all anti-virus suites and their effectiveness can be found here.

[Anti-Virus Ranking]

https://www.av-test.org/en/antivirus/home-windows/windows-10/february-2023/microsoft-defender-antivirus-consumer-4.18-231114/

A further mitigation technique is Intrusion Prevention (IPS) and/or Intrusion detection systems (IDS). An IDS system allows a network engineer to easily monitor and detect suspicious traffic across the network. An IPS improves this and will automatically detect and block suspicious traffic across the network. More information can be found here.

[IDS]

https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system

[IPS]

https://www.fortinet.com/resources/cyberglossary/what-is-an-ips

One strategy that a business can employ is employee awareness training, recent ransomware attacks have leveraged humans as the entry point through phishing emails, bad USB's, text's etc. This has enabled ransomware groups to bypass the need of an exploit to get onto a system. The NCSC has guides relating to this and other information to help businesses on how to educate their employees.

[NCSC]

https://www.ncsc.gov.uk/guidance/phishing

A final method to make it difficult for threat actors to deploy ransomware is network segmentation. By breaking a network up into VLAN's, Subnets and Services makes it difficult for the worm component of a ransomware like WannaCry to propagate through a network. Information on how to setup a modern network infrastructure can be found here.

[NCSC]

https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/network-architectures

2.4 Conclusion

In conclusion, Sample One is the Encryptor component of the WannaCry ransomware that caused severe damage to business and industries worldwide including the NHS from 2017 and can still be a threat today. By installing the provided Sample One onto a virtual machine it was analysed to identify it's type and characteristics. The sample makes use of standard windows functions from a 32 bit executable in order to maximise the damage it does across a variety of Windows Operating Systems. Through both static and dynamic analysis of Sample One the Indicators of Compromise (IOC) have been identified for this variant. Ultimately the best way to prevent this attack is to keep devices up to date and backed up. This ensures that ransomware like this is ineffective against targets as data can be recovered easily.

2.5 Future Work

In the future the possibility of identifying the keys stored in empty drive space or memory could be investigated, this would mean that no ransom would need to be paid. If the full sample of the WannaCry had been supplied including the worm and C2 component of the malware, this would have been analysed in order to understand better how it propagates across the network. Yara rules would also have been developed.

There are limitations of this analysis such as Sample One being an older variant of the WannaCry ransomware. Analysis of a more modern variant would be beneficial as it will likely have Tools Techniques and Procedures (TTP's) that bypass some of the patches allowing a better understanding of modern day risks.

REFERENCES

Tools for Malware Analysis

- [VMware] https://www.vmware.com/products/workstation-pro.html
- [Flare VM] https://github.com/mandiant/flare-vm
- [VirusTotal] https://www.virustotal.com/gui/home/upload
- [CFF Explorer] https://download.cnet.com/CFF-Explorer/3000-2383_4-10431156.html
- [Pe Studio] https://www.winitor.com/download
- [Cutter] https://cutter.re/
- [Sysinternals] https://learn.microsoft.com/en-us/sysinternals/downloads/procmon
- [MS Paint] https://apps.microsoft.com/store/detail/paint/9PCFS5B6T72H?hl=en-us&gl=us
- [010 Editor] https://www.sweetscape.com/download/010editor/download_010editor_win64.html
- [IDA] https://hex-rays.com/ida-free/
- [Regshot] https://regshot.en.softonic.com/?ex=DINS-635.2
- [Wireshark] https://www.wireshark.org/
- [vmss2core] https://flings.vmware.com/vmss2core
- [Volatility Workbench] https://www.osforensics.com/tools/volatility-workbench.html
- [InterAnalyze] https://www.intezer.com/intezer-analyze/
- [Fakenet] https://github.com/mandiant/flare-fakenet-ng/releases

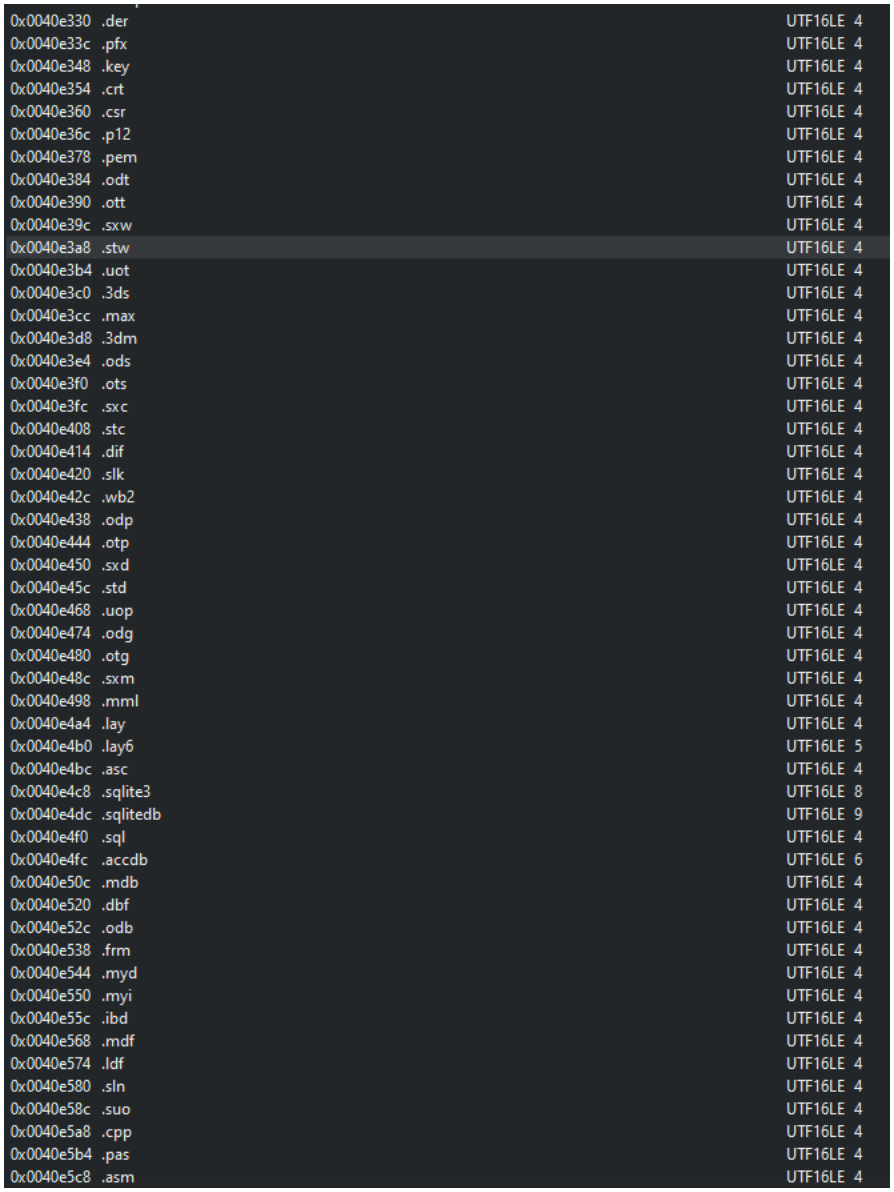
URL’s

- [Crowdstrike.com] [Written 28/02/2023] 12 Types of Malwares + Examples That You Should Know, https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/ [Accessed on 19/04/2023][Blog]
- [Safetydetectives.com][nd] Ransomware Facts, Trends & Statistics for 2023, https://www.safetydetectives.com/blog/ransomware-statistics/[Accessed on 28/02/2002][Blog]
- [Ditto.com] [Written 18/10/2018] WannaCry Attack Costs NHS over $100 million, https://www.datto.com/blog/ransomware-news-wannacry-attack-costs-nhs-over-100-million [Accessed on 19/04/2023][Blog]
- [Hypr.com][nd] What is the WannaCry Ransomware?, https://www.hypr.com/security-encyclopedia/wannacry [Accessed on 19/04/2023][Blog]
- [Microsoft.com][nd] Technical Documentation, https://learn.microsoft.com/en-us/docs/ [Accessed on 20/04/2023][Documentation].
- [blockchain.com][[nd] 13AM4-aEb94, https://www.blockchain.com/explorer/addresses/btc/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

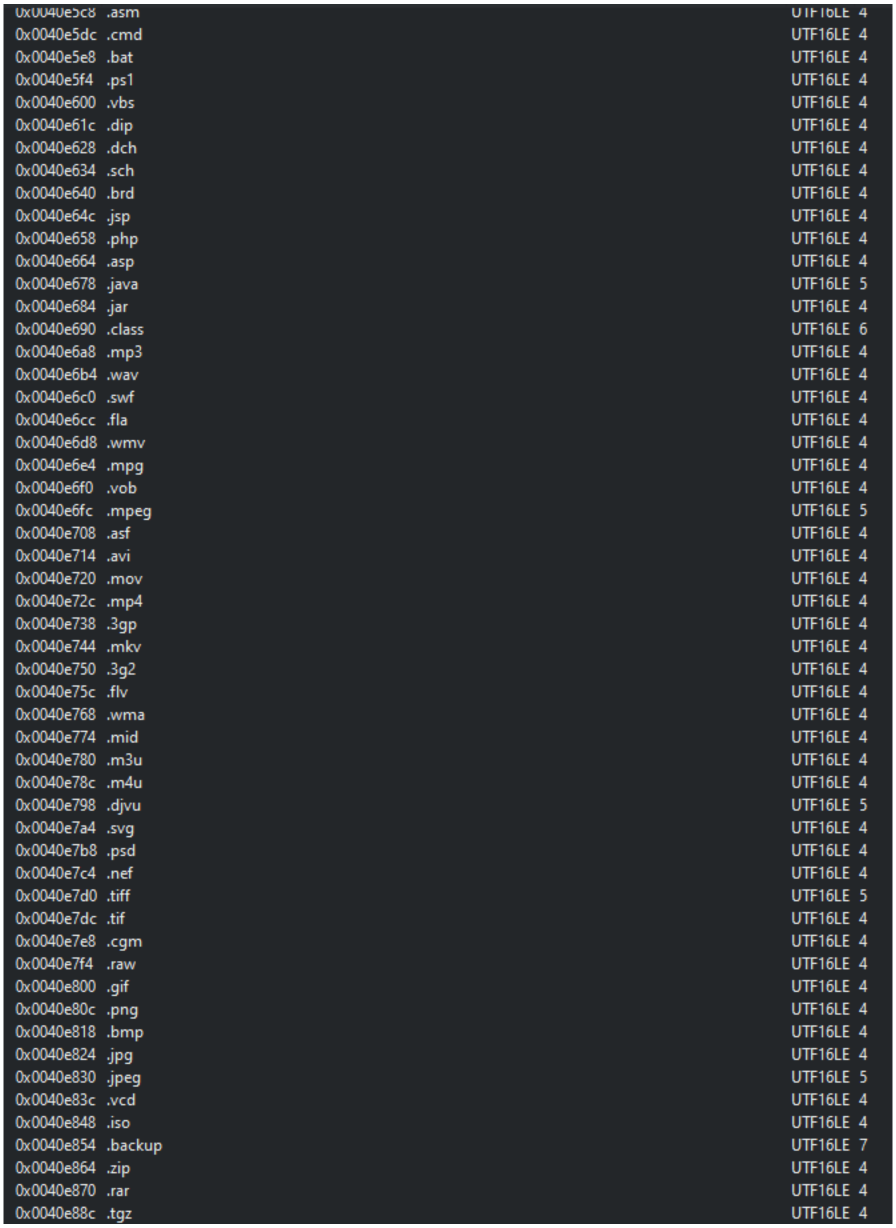
- [cyber-sectech.fandom.com][30 October 2017] WannaCry Attack, https://cyber-sectech.fandom.com/wiki/WannaCry_Attack#cite_note-:0-3 [Accessed on 27/04/2023]

APPENDICES

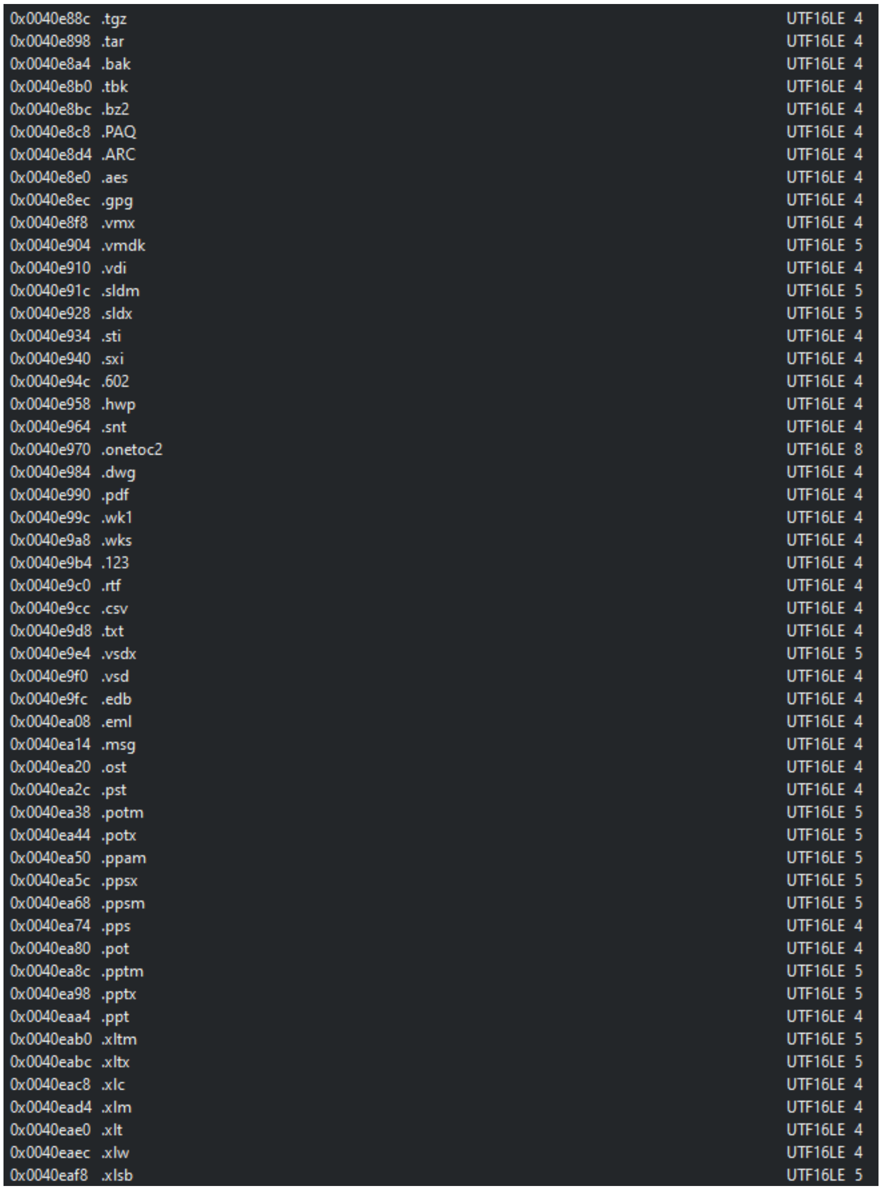
APPENDIX A "." STRING SEARCH



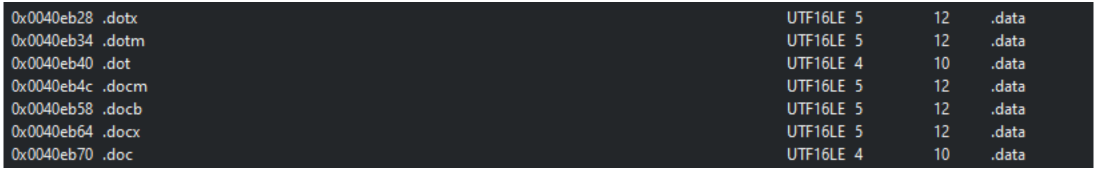
```
0x0040e330  .der                                                                UTF16LE  4
0x0040e33c  .pfx                                                                UTF16LE  4
0x0040e348  .key                                                                UTF16LE  4
0x0040e354  .crt                                                                UTF16LE  4
0x0040e360  .csr                                                                UTF16LE  4
0x0040e36c  .p12                                                                UTF16LE  4
0x0040e378  .pem                                                                UTF16LE  4
0x0040e384  .odt                                                                UTF16LE  4
0x0040e390  .ott                                                                UTF16LE  4
0x0040e39c  .sxw                                                                UTF16LE  4
0x0040e3a8  .stw                                                                UTF16LE  4
0x0040e3b4  .uot                                                                UTF16LE  4
0x0040e3c0  .3ds                                                                UTF16LE  4
0x0040e3cc  .max                                                                UTF16LE  4
0x0040e3d8  .3dm                                                                UTF16LE  4
0x0040e3e4  .ods                                                                UTF16LE  4
0x0040e3f0  .ots                                                                UTF16LE  4
0x0040e3fc  .sxc                                                                UTF16LE  4
0x0040e408  .stc                                                                UTF16LE  4
0x0040e414  .dif                                                                UTF16LE  4
0x0040e420  .slk                                                                UTF16LE  4
0x0040e42c  .wb2                                                                UTF16LE  4
0x0040e438  .odp                                                                UTF16LE  4
0x0040e444  .otp                                                                UTF16LE  4
0x0040e450  .sxd                                                                UTF16LE  4
0x0040e45c  .std                                                                UTF16LE  4
0x0040e468  .uop                                                                UTF16LE  4
0x0040e474  .odg                                                                UTF16LE  4
0x0040e480  .otg                                                                UTF16LE  4
0x0040e48c  .sxm                                                                UTF16LE  4
0x0040e498  .mml                                                                UTF16LE  4
0x0040e4a4  .lay                                                                UTF16LE  4
0x0040e4b0  .lay6                                                               UTF16LE  5
0x0040e4bc  .asc                                                                UTF16LE  4
0x0040e4c8  .sqlite3                                                            UTF16LE  8
0x0040e4dc  .sqlitedb                                                           UTF16LE  9
0x0040e4f0  .sql                                                                UTF16LE  4
0x0040e4fc  .accdb                                                              UTF16LE  6
0x0040e50c  .mdb                                                                UTF16LE  4
0x0040e520  .dbf                                                                UTF16LE  4
0x0040e52c  .odb                                                                UTF16LE  4
0x0040e538  .frm                                                                UTF16LE  4
0x0040e544  .myd                                                                UTF16LE  4
0x0040e550  .myi                                                                UTF16LE  4
0x0040e55c  .ibd                                                                UTF16LE  4
0x0040e568  .mdf                                                                UTF16LE  4
0x0040e574  .ldf                                                                UTF16LE  4
0x0040e580  .sln                                                                UTF16LE  4
0x0040e58c  .suo                                                                UTF16LE  4
0x0040e5a8  .cpp                                                                UTF16LE  4
0x0040e5b4  .pas                                                                UTF16LE  4
0x0040e5c8  .asm                                                                UTF16LE  4
```



```
0x0040e5c8  .asm        UTF16LE  4
0x0040e5dc  .cmd        UTF16LE  4
0x0040e5e8  .bat        UTF16LE  4
0x0040e5f4  .ps1        UTF16LE  4
0x0040e600  .vbs        UTF16LE  4
0x0040e61c  .dip        UTF16LE  4
0x0040e628  .dch        UTF16LE  4
0x0040e634  .sch        UTF16LE  4
0x0040e640  .brd        UTF16LE  4
0x0040e64c  .jsp        UTF16LE  4
0x0040e658  .php        UTF16LE  4
0x0040e664  .asp        UTF16LE  4
0x0040e678  .java       UTF16LE  5
0x0040e684  .jar        UTF16LE  4
0x0040e690  .class      UTF16LE  6
0x0040e6a8  .mp3        UTF16LE  4
0x0040e6b4  .wav        UTF16LE  4
0x0040e6c0  .swf        UTF16LE  4
0x0040e6cc  .fla        UTF16LE  4
0x0040e6d8  .wmv        UTF16LE  4
0x0040e6e4  .mpg        UTF16LE  4
0x0040e6f0  .vob        UTF16LE  4
0x0040e6fc  .mpeg       UTF16LE  5
0x0040e708  .asf        UTF16LE  4
0x0040e714  .avi        UTF16LE  4
0x0040e720  .mov        UTF16LE  4
0x0040e72c  .mp4        UTF16LE  4
0x0040e738  .3gp        UTF16LE  4
0x0040e744  .mkv        UTF16LE  4
0x0040e750  .3g2        UTF16LE  4
0x0040e75c  .flv        UTF16LE  4
0x0040e768  .wma        UTF16LE  4
0x0040e774  .mid        UTF16LE  4
0x0040e780  .m3u        UTF16LE  4
0x0040e78c  .m4u        UTF16LE  4
0x0040e798  .djvu       UTF16LE  5
0x0040e7a4  .svg        UTF16LE  4
0x0040e7b8  .psd        UTF16LE  4
0x0040e7c4  .nef        UTF16LE  4
0x0040e7d0  .tiff       UTF16LE  5
0x0040e7dc  .tif        UTF16LE  4
0x0040e7e8  .cgm        UTF16LE  4
0x0040e7f4  .raw        UTF16LE  4
0x0040e800  .gif        UTF16LE  4
0x0040e80c  .png        UTF16LE  4
0x0040e818  .bmp        UTF16LE  4
0x0040e824  .jpg        UTF16LE  4
0x0040e830  .jpeg       UTF16LE  5
0x0040e83c  .vcd        UTF16LE  4
0x0040e848  .iso        UTF16LE  4
0x0040e854  .backup     UTF16LE  7
0x0040e864  .zip        UTF16LE  4
0x0040e870  .rar        UTF16LE  4
0x0040e88c  .tgz        UTF16LE  4
```



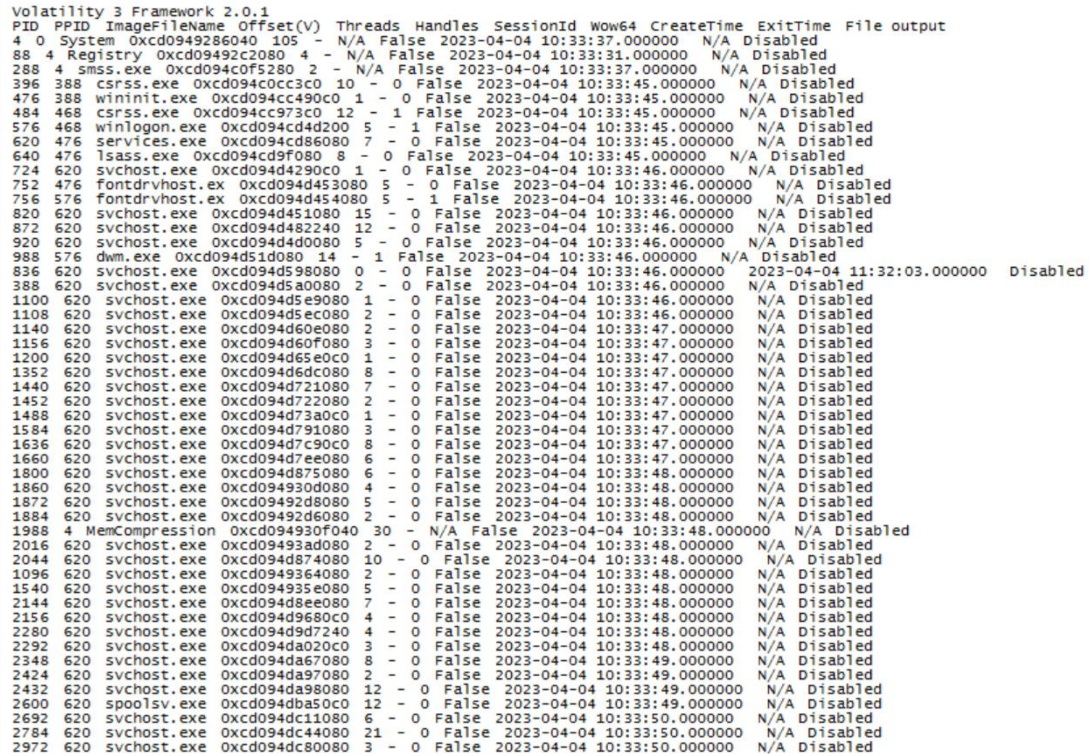
```
0x0040e88c  .tgz       UTF16LE  4
0x0040e898  .tar       UTF16LE  4
0x0040e8a4  .bak       UTF16LE  4
0x0040e8b0  .tbk       UTF16LE  4
0x0040e8bc  .bz2       UTF16LE  4
0x0040e8c8  .PAQ       UTF16LE  4
0x0040e8d4  .ARC       UTF16LE  4
0x0040e8e0  .aes       UTF16LE  4
0x0040e8ec  .gpg       UTF16LE  4
0x0040e8f8  .vmx       UTF16LE  4
0x0040e904  .vmdk      UTF16LE  5
0x0040e910  .vdi       UTF16LE  4
0x0040e91c  .sldm      UTF16LE  5
0x0040e928  .sldx      UTF16LE  5
0x0040e934  .sti       UTF16LE  4
0x0040e940  .sxi       UTF16LE  4
0x0040e94c  .602       UTF16LE  4
0x0040e958  .hwp       UTF16LE  4
0x0040e964  .snt       UTF16LE  4
0x0040e970  .onetoc2   UTF16LE  8
0x0040e984  .dwg       UTF16LE  4
0x0040e990  .pdf       UTF16LE  4
0x0040e99c  .wk1       UTF16LE  4
0x0040e9a8  .wks       UTF16LE  4
0x0040e9b4  .123       UTF16LE  4
0x0040e9c0  .rtf       UTF16LE  4
0x0040e9cc  .csv       UTF16LE  4
0x0040e9d8  .txt       UTF16LE  4
0x0040e9e4  .vsdx      UTF16LE  5
0x0040e9f0  .vsd       UTF16LE  4
0x0040e9fc  .edb       UTF16LE  4
0x0040ea08  .eml       UTF16LE  4
0x0040ea14  .msg       UTF16LE  4
0x0040ea20  .ost       UTF16LE  4
0x0040ea2c  .pst       UTF16LE  4
0x0040ea38  .potm      UTF16LE  5
0x0040ea44  .potx      UTF16LE  5
0x0040ea50  .ppam      UTF16LE  5
0x0040ea5c  .ppsx      UTF16LE  5
0x0040ea68  .ppsm      UTF16LE  5
0x0040ea74  .pps       UTF16LE  4
0x0040ea80  .pot       UTF16LE  4
0x0040ea8c  .pptm      UTF16LE  5
0x0040ea98  .pptx      UTF16LE  5
0x0040eaa4  .ppt       UTF16LE  4
0x0040eab0  .xltm      UTF16LE  5
0x0040eabc  .xltx      UTF16LE  5
0x0040eac8  .xlc       UTF16LE  4
0x0040ead4  .xlm       UTF16LE  4
0x0040eae0  .xlt       UTF16LE  4
0x0040eaec  .xlw       UTF16LE  4
0x0040eaf8  .xlsb      UTF16LE  5
```



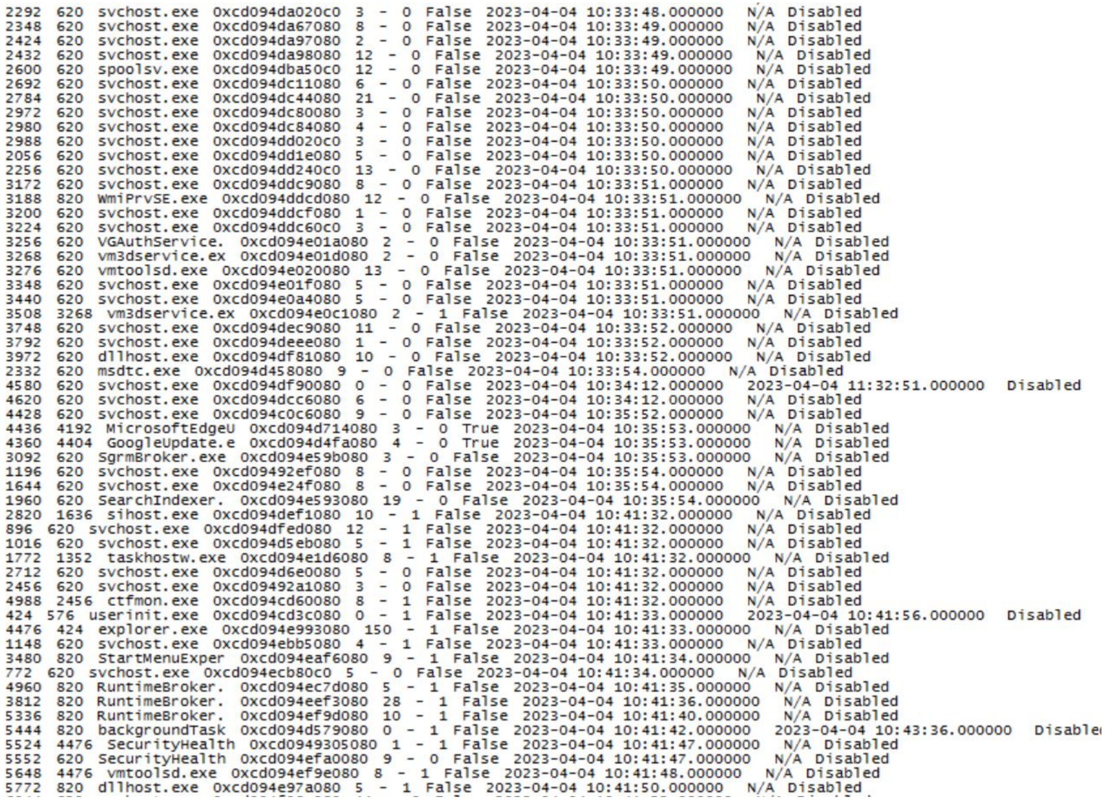
```
0x0040eb28  .dotx      UTF16LE  5      12      .data
0x0040eb34  .dotm      UTF16LE  5      12      .data
0x0040eb40  .dot       UTF16LE  4      10      .data
0x0040eb4c  .docm      UTF16LE  5      12      .data
0x0040eb58  .docb      UTF16LE  5      12      .data
0x0040eb64  .docx      UTF16LE  5      12      .data
0x0040eb70  .doc       UTF16LE  4      10      .data
```

APPENDIX B VOLATILITY

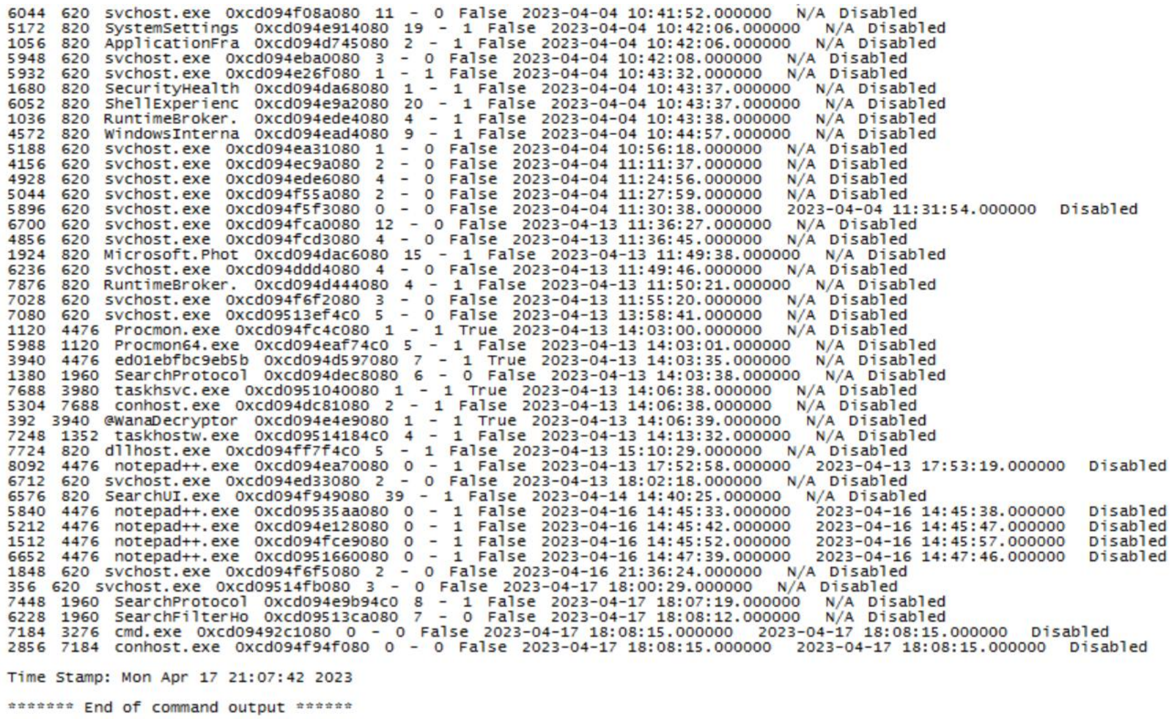
Pslist



```
Volatility 3 Framework 2.0.1
PID  PPID  ImageFileName  Offset(V)  Threads  Handles  SessionId  Wow64  CreateTime  ExitTime  File output
4  0  System  0xcd0949286040  105  -  N/A  False  2023-04-04 10:33:37.000000   N/A  Disabled
88  4  Registry  0xcd09492c2080  4  -  N/A  False  2023-04-04 10:33:31.000000   N/A  Disabled
288  4  smss.exe  0xcd094c0f5280  2  -  N/A  False  2023-04-04 10:33:37.000000   N/A  Disabled
396  388  csrss.exe  0xcd094c0cc3c0  10  -  0  False  2023-04-04 10:33:45.000000   N/A  Disabled
476  388  wininit.exe  0xcd094cc490c0  1  -  0  False  2023-04-04 10:33:45.000000   N/A  Disabled
484  468  csrss.exe  0xcd094cc973c0  12  -  1  False  2023-04-04 10:33:45.000000   N/A  Disabled
576  468  winlogon.exe  0xcd094cd4d200  5  -  1  False  2023-04-04 10:33:45.000000   N/A  Disabled
620  476  services.exe  0xcd094cd86080  7  -  0  False  2023-04-04 10:33:45.000000   N/A  Disabled
640  476  lsass.exe  0xcd094cd9f080  8  -  0  False  2023-04-04 10:33:45.000000   N/A  Disabled
724  620  svchost.exe  0xcd094d4290c0  1  -  0  False  2023-04-04 10:33:46.000000   N/A  Disabled
752  476  fontdrvhost.ex  0xcd094d453080  5  -  0  False  2023-04-04 10:33:46.000000   N/A  Disabled
756  576  fontdrvhost.ex  0xcd094d454080  5  -  1  False  2023-04-04 10:33:46.000000   N/A  Disabled
820  620  svchost.exe  0xcd094d451080  15  -  0  False  2023-04-04 10:33:46.000000   N/A  Disabled
872  620  svchost.exe  0xcd094d482240  12  -  0  False  2023-04-04 10:33:46.000000   N/A  Disabled
920  620  svchost.exe  0xcd094d4d0080  5  -  0  False  2023-04-04 10:33:46.000000   N/A  Disabled
988  576  dwm.exe  0xcd094d51d080  14  -  1  False  2023-04-04 10:33:46.000000   N/A  Disabled
836  620  svchost.exe  0xcd094d598080  0  -  0  False  2023-04-04 10:33:46.000000   2023-04-04 11:32:03.000000   Disabled
388  620  svchost.exe  0xcd094d5a0080  2  -  0  False  2023-04-04 10:33:46.000000   N/A  Disabled
1100  620  svchost.exe  0xcd094d5e9080  1  -  0  False  2023-04-04 10:33:46.000000   N/A  Disabled
1108  620  svchost.exe  0xcd094d5ec080  2  -  0  False  2023-04-04 10:33:46.000000   N/A  Disabled
1140  620  svchost.exe  0xcd094d60e080  2  -  0  False  2023-04-04 10:33:47.000000   N/A  Disabled
1156  620  svchost.exe  0xcd094d60f080  3  -  0  False  2023-04-04 10:33:47.000000   N/A  Disabled
1200  620  svchost.exe  0xcd094d65e0c0  1  -  0  False  2023-04-04 10:33:47.000000   N/A  Disabled
1352  620  svchost.exe  0xcd094d6dc080  8  -  0  False  2023-04-04 10:33:47.000000   N/A  Disabled
1440  620  svchost.exe  0xcd094d721080  7  -  0  False  2023-04-04 10:33:47.000000   N/A  Disabled
1452  620  svchost.exe  0xcd094d722080  2  -  0  False  2023-04-04 10:33:47.000000   N/A  Disabled
1488  620  svchost.exe  0xcd094d73a0c0  1  -  0  False  2023-04-04 10:33:47.000000   N/A  Disabled
1584  620  svchost.exe  0xcd094d791080  3  -  0  False  2023-04-04 10:33:47.000000   N/A  Disabled
1636  620  svchost.exe  0xcd094d7c90c0  8  -  0  False  2023-04-04 10:33:47.000000   N/A  Disabled
1660  620  svchost.exe  0xcd094d7ee080  6  -  0  False  2023-04-04 10:33:47.000000   N/A  Disabled
1800  620  svchost.exe  0xcd094d875080  6  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
1860  620  svchost.exe  0xcd094930d080  4  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
1872  620  svchost.exe  0xcd09492d8080  5  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
1884  620  svchost.exe  0xcd09492d6080  2  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
1988  4  MemCompression  0xcd094930f040  30  -  N/A  False  2023-04-04 10:33:48.000000   N/A  Disabled
2016  620  svchost.exe  0xcd09493ad080  2  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
2044  620  svchost.exe  0xcd094d874080  10  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
1096  620  svchost.exe  0xcd0949364080  2  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
1540  620  svchost.exe  0xcd094935e080  5  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
2144  620  svchost.exe  0xcd094d8ee080  7  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
2156  620  svchost.exe  0xcd094d9680c0  4  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
2280  620  svchost.exe  0xcd094d9d7240  4  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
2292  620  svchost.exe  0xcd094da020c0  3  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
2348  620  svchost.exe  0xcd094da67080  8  -  0  False  2023-04-04 10:33:49.000000   N/A  Disabled
2424  620  svchost.exe  0xcd094da97080  2  -  0  False  2023-04-04 10:33:49.000000   N/A  Disabled
2432  620  svchost.exe  0xcd094da98080  12  -  0  False  2023-04-04 10:33:49.000000   N/A  Disabled
2600  620  spoolsv.exe  0xcd094dba50c0  12  -  0  False  2023-04-04 10:33:49.000000   N/A  Disabled
2692  620  svchost.exe  0xcd094dc11080  6  -  0  False  2023-04-04 10:33:50.000000   N/A  Disabled
2784  620  svchost.exe  0xcd094dc44080  21  -  0  False  2023-04-04 10:33:50.000000   N/A  Disabled
2972  620  svchost.exe  0xcd094dc80080  3  -  0  False  2023-04-04 10:33:50.000000   N/A  Disabled
```



```
2292  620  svchost.exe  0xcd094da020c0  3  -  0  False  2023-04-04 10:33:48.000000   N/A  Disabled
2348  620  svchost.exe  0xcd094da67080  8  -  0  False  2023-04-04 10:33:49.000000   N/A  Disabled
2424  620  svchost.exe  0xcd094da97080  2  -  0  False  2023-04-04 10:33:49.000000   N/A  Disabled
2432  620  svchost.exe  0xcd094da98080  12  -  0  False  2023-04-04 10:33:49.000000   N/A  Disabled
2600  620  spoolsv.exe  0xcd094dba50c0  12  -  0  False  2023-04-04 10:33:49.000000   N/A  Disabled
2692  620  svchost.exe  0xcd094dc11080  6  -  0  False  2023-04-04 10:33:50.000000   N/A  Disabled
2784  620  svchost.exe  0xcd094dc44080  21  -  0  False  2023-04-04 10:33:50.000000   N/A  Disabled
2972  620  svchost.exe  0xcd094dc80080  3  -  0  False  2023-04-04 10:33:50.000000   N/A  Disabled
2980  620  svchost.exe  0xcd094dc84080  4  -  0  False  2023-04-04 10:33:50.000000   N/A  Disabled
2988  620  svchost.exe  0xcd094dd020c0  3  -  0  False  2023-04-04 10:33:50.000000   N/A  Disabled
2056  620  svchost.exe  0xcd094dd1e080  5  -  0  False  2023-04-04 10:33:50.000000   N/A  Disabled
2256  620  svchost.exe  0xcd094dd240c0  13  -  0  False  2023-04-04 10:33:50.000000   N/A  Disabled
3172  620  svchost.exe  0xcd094ddc9080  8  -  0  False  2023-04-04 10:33:51.000000   N/A  Disabled
3188  820  WmiPrvSE.exe  0xcd094ddcd080  12  -  0  False  2023-04-04 10:33:51.000000   N/A  Disabled
3200  620  svchost.exe  0xcd094ddcf080  1  -  0  False  2023-04-04 10:33:51.000000   N/A  Disabled
3224  620  svchost.exe  0xcd094ddc60c0  3  -  0  False  2023-04-04 10:33:51.000000   N/A  Disabled
3256  620  VGAuthService.  0xcd094e01a080  2  -  0  False  2023-04-04 10:33:51.000000   N/A  Disabled
3268  620  vm3dservice.ex  0xcd094e01d080  2  -  0  False  2023-04-04 10:33:51.000000   N/A  Disabled
3276  620  vmtoolsd.exe  0xcd094e020080  13  -  0  False  2023-04-04 10:33:51.000000   N/A  Disabled
3348  620  svchost.exe  0xcd094e01f080  5  -  0  False  2023-04-04 10:33:51.000000   N/A  Disabled
3440  620  svchost.exe  0xcd094e0a4080  5  -  0  False  2023-04-04 10:33:51.000000   N/A  Disabled
3508  3268  vm3dservice.ex  0xcd094e0c1080  2  -  1  False  2023-04-04 10:33:51.000000   N/A  Disabled
3748  620  svchost.exe  0xcd094dec9080  11  -  0  False  2023-04-04 10:33:52.000000   N/A  Disabled
3792  620  svchost.exe  0xcd094deee080  1  -  0  False  2023-04-04 10:33:52.000000   N/A  Disabled
3972  620  dllhost.exe  0xcd094df81080  10  -  0  False  2023-04-04 10:33:52.000000   N/A  Disabled
2332  620  msdtc.exe  0xcd094d458080  9  -  0  False  2023-04-04 10:33:54.000000   N/A  Disabled
4580  620  svchost.exe  0xcd094df90080  0  -  0  False  2023-04-04 10:34:12.000000   2023-04-04 11:32:51.000000   Disabled
4620  620  svchost.exe  0xcd094dcc6080  6  -  0  False  2023-04-04 10:34:12.000000   N/A  Disabled
4428  620  svchost.exe  0xcd094c0c6080  9  -  0  False  2023-04-04 10:35:52.000000   N/A  Disabled
4436  4192  MicrosoftEdgeU  0xcd094d714080  3  -  0  True  2023-04-04 10:35:53.000000   N/A  Disabled
4360  4404  GoogleUpdate.e  0xcd094d4fa080  4  -  0  True  2023-04-04 10:35:53.000000   N/A  Disabled
3092  620  SgrmBroker.exe  0xcd094e59b080  3  -  0  False  2023-04-04 10:35:53.000000   N/A  Disabled
1196  620  svchost.exe  0xcd09492ef080  8  -  0  False  2023-04-04 10:35:54.000000   N/A  Disabled
1644  620  svchost.exe  0xcd094e24f080  8  -  0  False  2023-04-04 10:35:54.000000   N/A  Disabled
1960  620  SearchIndexer.  0xcd094e593080  19  -  0  False  2023-04-04 10:35:54.000000   N/A  Disabled
2820  1636  sihost.exe  0xcd094def1080  10  -  1  False  2023-04-04 10:41:32.000000   N/A  Disabled
896  620  svchost.exe  0xcd094dfed080  12  -  1  False  2023-04-04 10:41:32.000000   N/A  Disabled
1016  620  svchost.exe  0xcd094d5eb080  5  -  1  False  2023-04-04 10:41:32.000000   N/A  Disabled
1772  1352  taskhostw.exe  0xcd094e1d6080  8  -  1  False  2023-04-04 10:41:32.000000   N/A  Disabled
2712  620  svchost.exe  0xcd094d6e0080  5  -  0  False  2023-04-04 10:41:32.000000   N/A  Disabled
2456  620  svchost.exe  0xcd09492a1080  3  -  0  False  2023-04-04 10:41:32.000000   N/A  Disabled
4988  2456  ctfmon.exe  0xcd094cd60080  8  -  1  False  2023-04-04 10:41:32.000000   N/A  Disabled
424  576  userinit.exe  0xcd094cd3c080  0  -  1  False  2023-04-04 10:41:33.000000   2023-04-04 10:41:56.000000   Disabled
4476  424  explorer.exe  0xcd094e993080  150  -  1  False  2023-04-04 10:41:33.000000   N/A  Disabled
1148  620  svchost.exe  0xcd094ebb5080  4  -  1  False  2023-04-04 10:41:33.000000   N/A  Disabled
3480  820  StartMenuExper  0xcd094eaf6080  9  -  1  False  2023-04-04 10:41:34.000000   N/A  Disabled
772  620  svchost.exe  0xcd094ecb80c0  5  -  0  False  2023-04-04 10:41:34.000000   N/A  Disabled
4960  820  RuntimeBroker.  0xcd094ec7d080  5  -  1  False  2023-04-04 10:41:35.000000   N/A  Disabled
3812  820  RuntimeBroker.  0xcd094eef3080  28  -  1  False  2023-04-04 10:41:36.000000   N/A  Disabled
5336  820  RuntimeBroker.  0xcd094ef9d080  10  -  1  False  2023-04-04 10:41:40.000000   N/A  Disabled
5444  820  backgroundTask  0xcd094d579080  0  -  1  False  2023-04-04 10:41:42.000000   2023-04-04 10:43:36.000000   Disable
5524  4476  SecurityHealth  0xcd0949305080  1  -  1  False  2023-04-04 10:41:47.000000   N/A  Disabled
5552  620  SecurityHealth  0xcd094efa0080  9  -  0  False  2023-04-04 10:41:47.000000   N/A  Disabled
5648  4476  vmtoolsd.exe  0xcd094ef9e080  8  -  1  False  2023-04-04 10:41:48.000000   N/A  Disabled
5772  820  dllhost.exe  0xcd094e97a080  5  -  1  False  2023-04-04 10:41:50.000000   N/A  Disabled
```



```
6044  620  svchost.exe  0xcd094f08a080  11  -  0  False  2023-04-04 10:41:52.000000   N/A  Disabled
5172  820  SystemSettings  0xcd094e914080  19  -  1  False  2023-04-04 10:42:06.000000   N/A  Disabled
1056  820  ApplicationFra  0xcd094d745080  2  -  1  False  2023-04-04 10:42:06.000000   N/A  Disabled
5948  620  svchost.exe  0xcd094eba0080  3  -  0  False  2023-04-04 10:42:08.000000   N/A  Disabled
5932  620  svchost.exe  0xcd094e26f080  1  -  1  False  2023-04-04 10:43:32.000000   N/A  Disabled
1680  820  SecurityHealth  0xcd094da68080  1  -  1  False  2023-04-04 10:43:37.000000   N/A  Disabled
6052  820  ShellExperienc  0xcd094e9a2080  20  -  1  False  2023-04-04 10:43:37.000000   N/A  Disabled
1036  820  RuntimeBroker.  0xcd094ede4080  4  -  1  False  2023-04-04 10:43:38.000000   N/A  Disabled
4572  820  WindowsInterna  0xcd094ead4080  9  -  1  False  2023-04-04 10:44:57.000000   N/A  Disabled
5188  620  svchost.exe  0xcd094ea31080  1  -  0  False  2023-04-04 10:56:18.000000   N/A  Disabled
4156  620  svchost.exe  0xcd094ec9a080  2  -  0  False  2023-04-04 11:11:37.000000   N/A  Disabled
4928  620  svchost.exe  0xcd094ede6080  4  -  0  False  2023-04-04 11:24:56.000000   N/A  Disabled
5044  620  svchost.exe  0xcd094f55a080  2  -  0  False  2023-04-04 11:27:59.000000   N/A  Disabled
5896  620  svchost.exe  0xcd094f5f3080  0  -  0  False  2023-04-04 11:30:38.000000   2023-04-04 11:31:54.000000   Disabled
6700  620  svchost.exe  0xcd094fca0080  12  -  0  False  2023-04-13 11:36:27.000000   N/A  Disabled
4856  620  svchost.exe  0xcd094fcd3080  4  -  0  False  2023-04-13 11:36:45.000000   N/A  Disabled
1924  820  Microsoft.Phot  0xcd094dac6080  15  -  1  False  2023-04-13 11:49:38.000000   N/A  Disabled
6236  620  svchost.exe  0xcd094ddd4080  4  -  0  False  2023-04-13 11:49:46.000000   N/A  Disabled
7876  820  RuntimeBroker.  0xcd094d444080  4  -  1  False  2023-04-13 11:50:21.000000   N/A  Disabled
7028  620  svchost.exe  0xcd094f6f2080  3  -  0  False  2023-04-13 11:55:20.000000   N/A  Disabled
7080  620  svchost.exe  0xcd09513ef4c0  5  -  0  False  2023-04-13 13:58:41.000000   N/A  Disabled
1120  4476  Procmon.exe  0xcd094fc4c080  1  -  1  True  2023-04-13 14:03:00.000000   N/A  Disabled
5988  1120  Procmon64.exe  0xcd094eaf74c0  5  -  1  False  2023-04-13 14:03:01.000000   N/A  Disabled
3940  4476  ed01ebfbc9eb5b  0xcd094d597080  7  -  1  True  2023-04-13 14:03:35.000000   N/A  Disabled
1380  1960  SearchProtocol  0xcd094dec8080  6  -  0  False  2023-04-13 14:03:38.000000   N/A  Disabled
7688  3980  taskhsvc.exe  0xcd0951040080  1  -  1  True  2023-04-13 14:06:38.000000   N/A  Disabled
5304  7688  conhost.exe  0xcd094dc81080  2  -  1  False  2023-04-13 14:06:38.000000   N/A  Disabled
392  3940  @WanaDecryptor  0xcd094e4e9080  1  -  1  True  2023-04-13 14:06:39.000000   N/A  Disabled
7248  1352  taskhostw.exe  0xcd09514184c0  4  -  1  False  2023-04-13 14:13:32.000000   N/A  Disabled
7724  820  dllhost.exe  0xcd094ff7f4c0  5  -  1  False  2023-04-13 15:10:29.000000   N/A  Disabled
8092  4476  notepad++.exe  0xcd094ea70080  0  -  1  False  2023-04-13 17:52:58.000000   2023-04-13 17:53:19.000000   Disabled
6712  620  svchost.exe  0xcd094ed33080  2  -  0  False  2023-04-13 18:02:18.000000   N/A  Disabled
6576  820  SearchUI.exe  0xcd094f949080  39  -  1  False  2023-04-14 14:40:25.000000   N/A  Disabled
5840  4476  notepad++.exe  0xcd09535aa080  0  -  1  False  2023-04-16 14:45:33.000000   2023-04-16 14:45:38.000000   Disabled
5212  4476  notepad++.exe  0xcd094e128080  0  -  1  False  2023-04-16 14:45:42.000000   2023-04-16 14:45:47.000000   Disabled
1512  4476  notepad++.exe  0xcd094fce9080  0  -  1  False  2023-04-16 14:45:52.000000   2023-04-16 14:45:57.000000   Disabled
6652  4476  notepad++.exe  0xcd0951660080  0  -  1  False  2023-04-16 14:47:39.000000   2023-04-16 14:47:46.000000   Disabled
1848  620  svchost.exe  0xcd094f6f5080  2  -  0  False  2023-04-16 21:36:24.000000   N/A  Disabled
356  620  svchost.exe  0xcd09514fb080  3  -  0  False  2023-04-17 18:00:29.000000   N/A  Disabled
7448  1960  SearchProtocol  0xcd094e9b94c0  8  -  1  False  2023-04-17 18:07:19.000000   N/A  Disabled
6228  1960  SearchFilterHo  0xcd09513ca080  7  -  0  False  2023-04-17 18:08:12.000000   N/A  Disabled
7184  3276  cmd.exe  0xcd09492c1080  0  -  0  False  2023-04-17 18:08:15.000000   2023-04-17 18:08:15.000000   Disabled
2856  7184  conhost.exe  0xcd094f94f080  0  -  0  False  2023-04-17 18:08:15.000000   2023-04-17 18:08:15.000000   Disabled

Time Stamp: Mon Apr 17 21:07:42 2023

******* End of command output ******
```

Filescan

```
0xcd094e35d3d0  \Windows\System32\msxml3.dll    216
0xcd094e35d560  \Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\280810\1677463469    216
0xcd094e35d6f0  \Windows\SystemResources\Windows.UI.ShellCommon\pris\Windows.UI.ShellCommon.en-US.pri   216
0xcd094e35d880  \Windows\System32\ConhostV1.dll 216
0xcd094e35da10  \$Directory    216
0xcd094e35dd30  \Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\bf92dcc11e428fd5adf02632b5d4414f\mscorlib.ni.dll  216
0xcd094e35dec0  \Windows\System32\ContactApis.dll       216
0xcd094e35e1e0  \Windows\System32\pkeyhelper.dll       216
0xcd094e35e370  \Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvc.dll       216
0xcd094e35e500  \Windows\Microsoft.NET\Framework\v4.0.30319\fusion.dll  216
0xcd094e35e690  \Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258922915019775.txt.WNCRYT      216
0xcd094e35e820  \Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll  216
0xcd094e35e9b0  \Windows\System32\ContentDeliveryManager.Utilities.dll  216
0xcd094e35eb40  \$Directory    216
0xcd094e35ecd0  \Windows\SysWOW64\ucrtbase_clr0400.dll  216
0xcd094e35ee60  \Windows\System32\EdgeContent.dll      216
0xcd094e35f180  \Windows\System32\LicenseManagerSvc.dll 216
0xcd094e35f310  \Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258923214228393.txt.WNCRYT      216
0xcd094e35f4a0  \Windows\System32\DriverStore\FileRepository\pci.inf_amd64_8229e68f95778644\pci.inf     216
0xcd094e35f630  \Windows\assembly\NativeImages_v4.0.30319_32\System\9340a40c55ba464d0af1399814a708eb\System.ni.dll      216
0xcd094e35fae0  \Windows\servicing\Packages\Microsoft-Windows-Multimedia-MF-WOW64-Package~31bf3856ad364e35~amd64~~10.0.18362.418.mum       216
0xcd094e35fe00  \$Directory    216
0xcd094e360120  \CMApi  216
0xcd094e360440  \Windows\Registration\R000000000006.clb 216
0xcd094e3605d0  \Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\resources.pri       216
0xcd094e360760  \Windows\System32\en-US\windows.storage.dll.mui 216
0xcd094e360a80  \Windows\System32\AdaptiveCards.dll     216
0xcd094e360c10  \Windows\rescache\_merged\4124255888\3469843017.pri     216
0xcd094e360da0  \$Directory    216
```

```
0xcd094e3610c0  \Windows\ShellExperiences\ClockFlyoutExperience.dll     216
0xcd094e3613e0  \Windows\ShellExperiences\BatteryFlyoutExperience.dll   216
0xcd094e361700  \Windows\System32\browser_broker.exe    216
0xcd094e361a20  \Windows\System32\en-US\KernelBase.dll.mui      216
0xcd094e361bb0  \Windows\servicing\Packages\Microsoft-Windows-PeerDist-Client-WOW64-
Package~31bf3856ad364e35~amd64~~10.0.18362.1.mum        216
0xcd094e361ed0  \Windows\System32\ContactActivation.dll 216
0xcd094e362510  \Windows\System32\certCredProvider.dll  216
0xcd094e3629c0  \Windows\servicing\Packages\Microsoft-Windows-InternetExplorer-Package-
ua~31bf3856ad364e35~amd64~~10.0.18362.1.mum  216
0xcd094e362b50  \$Directory     216
0xcd094e362ce0  \Windows\System32\Dism\OSProvider.dll   216
0xcd094e362e70  \Windows\System32\hgcpl.dll     216
0xcd094e363190  \Windows\System32\mfsvr.dll     216
0xcd094e363320  \Windows\System32\VAN.dll       216
0xcd094e3634b0  \Windows\System32\scrobj.dll    216
0xcd094e363640  \$Directory     216
0xcd094e3637d0  \Program Files\Common Files\microsoft shared\ink\InkObj.dll     216
0xcd094e363960  \Windows\System32\Windows.Services.TargetedContent.dll  216
0xcd094e363c80  \Program Files\Common Files\microsoft shared\ink\tipskins.dll   216
0xcd094e364130
\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\46e353730ff652f2cc418d8cc7c51cf3\System.Management.ni.dll    216
0xcd094e3642c0  \Windows\System32\en-US\occache.dll.mui 216
0xcd094e364450  \Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe        216
0xcd094e3645e0  \Windows\System32\en-US\ShutdownUX.dll.mui      216
0xcd094e364770  \Windows\System32\msxml3r.dll   216
0xcd094e364a90  \Windows\System32\fdPnp.dll     216
0xcd094e364c20  \Windows\System32\Dism\SetupPlatformProvider.dll        216
0xcd094e364db0  \$Directory     216
0xcd094e3650d0  \Program Files\Common Files\microsoft shared\ink\tabskb.dll     216
0xcd094e3653f0  \Windows\System32\Dism\OfflineSetupProvider.dll 216
0xcd094e365580
\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\46e353730ff652f2cc418d8cc7c51cf3\System.Management.ni.dll.aux
216
0xcd094e365710  \Windows\System32\Dism\ProvProvider.dll 216
0xcd094e3658a0  \Sessions\1\AppContainerNamedObjects\S-1-15-2-1861897761-1695161497-2927542615-642690995-327840285-
2659745135-2630312742    216
0xcd094e365a30  \Program Files\Common Files\microsoft shared\ink\TabTip.exe     216
0xcd094e365bc0  \Windows\System32\mf.dll        216
0xcd094e365ee0  \Windows\System32\msfeeds.dll   216
0xcd094e366200  \Windows\System32\Dism\SmiProvider.dll  216
0xcd094e366390  \Windows\System32\MP3DMOD.DLL   216
0xcd094e366520  \Windows\System32\Dism\TransmogProvider.dll     216
0xcd094e3666b0  \$Directory     216
0xcd094e366840  \$Directory     216
0xcd094e366b60  \Windows\System32\WMVCORE.DLL   216
0xcd094e366cf0  \Windows\System32\mfperfhelper.dll      216
0xcd094e366e80  \Windows\System32\msoert2.dll   216
0xcd094e3671a0  \Windows\System32\SystemSettings.DataModel.dll  216
0xcd094e3674c0  \Windows\System32\spfileq.dll   216
0xcd094e367970  \$Directory     216
0xcd094e367b00  \Windows\System32\Dism\UnattendProvider.dll     216
0xcd094e367e20  \Windows\System32\hnetcfg.dll   216
0xcd094e368140  \Windows\System32\AppxPackaging.dll     216
0xcd094e368460  \Windows\System32\netcfgx.dll   216
0xcd094e3685f0  \Windows\System32\Dism\VhdProvider.dll  216
0xcd094e368910  \Windows\System32\Dism\SysprepProvider.dll      216
0xcd094e368c30  \Windows\System32\imgutil.dll   216
0xcd094e368dc0  \Windows\System32\DriverStore\en-US\pci.inf_loc 216
0xcd094e3690e0  \Windows\System32\lsmproxy.dll  216
0xcd094e369400  \Program Files (x86)\Microsoft Visual
Studio\2017\BuildTools\Common7\IDE\PrivateAssemblies\Microsoft.VisualStudio.DeveloperTools.dll        216
0xcd094e369590
\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Configuration\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Configuration.dll       216
0xcd094e369720  \Windows\System32\imapi2fs.dll  216
0xcd094e3698b0  \Windows\System32\mfh264enc.dll 216
```

```
0xcd094e369a40  \Windows\System32\DriverStore\FileRepository\vmci.inf_amd64_5e38a278d114b813\vmci.inf   216
0xcd094e369d60  \$Directory     216
0xcd094e369ef0
\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\11878517dd3152d405eed8c5c5d0c552\System.Windows.Forms.ni.
dll     216
0xcd094e36a080  \Windows\System32\inetcomm.dll  216
0xcd094e36a210  \Windows\System32\filemgmt.dll  216
0xcd094e36a3a0  \Windows\servicing\Packages\Package_for_KB4513661~31bf3856ad364e35~amd64~~10.0.1.16.mum 216
0xcd094e36a530  \Windows\System32\MP4SDECD.DLL  216
0xcd094e36a6c0  \Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll     216
0xcd094e36a850  \Windows\assembly\GAC_32\System.EnterpriseServices\2.0.0.0__b03f5f7f11d50a3a\System.EnterpriseServices.dll 216
0xcd094e36a9e0  \Windows\servicing\Packages\HyperV-Storage-VirtualDevice-SCSI-onecore-Package~31bf3856ad364e35~amd64~en-
US~10.0.18362.1.mum 216
0xcd094e36ab70  \Windows\WinSxS\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.18362.411_none_5f53d2d858cf8961\wcp.dll       216
0xcd094e36ad00  \Program Files (x86)\Microsoft Visual Studio\2017\BuildTools\Common7\IDE\PrivateAssemblies\MetricsPackage.dll       216
0xcd094e36ae90  \$Directory     216
0xcd094e36b1b0  \Windows\Microsoft.NET\Framework64\v4.0.30319\mscoree.tlb       216
0xcd094e36b340  \Program Files (x86)\Microsoft Visual
Studio\2017\BuildTools\Common7\IDE\PrivateAssemblies\Microsoft.VisualStudio.CodeAnalysis.Sdk.UI.dll   216
0xcd094e36b4d0  \Windows\ImmersiveControlPanel\en-US\SystemSettings.exe.mui     216
0xcd094e36b660  \Windows\System32\mycomput.dll  216
0xcd094e36bb10  \$Directory     216
0xcd094e36be30  \Windows\System32\licmgr10.dll  216
0xcd094e36c150  \$Directory     216
0xcd094e36c2e0  \Windows\Microsoft.NET\assembly\GAC_32\System.Web\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Web.dll 216
0xcd094e36c470  \Program Files (x86)\Microsoft Visual
Studio\2017\BuildTools\Common7\IDE\PrivateAssemblies\Microsoft.VisualStudio.CodeAnalysis.Common.dll   216
0xcd094e36c600  \Windows\System32\PlayToManager.dll     216
0xcd094e36c920  \$Directory     216
0xcd094e36cab0  \Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.9659_none_d08cfd96442b25cc\msvcr80.dll   216
0xcd094e36cc40  \Windows\System32\LockController.dll    216
0xcd094e36cdd0  \Windows\assembly\GAC_MSIL\Accessibility\2.0.0.0__b03f5f7f11d50a3a\Accessibility.dll    216
0xcd094e36d0f0  \Program Files (x86)\Microsoft Visual
Studio\2017\BuildTools\Common7\IDE\PrivateAssemblies\Microsoft.VisualStudio.CodeAnalysis.dll  216
0xcd094e36d280  \Windows\System32\unenrollhook.dll      216
0xcd094e36d5a0  \Windows\assembly\GAC_32\System.Transactions\2.0.0.0__b77a5c561934e089\System.Transactions.dll  216
0xcd094e36d730  \Windows\System32\MFMediaEngine.dll     216
0xcd094e36d8c0  \Windows\System32\LockAppBroker.dll     216
0xcd094e36da50  \Program Files (x86)\Microsoft Visual Studio\2017\BuildTools\Common7\IDE\PrivateAssemblies\FxCopSdk.dll 216
0xcd094e36dbe0  \Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll       216
0xcd094e36dd70  \$Directory     216
0xcd094e36e090  \Windows\System32\SensorsApi.dll        216
0xcd094e36e220  \Windows\System32\mfasfsrcsnk.dll       216
0xcd094e36e3b0  \Program Files (x86)\Microsoft Visual Studio\2017\BuildTools\Common7\IDE\PrivateAssemblies\Microsoft.Cci.dl216
0xcd094e36e540  \Windows\System32\srclient.dll  216
0xcd094e36e6d0  \Windows\System32\MSAudDecMFT.dll       216
0xcd094e36e9f0  \Windows\System32\MbaeApiPublic.dll     216
0xcd094e36eb80  \Windows\System32\NetSetupShim.dll      216
0xcd094e36eea0  \Windows\SysWOW64\WofUtil.dll   216
0xcd094e36f1c0  \$Directory     216
0xcd094e36f350  \Windows\System32\en-US\wscapi.dll.mui  216
0xcd094e36f670  \Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppData\CacheStorage\CacheStorage.edb
216
0xcd094e36f800  \$Directory     216
0xcd094e36f990  \Windows\servicing\Packages\HyperV-Storage-VirtualDevice-SMB-onecore-Package~31bf3856ad364e35~amd64~en-
US~10.0.18362.1.mum  216
0xcd094e36fcb0  \Windows\System32\LocationWinPalMisc.dll        216
0xcd094e36fe40  \Windows\WinSxS\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.18362.411_none_5f53d2d858cf8961\dpx.dll       216
0xcd094e370160  \Windows\System32\RoamingSecurity.dll   216
0xcd094e3702f0  \Windows\System32\MFCaptureEngine.dll   216
0xcd094e370480  \Program Files (x86)\Microsoft Visual Studio\2017\BuildTools\MSBuild\15.0\Bin\Roslyn\VBCSCompiler.exe   216
0xcd094e370610  \Windows\System32\LocationFrameworkPS.dll       216
0xcd094e3707a0  \Windows\System32\SecurityCenterBrokerPS.dll    216
0xcd094e370930  \Windows\System32\PortableDeviceClassExtension.dll      216
```

```
0xcd094e370ac0  \$Directory     216
0xcd094e370c50  \Program Files (x86)\Microsoft Visual Studio\2017\BuildTools\MSBuild\15.0\Bin\Roslyn\Microsoft.CodeAnalysis.dll     216
0xcd094e370de0  \Windows\Microsoft.NET\assembly\GAC_MSIL\System.Reflection\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Reflection.dll
216
0xcd094e371100
\Windows\assembly\NativeImages_v4.0.30319_64\System.Security\6a654c317ce4dba078abb5e13062ee95\System.Security.ni.dll.aux    216
0xcd094e3715b0  \Windows\servicing\Packages\HyperV-Storage-VirtualDevice-SMB-Package~31bf3856ad364e35~amd64~en-
US~10.0.18362.1.mum  216
0xcd094e371740  \Windows\System32\LocationFramework.dll 216
0xcd094e3718d0  \Windows\System32\LocationFrameworkInternalPS.dll       216
0xcd094e371a60  \$Directory     216
0xcd094e371d80  \Windows\System32\SystemSettingsBroker.exe      216
0xcd094e3720a0  \Windows\System32\ngclocal.dll  216
0xcd094e372230  \Windows\System32\SensorsClassExtension.dll     216
0xcd094e3723c0  \Windows\System32\SecurityHealthSystray.exe     216
0xcd094e372550  \Windows\System32\wcmapi.dll    216
0xcd094e3726e0  \Windows\System32\WUDFx.dll     216
0xcd094e372870  \Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppData\CacheStorage\CacheStorage.jfm
216
0xcd094e372a00  \Windows\System32\WwaApi.dll    216
0xcd094e372b90  \$Directory     216
0xcd094e372d20  \Windows\servicing\Packages\Microsoft-OneCore-Multimedia-MFPMP-WOW64-Package~31bf3856ad364e35~amd64~en-
US~10.0.18362.1.mum  216
0xcd094e372eb0  \Windows\Globalization\ICU\zoneinfo64.res       216
0xcd094e4441e0  \Windows\System32\wbem\wbemdisp.dll     216
0xcd094e444370
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133261281769166
927.txt.WNCRYT       216
0xcd094e444500  \Windows\System32\UiaManager.dll        216
0xcd094e444690  \$Directory     216
0xcd094e444820  \Windows\System32\WindowsCodecsExt.dll  216
0xcd094e4449b0  \Windows\System32\VaultRoaming.dll      216
0xcd094e444b40  \Windows\System32\WebRuntimeManager.dll 216
0xcd094e444cd0  \Windows\System32\Windows.UI.Search.dll 216
0xcd094e445310  \Sessions\1\AppContainerNamedObjects\S-1-15-2-3945102849-3632965805-3846928828-240845225-3300287824-
62672950-817265009      216
0xcd094e4454a0  \Windows\System32\Windows.Media.Audio.dll       216
0xcd094e445630  \$Directory     216
0xcd094e4457c0  \Windows\rescache\_merged\4046380488\1605388177.pri     216
0xcd094e445950  \Windows\System32\WMADMOE.DLL   216
0xcd094e445e00  \Windows\SystemApps\InputApp_cw5n1h2txyewy\WindowsInternal.ComposableShell.Experiences.TextInput.InputApp.exe
216
0xcd094e4465d0  \Windows\System32\XamlTileRender.dll    216
0xcd094e446760  \Windows\System32       216
0xcd094e4468f0  \$Directory     216
0xcd094e446da0  \Windows\System32\wbem\NCProv.dll       216
0xcd094e4470c0  \Windows\System32\WWAHost.exe   216
0xcd094e447250  \Windows\System32\WUDFHost.exe  216
0xcd094e4473e0  \Windows\SystemApps\Microsoft.LockApp_cw5n1h2txyewy\LockApp.exe 216
0xcd094e447570  \Windows\System32\Windows.Media.MediaControl.dll        216
0xcd094e447700  \Windows\System32       216
0xcd094e447d40  \$Directory     216
0xcd094e447ed0  \$Directory     216
0xcd094e4481f0  \Windows\System32\oleacc.dll    216
0xcd094e448380  \Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\eData.dll     216
0xcd094e448510  \$Directory     216
0xcd094e4486a0  \Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\eView.dll     216
0xcd094e448830  \Windows\System32\sbservicetrigger.dll  216
0xcd094e4489c0  \Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.18362.418_none_e6c6b287130d565216
0xcd094e448b50  \Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\eModel.dll    216
0xcd094e448e70  \$Directory     216
0xcd094e449190  \Windows\Registration\R000000000006.clb 216
0xcd094e449320  \ProgramData\Microsoft\Windows Security Health\Logs\SHS-04042023-114148-7-3f-18362.1.amd64fre.19h1_release.190318-
1202.etl  216
0xcd094e4494b0  \$Directory     216
```

```
0xcd094e4497d0  \Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppData\CacheStorage\CacheStorage.edb
216
0xcd094e449c80  \Windows\System32\Windows.ApplicationModel.LockScreen.dll       216
0xcd094e449e10  \CMApi  216
0xcd094e44a2c0  \Windows\System32\Windows.Graphics.Printing.dll 216
0xcd094e44a450  \Windows\System32\Windows.Internal.ShellCommon.Broker.dll       216
0xcd094e44a5e0  \Windows\SysWOW64\dpapi.dll     216
0xcd094e44a900  \Windows\SysWOW64\dcomp.dll     216
0xcd094e44aa90  \Windows\SysWOW64\devobj.dll    216
0xcd094e44ac20  \Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe     216
0xcd094e44adb0  \Windows\SysWOW64\winmm.dll     216
0xcd094e44b0d0  \Windows\SysWOW64\Wpc.dll       216
0xcd094e44b260  \Windows\SysWOW64\dxgi.dll      216
0xcd094e44b580  \Windows\SysWOW64\d3d9.dll      216
0xcd094e44b710  \Windows\SysWOW64\avrt.dll      216
0xcd094e44b8a0  \Windows\SysWOW64\d2d1.dll      216
0xcd094e44ba30  \Windows\SysWOW64\mlang.dll     216
0xcd094e44bbc0  \Windows\SysWOW64\mfsvr.dll     216
0xcd094e44bd50  \Windows\SysWOW64\mswsock.dll   216
0xcd094e44c200  \Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\CortanaSpeechux.dll 216
0xcd094e44c520  \Windows\SysWOW64\mf.dll        216
0xcd094e44c6b0  \Windows\SysWOW64\atl.dll       216
0xcd094e44c840  \Windows\SysWOW64\esent.dll     216
0xcd094e44c9d0  \Windows\SysWOW64\duser.dll     216
0xcd094e44cb60  \Windows\SysWOW64\dui70.dll     216
0xcd094e44ccf0  \Windows\SysWOW64\d3d11.dll     216
0xcd094e44d1a0  \Windows\SysWOW64\gpapi.dll     216
0xcd094e44d330  \Windows\SysWOW64\mscms.dll     216
0xcd094e44d650  \Windows\System32\en-US\KernelBase.dll.mui      216
0xcd094e44d7e0
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258842780945
206.txt.WNCRYT      216
0xcd094e44d970
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258834892395
692.txt.WNCRYT      216
0xcd094e44db00  \Windows\SysWOW64\oleacc.dll    216
0xcd094e44dc90  \Windows\SysWOW64\RTWorkQ.dll   216
0xcd094e44de20  \Windows\SysWOW64\cabinet.dll   216
0xcd094e44e140
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258842480700
632.txt.WNCRYT      216
0xcd094e44e460  \Windows\SysWOW64\devrtl.dll    216
0xcd094e44e5f0  \Windows\SysWOW64\Chakra.dll    216
0xcd094e44e910  \Windows\SysWOW64\tquery.dll    216
0xcd094e44eaa0  \Windows\SysWOW64\mfcore.dll    216
0xcd094e44ec30  \Windows\SysWOW64\msv1_0.dll    216
0xcd094e44edc0  \Windows\SysWOW64\mfc42u.dll    216
0xcd094e44f0e0  \Windows\SysWOW64\ninput.dll    216
0xcd094e44f270  \Windows\SysWOW64\secur32.dll   216
0xcd094e44f400  \Windows\SysWOW64\dsound.dll    216
0xcd094e44f590  \Windows\SysWOW64\msvcp110_win.dll      216
0xcd094e44fa40  \Windows\SysWOW64\imgutil.dll   216
0xcd094e44fbd0
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258841134264
267.txt.WNCRYT      216
0xcd094e44fef0  \Windows\SysWOW64\MP3DMOD.DLL   216
0xcd094e450080  \Windows\SysWOW64\mshtml.dll    216
0xcd094e450210  \Windows\SysWOW64\mfplat.dll    216
0xcd094e4503a0  \Windows\SysWOW64\msimtf.dll    216
0xcd094e450530  \Windows\SysWOW64\DWrite.dll    216
0xcd094e450850  \Windows\SysWOW64\nlaapi.dll    216
0xcd094e4509e0  \Windows\SysWOW64\dbghelp.dll   216
0xcd094e450b70  \Windows\SysWOW64\wdigest.dll   216
0xcd094e450d00  \Windows\SysWOW64\wtsapi32.dll  216
0xcd094e450e90  \Windows\SysWOW64\msftedit.dll  216
0xcd094e4511b0  \Windows\SysWOW64\prnfldr.dll   216
```

```
0xcd094e451340  \Windows\SysWOW64\mssprxy.dll   216
0xcd094e4514d0  \Windows\SysWOW64\MrmCoreR.dll  216
0xcd094e451660  \Windows\SysWOW64\twinapi.dll   216
0xcd094e4517f0  \Windows\SysWOW64\cryptui.dll   216
0xcd094e451980  \Windows\SysWOW64\actxprxy.dll  216
0xcd094e451b10  \Windows\SysWOW64\MMDevAPI.dll  216
0xcd094e451ca0  \Windows\SysWOW64\jscript9.dll  216
0xcd094e451e30  \Windows\SysWOW64\wininet.dll   216
0xcd094e452150  \Windows\SysWOW64\wkscli.dll    216
0xcd094e452470  \Windows\SysWOW64\cryptnet.dll  216
0xcd094e452600
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258839721465
835.txt.WNCRYT      216
0xcd094e452790  \Windows\System32       216
0xcd094e452ab0  \Windows        216
0xcd094e452c40  \Windows\SysWOW64\AudioSes.dll  216
0xcd094e452dd0  \Windows\SysWOW64\winnsi.dll    216
0xcd094e4530f0  \Windows\SysWOW64\dinput8.dll   216
0xcd094e453280  \Windows\SysWOW64\drvstore.dll  216
0xcd094e453410  \Windows\SysWOW64\schannel.dll  216
0xcd094e453730  \Windows\SysWOW64\netapi32.dll  216
0xcd094e4538c0  \Windows\SysWOW64\netutils.dll  216
0xcd094e453a50  \Windows\SysWOW64\msfeeds.dll   216
0xcd094e453d70  \Windows\SysWOW64\WindowsCodecs.dll     216
0xcd094e454090  \Windows\SysWOW64\Windows.Graphics.dll  216
0xcd094e454220  \Windows\SysWOW64\Windows.Media.Audio.dll       216
0xcd094e4543b0  \Windows\SysWOW64\Windows.Globalization.dll     216
0xcd094e454540  \Windows\SysWOW64\WindowsCodecsExt.dll  216
0xcd094e4549f0  \Windows\SysWOW64\Windows.UI.dll        216
0xcd094e454d10  \Windows\SysWOW64\Windows.Media.dll     216
0xcd094e454ea0  \Windows\SysWOW64\UIAutomationCore.dll  216
0xcd094e455350  \Windows\SysWOW64\Windows.Media.MediaControl.dll        216
0xcd094e4554e0  \Windows\SysWOW64\webservices.dll       216
0xcd094e455670  \Windows\SysWOW64\mfmp4srcsnk.dll       216
0xcd094e455800  \Windows\SysWOW64\winmmbase.dll 216
0xcd094e455990  \Windows\SysWOW64\MFMediaEngine.dll     216
0xcd094e455b20  \Windows\SysWOW64\FirewallAPI.dll       216
0xcd094e455cb0
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258840021321
078.txt.WNCRYT      216
0xcd094e455e40  \Windows\SysWOW64\PhotoMetadataHandler.dll      216
0xcd094e456160  \Windows\SysWOW64\d3d10warp.dll 216
0xcd094e4562f0  \Windows\SysWOW64\Windows.Networking.Connectivity.dll   216
0xcd094e456480  \Windows\SystemResources\TextInput\TextInput.pri        216
0xcd094e456610  \$Directory     216
0xcd094e4567a0  \Windows\SysWOW64\ncryptsslp.dll        216
0xcd094e456930  \Windows\SysWOW64\edgehtml.dll  216
0xcd094e456ac0  \Windows\SysWOW64\UIAnimation.dll       216
0xcd094e456c50  \Windows\SysWOW64\Windows.UI.Xaml.dll   216
0xcd094e4575b0  \Windows\System32\PlaySndSrv.dll        216
0xcd094e457a60  \Program Files (x86)\Google\Update\1.3.36.152\goopdate.dll      216
0xcd094e457bf0  \Windows\SysWOW64\IPHLPAPI.DLL  216
0xcd094e4580a0
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258835190811
211.txt.WNCRYT      216
0xcd094e4583c0  \Windows\Registration\R000000000006.clb 216
0xcd094e4586e0  \$Directory     216
0xcd094e458870  \Windows\SysWOW64\version.dll   216
0xcd094e458a00  \Windows\SysWOW64\userenv.dll   216
0xcd094e458b90  \Windows\System32\MsCtfMonitor.dll      216
0xcd094e458d20  \Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.18362.418_none_2e73e95e27897f63\comctl32.dll     216
0xcd094e4591d0  \$Directory     216
0xcd094e4599a0  \$Directory     216
0xcd094e459b30  \Program Files (x86)\Google\Update\GoogleUpdate.exe     216
0xcd094e45a170  \Windows\SysWOW64\msimg32.dll   216
```

```
0xcd094e45a300  \Windows\SysWOW64\uxtheme.dll   216
0xcd094e45a490  \Windows\System32\oleaccrc.dll  216
0xcd094e45a620  \Windows\SysWOW64\cscapi.dll    216
0xcd094e45a7b0  \Windows\SysWOW64\ntmarta.dll   216
0xcd094e45b110  \Windows\SysWOW64\dsreg.dll     216
0xcd094e45b8e0  \Windows\SysWOW64\dbgcore.dll   216
0xcd094e45ba70  \Windows\System32\svchost.exe   216
0xcd094e45bd90  \Windows\System32       216
0xcd094e45c0b0  \Windows\SysWOW64\winhttp.dll   216
0xcd094e45c560  \Windows\System32\en-US\wer.dll.mui     216
0xcd094e45c6f0  \Windows\SysWOW64\ncrypt.dll    216
0xcd094e45c880  \Windows\System32\en-US\svchost.exe.mui 216
0xcd094e45ca10  \Windows\System32\cdpsvc.dll    216
0xcd094e45cd30  \Windows\SysWOW64\ntasn1.dll    216
0xcd094e45e180  \Windows\Registration\R000000000006.clb 216
0xcd094e45e310  \Windows\System32\ShareHost.dll 216
0xcd094e45e4a0  \Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.18362.418_none_2a23d356466d526c       216
0xcd094e45e630  \CMApi  216
0xcd094e45e7c0  \Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.18362.418_none_2a23d356466d526c\comctl32.dll  216
0xcd094e45eae0  \Windows\System32\Windows.Networking.Connectivity.dll   216
0xcd094e45ec70  \Windows\System32\en-US\ole32.dll.mui   216
0xcd094e45f440  \Endpoint       216
0xcd094e45f760  \Windows\System32\en-US\crypt32.dll.mui 216
0xcd094e45f8f0  \Windows\Fonts\micross.ttf      216
0xcd094e460250  \Windows\Fonts\segoeuisl.ttf    216
0xcd094e460570  \Endpoint       216
0xcd094e460700  \Program Files (x86)\Microsoft\EdgeUpdate\1.3.173.45\msedgeupdateres_en.dll     216
0xcd094e460890  \Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe       216
0xcd094e460a20  \Endpoint       216
0xcd094e460bb0  \CMNotify       216
0xcd094e460ed0  \Windows\System32\msutb.dll     216
0xcd094e461380  \Windows\System32\shdocvw.dll   216
0xcd094e461510  \CMNotify       216
0xcd094e461ce0  \$Directory     216
0xcd094e461e70  \Windows\System32\mlang.dll     216
0xcd094e462190  \$Directory     216
0xcd094e462640  \Endpoint       216
0xcd094e462e10  \CMApi  216
0xcd094e463450  \$Directory     216
0xcd094e4635e0  \Program Files (x86)\Google\Update\GoogleUpdate.exe     216
0xcd094e463770  \$Directory     216
0xcd094e463c20  \Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.18362.418_none_2e73e95e27897f63
216
0xcd094e464260  \Windows\SysWOW64\winsta.dll    216
0xcd094e4648a0  \Windows\System32\en-US\svchost.exe.mui 216
0xcd094e464a30  \ProgramData\Microsoft\EdgeUpdate\Log\MicrosoftEdgeUpdate.log   216
0xcd094e464bc0  \Program Files (x86)\Microsoft\EdgeUpdate\1.3.173.45\msedgeupdate.dll   216
0xcd094e464d50  \Windows\Registration\R000000000006.clb 216
0xcd094e465200  \Windows\System32\wlidprov.dll  216
0xcd094e465390  \Windows        216
0xcd094e465520  \Windows\System32\edputil.dll   216
0xcd094e4656b0  \Program Files (x86)\Google\Update\1.3.36.152   216
0xcd094e4659d0  \Windows\SysWOW64\iertutil.dll  216
0xcd094e465cf0  \Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe       216
0xcd094e465e80  \Program Files (x86)\Microsoft\EdgeUpdate\1.3.173.45    216
0xcd094e4661a0  \ProgramData\Microsoft\EdgeUpdate\Log\MicrosoftEdgeUpdate.log   216
0xcd094e466330  \Windows\SysWOW64\apphelp.dll   216
0xcd094e4664c0  \Windows\SysWOW64\taskschd.dll  216
0xcd094e4667e0  \$Directory     216
0xcd094e466e20  \Windows\System32\cryptsp.dll   216
0xcd094e467140  \CMApi  216
0xcd094e4672d0  \Windows\SysWOW64\atlthunk.dll  216
0xcd094e467910  \Windows\System32\en-US\MsCtfMonitor.dll.mui    216
0xcd094e467aa0  \Windows\SysWOW64\dhcpcsvc.dll  216
```

```
0xcd094e467c30  \Windows\System32\svchost.exe   216
0xcd094e4680e0  \Windows\System32\QuietHours.dll        216
0xcd094e468270  \Windows\System32\dmxmlhelputils.dll    216
0xcd094e468720  \Windows\System32\en-US\svchost.exe.mui 216
0xcd094e4688b0  \Windows\Registration\R000000000006.clb 216
0xcd094e468a40  \Windows\System32\usosvc.dll    216
0xcd094e468ef0  \$Directory     216
0xcd094e4693a0  \$Directory     216
0xcd094e469850  \Windows\System32       216
0xcd094e469b70  \Windows\Registration\R000000000006.clb 216
0xcd094e469e90  \Windows\System32\kernel32.dll  216
0xcd094e46a1b0  \Windows\SysWOW64\webio.dll     216
0xcd094e46a340  \Windows\System32\win32u.dll    216
0xcd094e46a4d0  \Windows\System32\msvcp_win.dll 216
0xcd094e46a7f0  \Windows\System32\msvcrt.dll    216
0xcd094e46ab10  \Windows\System32\rpcrt4.dll    216
0xcd094e46aca0  \Windows\System32\ucrtbase.dll  216
0xcd094e46ae30  \Windows\System32\svchost.exe   216
0xcd094e46b2e0  \Windows\System32\SgrmBroker.exe        216
0xcd094e46b470  \Windows\System32\sechost.dll   216
0xcd094e46b790  \Windows\System32\advapi32.dll  216
0xcd094e46b920  \Windows\SysWOW64\dnsapi.dll    216
0xcd094e46bab0  \Windows\System32\umpdc.dll     216
0xcd094e46bdd0  \Windows\System32\powrprof.dll  216
0xcd094e46c5a0  \Windows\System32\combase.dll   216
0xcd094e46c8c0  \Windows        216
0xcd094e46d3b0  \Windows\System32\gdi32.dll     216
0xcd094e46d540  \Windows\SysWOW64\msxml6.dll    216
0xcd094e46d6d0  \Windows\System32       216
0xcd094e46dd10  \Windows\System32\svchost.exe   216
0xcd094e46dea0  \Windows\System32\en-US\wdmaud.drv.mui  216
0xcd094e46e350  \Windows\System32\cryptxml.dll  216
0xcd094e46e4e0  \Windows\System32\user32.dll    216
0xcd094e46e990  \Windows\System32\Windows.Security.Authentication.OnlineId.dll  216
0xcd094e46eb20  \Windows\System32\gdi32full.dll 216
0xcd094e46ecb0  \Windows\Fonts\seguisb.ttf      216
0xcd094e46f160  \Users\user\AppData\Local\Packages\InputApp_cw5n1h2txyewy\Settings\settings.dat 216
0xcd094e46f610  \Windows\System32\SgrmEnclave.dll       216
0xcd094e46f7a0  \Users\user\AppData\Local\Packages\InputApp_cw5n1h2txyewy\Settings\settings.dat.LOG1    216
0xcd094e46fac0  \Users\user\AppData\Local\Packages\InputApp_cw5n1h2txyewy\Settings\settings.dat.LOG2    216
0xcd094e470290  \Windows\System32\Windows.Security.Authentication.Web.Core.dll  216
0xcd094e470420  \Windows\System32\en-US\kernel32.dll.mui        216
0xcd094e470740  \Windows\System32\usocoreps.dll 216
0xcd094e470a60  \Windows\System32\InputService.dll      216
0xcd094e470bf0  \Windows\System32\en-US\svchost.exe.mui 216
0xcd094e470d80  \Windows\System32\en-US\MMDevAPI.dll.mui        216
0xcd094e4710a0  \Windows\System32\dmiso8601utils.dll    216
0xcd094e471550  \Windows\System32\wuapi.dll     216
0xcd094e4716e0  \Windows\System32\usoapi.dll    216
0xcd094e471b90  \Windows\System32\vbsapi.dll    216
0xcd094e471eb0  \Windows\System32\wwapi.dll     216
0xcd094e4721d0  \Windows\System32\SecurityCenterBroker.dll      216
0xcd094e472360  \Windows\System32\SearchIndexer.exe     216
0xcd094e4724f0  \Windows\Registration\R000000000006.clb 216
0xcd094e472680  \Windows\Registration\R000000000006.clb 216
0xcd094e4729a0  \Windows\System32\wscsvc.dll    216
0xcd094e472b30  \Windows\Registration\R000000000006.clb 216
0xcd094e472cc0  \Windows\System32       216
0xcd094e473170  \Windows\System32\en-US\ESENT.dll.mui   216
0xcd094e473620  \Windows\System32\en-US\SearchIndexer.exe.mui   216
0xcd094e473650  奿毛夆 奿毛夆   0
0xcd094e4737b0  \ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb     216
0xcd094e473940  \Program Files\Common Files\microsoft shared\ink\IpsPlugin.dll  216
0xcd094e473c60  \MsFteWds       216
0xcd094e474750  \ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.jfm     216
```

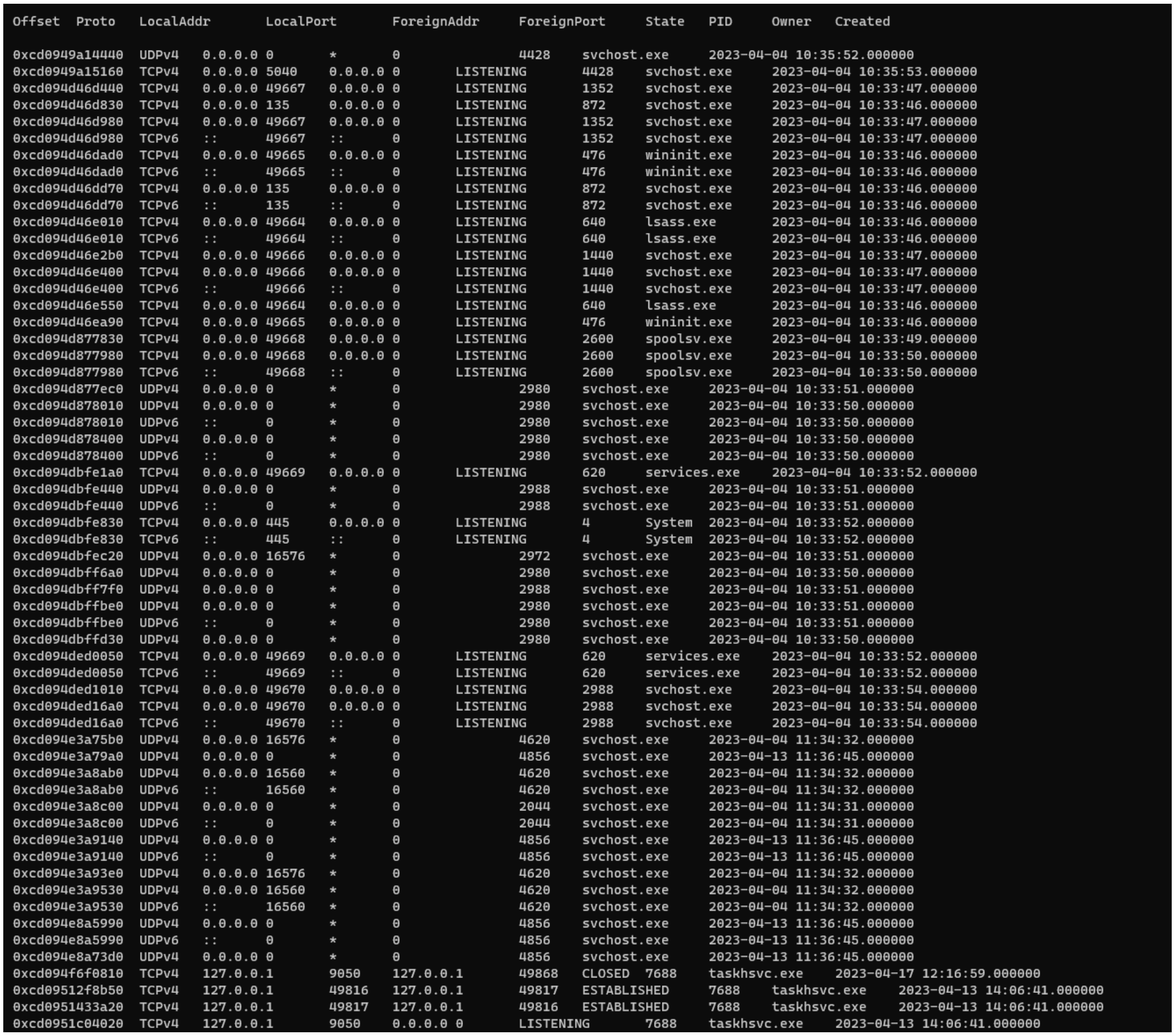
```
0xcd094e4750b0  \Windows\System32\mssrch.dll    216
0xcd094e475560  \Windows\Registration\R000000000006.clb 216
0xcd094e475880  \ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\PropMap\CiPT0000.000       216
0xcd094e475ba0  \ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb     216
0xcd094e475ec0  \$Directory     216
0xcd094e4761e0  \$Directory     216
0xcd094e476820  \ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\SecStore\CiST0000.000      216
0xcd094e4769b0  \Windows\System32\en-US\vsstrace.dll.mui        216
0xcd094e476b40  \Windows\System32\mssprxy.dll   216
0xcd094e476cd0  \Windows\SystemResources\tquery.dll.mun 216
0xcd094e477180  \$Directory     216
0xcd094e477310  \$Directory     216
0xcd094e477630  \CMNotify       216
0xcd094e4777c0  \$Directory     216
0xcd094e477ae0  \$Directory     216
0xcd094e477c70  \Windows\Fonts\StaticCache.dat  216
0xcd094e477e00  \CMNotify       216
0xcd094e478440  \CMNotify       216
0xcd094e4785d0  \$Directory     216
0xcd094e4788f0  \$Directory     216
0xcd094e478da0  \$Directory     216
0xcd094e4790c0  \$Directory     216
0xcd094e479250  \CMApi  216
0xcd094e479570  \$Directory     216
0xcd094e479700  \Windows\System32\DesktopShellExt.dll   216
0xcd094e479a20  \Windows\System32\TextInputMethodFormatter.dll  216
0xcd094e479d40  \CMApi  216
0xcd094e479ed0  \Windows\Fonts\StaticCache.dat  216
0xcd094e47a830  \Windows\System32\daxexec.dll   216
0xcd094e47ab50  \Windows\System32\CoreShellExtFramework.dll     216
0xcd094e47b320  \Windows\System32\en-US\oleaccrc.dll.mui        216
0xcd094e47b640  \$Directory     216
0xcd094e47b7d0  \Windows\System32\container.dll 216
0xcd094e47b960  \$Directory     216
0xcd094e47be10  \CMNotify       216
0xcd094e47c450  \$Directory     216
0xcd094e47c900  \Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4FirewallDiagnostics.evtx
216
0xcd094e47ca90  \Windows\System32\TaskSchdPS.dll        216
0xcd094e47cc20  \Windows\System32\cldapi.dll    216
0xcd094e47cdb0  \Program Files\VMware\VMware Tools\plugins\vmusr\desktopEvents.dll      216
0xcd094e47d3f0  \Windows\System32\vaultcli.dll  216
0xcd094e47d710  \Windows\Registration\R000000000006.clb 216
0xcd094e47da30  \$Directory     216
0xcd094e47dee0  \Windows\Fonts\StaticCache.dat  216
0xcd094e47e200  \Windows\System32\NPSM.dll      216
0xcd094e47e840  \$Directory     216
0xcd094e47eb60  \Windows\Prefetch\DLLHOST.EXE-4B6CB38A.pf       216
0xcd094e47f1a0  \Windows\System32       216
0xcd094e47f7e0  \Users\user\AppData\Local\Microsoft\GameDVR\KnownGameList.bin   216
0xcd094e480460  \Windows\System32\configmanager2.dll    216
0xcd094e4805f0  \$Directory     216
0xcd094e480910  \$Directory     216
0xcd094e481400  \Windows\appcompat\Programs\Amcache.hve 216
0xcd094e4818b0  \$Directory     216
0xcd094e481a40
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258836267911
022.txt.WNCRYT      216
0xcd094e481d60  \$Directory     216
0xcd094e481ef0
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258836567849
020.txt.WNCRYT      216
0xcd094e482210  \$Directory     216
0xcd094e4823a0  \Windows\System32\dllhost.exe   216
0xcd094e482530  \CMNotify       216
```

```
0xcd094e482e90
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258846921257
431.txt.WNCRYT      216
0xcd094e4834d0  \Users\user\AppData\Local\Microsoft\Internet Explorer\CacheStorage\edb.log      216
0xcd094e483980  \Windows\System32       216
0xcd094e802370  \Windows\SystemResources\imageres.dll.mun       216
0xcd094e802500
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258932715519
572.txt.WNCRYT      216
0xcd094e802690
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133258933015655
565.txt.WNCRYT      216
0xcd094e8029b0  \Windows\System32\OneCoreCommonProxyStub.dll    216
0xcd094e802e60  \Windows\System32\dsrole.dll    216
0xcd094e803180  \Windows\System32\sppobjs.dll   216
0xcd094e803310  \CMApi  216
0xcd094e803630  \Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-manifest-signed.xrm-ms       216
0xcd094e8037c0  \Windows\System32\Dism\DismProv.dll     216
0xcd094e803950  \Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-manifest-signed.xrm-ms 216
0xcd094e803ae0  \Windows\Microsoft.NET\Framework64\v4.0.30319\WMINet_Utils.dll  216
0xcd094e8042b0  \Windows\System32\SecurityHealthHost.exe        216
0xcd094e804440  \Windows\System32\SessEnv.dll   216
0xcd094e804760
\Users\user\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\e353de90c46ecf50.automaticDestinations-ms       216
0xcd094e8048f0  \Windows\System32       216
0xcd094e804a80  \Windows\System32\AssignedAccessManager.dll     216
0xcd094e804da0  \$Directory     216
0xcd094e8050c0  \Windows\System32\Clipc.dll     216
0xcd094e805250  \Windows\System32\Speech_OneCore\common\sapi_onecore.dll        216
0xcd094e8053e0  \Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat{5c5a2f65-b67b-11ed-a14d-
000c2955f605}.TMContainer00000000000000000002.regtrans-ms  216
0xcd094e805570  \Device\HarddiskVolume3\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat{5c5a2f65-b67b-11ed-a14d-
000c2955f605}.TM    216
0xcd094e805700  \Users\user\NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TMContainer00000000000000000001.regtrans-ms   216
0xcd094e805890  \$Directory     216
0xcd094e805a20  \Windows\System32\Windows.CloudStore.dll        216
0xcd094e805bb0  \Windows\System32\en-US\KernelBase.dll.mui      216
0xcd094e805d40  \Windows\System32\duser.dll     216
0xcd094e805ed0  \$Directory     216
0xcd094e806380  \Users\user\NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TM.blf     216
0xcd094e806510  \Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2   216
0xcd094e806830  \Device\HarddiskVolume3\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat{5c5a2f65-b67b-11ed-a14d-
000c2955f605}.TM    216
0xcd094e806ce0  \$Directory     216
0xcd094e807190  \Device\HarddiskVolume3\Users\user\NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TM  216
0xcd094e807320  \Users\user\NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TMContainer00000000000000000002.regtrans-ms   216
0xcd094e807640  \Device\HarddiskVolume3\Users\user\NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TM  216
0xcd094e8077d0  \Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat{5c5a2f65-b67b-11ed-a14d-000c2955f605}.TM.blf   216
0xcd094e807960  \Windows\Registration\R000000000006.clb 216
0xcd094e807af0  \Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat        216
0xcd094e807c80  \Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1   216
0xcd094e807e10  \Users\user\ntuser.dat.LOG2     216
0xcd094e808130  \Users\user\NTUSER.DAT  216
0xcd094e8082c0  \Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat{5c5a2f65-b67b-11ed-a14d-
000c2955f605}.TMContainer00000000000000000001.regtrans-ms  216
0xcd094e808450  \Users\user\ntuser.dat.LOG1     216
0xcd094e8085e0  \Windows\System32\sihost.exe    216
0xcd094e808770  \Windows\System32\QuickActionsDataModel.dll     216
0xcd094e808c20  \Windows\System32\SettingSync.dll       216
0xcd094e8090d0  \Windows\System32\AppxAllUserStore.dll  216
0xcd094e809260  \Windows\System32\mfc42.dll     216
0xcd094e8093f0  \Windows\System32\en-US\winsrv.dll.mui  216
0xcd094e809580  \CMNotify       216
0xcd094e809710  \Windows\System32       216
0xcd094e8098a0  \Windows\System32\spp\store\2.0\cache\cache.dat 216
0xcd094e809a30  \Windows\System32\svchost.exe   216
```

```
0xcd094e809bc0  \Windows\System32\cdpusersvc.dll        216
0xcd094e809d50  \$Directory     216
0xcd094e80a200  \Windows\System32\en-US\KernelBase.dll.mui      216
0xcd094e80a390  \Windows\System32\en-US\lsm.dll.mui     216
0xcd094e80a520  \Windows\System32\en-US\user32.dll.mui  216
0xcd094e80a6b0  \Windows\System32       216
0xcd094e80a840  \Windows\ShellExperiences\Windows.UI.ActionCenter.dll   216
0xcd094e80a9d0  \CMApi  216
0xcd094e80ab60  \Windows\System32\en-US\windows.storage.dll.mui 216
0xcd094e80acf0  \Windows\System32\spp\store\2.0\tokens.dat      216
0xcd094e80ae80  \Windows\Temp\vmware-vmusr-user.log     216
0xcd094e80b1a0  \Windows\System32\en-US\svchost.exe.mui 216
0xcd094e80b4c0  \Windows\Registration\R000000000006.clb 216
0xcd094e80b650  \Windows\System32\shacctprofile.dll     216
0xcd094e80b7e0  \Windows\System32\wwapi.dll     216
0xcd094e80b970  \Program Files\VMware\VMware Tools\plugins\vmusr\unity.dll      216
0xcd094e80bb00  \Program Files\VMware\VMware Tools\glibmm-2.4.dll       216
0xcd094e80c140  \Program Files\VMware\VMware Tools\sigc-2.0.dll 216
0xcd094e80c2d0  \Windows\System32\enrollmentapi.dll     216
0xcd094e80c460  \Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.18362.418_none_2a23d356466d526c       216
0xcd094e80c5f0  \Windows\System32\mfc140enu.dll 216
0xcd094e80c780  \Windows\Registration\R000000000006.clb 216
0xcd094e80c910  \Windows\System32\Microsoft.Bluetooth.Proxy.dll 216
0xcd094e80caa0  \Windows\System32\svchost.exe   216
0xcd094e80cc30  \Windows\System32\NotificationController.dll    216
0xcd094e80cdc0  \CMApi  216
0xcd094e80d0e0  \Program Files\VMware\VMware Tools\plugins\vmusr\dndcp.dll      216
0xcd094e80d270  \Windows\System32\webservices.dll       216
0xcd094e80d400  \Program Files\VMware\VMware Tools\plugins\vmusr\vmtray.dll     216
0xcd094e80d590  \Windows\System32\mfc140u.dll   216
0xcd094e80da40  \Windows\System32\ExecModelClient.dll   216
0xcd094e80dbd0  \Windows\System32\cryptxml.dll  216
0xcd094e80dd60  \Windows\System32\das.dll       216
0xcd094e80def0  \Windows\Registration\R000000000006.clb 216
0xcd094e80e080  \Windows\System32       216
0xcd094e80e210  \Windows\System32\deviceaccess.dll      216
0xcd094e80e3a0  \Windows\System32\xmllite.dll   216
0xcd094e80e530  \Windows\System32\WpnUserService.dll    216
0xcd094e80e6c0  \Windows\Registration\R000000000006.clb 216
0xcd094e80e850  \$Directory     216
0xcd094e80e9e0  \Windows\System32\ActivationManager.dll 216
0xcd094e80eb70  \Windows\System32\omadmapi.dll  216
0xcd094e80ed00  \Windows\System32\iri.dll       216
0xcd094e80ee90  \Windows\System32\tokenbinding.dll      216
0xcd094e80f1b0  \Windows\System32       216
0xcd094e80f340  \Windows\System32\en-US\svchost.exe.mui 216
0xcd094e80f4d0  \Program Files\VMware\VMware Tools\VMToolsHook64.dll    216
0xcd094e80f660  \Windows\Prefetch\PfPre_9e476548.mkd    216
0xcd094e80f7f0  \Windows\System32\en-US\cmd.exe.mui     216
0xcd094e80f980  \Windows\System32\dataclen.dll  216
0xcd094e80fca0  \Windows\System32\AppointmentActivation.dll     216
0xcd094e80fe30  \Windows\System32\TokenBroker.dll       216
0xcd094e810150  \Windows\System32\enterprisecsps.dll    216
0xcd094e8102e0  \Program Files\VMware\VMware Tools\suspend-vm-default.bat       216
0xcd094e810470  \Windows\System32\ClipboardServer.dll   216
0xcd094e810790  \Windows\System32\dmenterprisediagnostics.dll   216
0xcd094e810920  \Windows\System32\TabSvc.dll    216
0xcd094e810ab0  \Windows\System32\dui70.dll     216
0xcd094e810c40  \Windows\System32\modernexecserver.dll  216
0xcd094e810dd0  \Windows\System32\AppResolver.dll       216
0xcd094e811410  \$Directory     216
0xcd094e8115a0  \Windows\System32\WindowManagement.dll  216
0xcd094e811730  \$Directory     216
0xcd094e8118c0  \Windows\System32\en-US\taskhostw.exe.mui       216
0xcd094e811a50  \Windows\System32\Windows.StateRepositoryClient.dll     216
```

```
0xcd094e811be0  \$Directory    216
0xcd094e811d70  \$Directory    216
0xcd094e812090  \Windows\System32\en-US\ctfmon.exe.mui  216
0xcd094e812220  \Windows\System32\ctfmon.exe   216
0xcd094e8123b0  \Windows\Fonts\segoeuib.ttf    216
0xcd094e812540  \Windows\System32\CertEnroll.dll       216
0xcd094e8126d0  \CMApi  216
0xcd094e812860  \Windows\System32      216
0xcd094e8129f0  \Windows\System32\en-US\slui.exe.mui   216
0xcd094e812b80  \Users\user\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db       216
0xcd094e812d10  \Windows\System32\certca.dll   216
0xcd094e812ea0  \$Directory    216
0xcd094e8131c0  \Windows\System32\notificationplatformcomponent.dll     216
0xcd094e813350  \CMApi  216
0xcd094e8134e0  \Windows\System32\taskhostw.exe 216
0xcd094e813670  \Windows\System32\slwga.dll     216
0xcd094e813800  \Users\user\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db-shm   216
0xcd094e813990  \Windows\System32\AppContracts.dll     216
0xcd094e813cb0  \Users\user\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db-wal   216
0xcd094e813e40  \$Directory    216
0xcd094e814160  \Users\user\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat   216
0xcd094e8142f0  \Program Files\Eclipse Adoptium\jdk-11.0.18.10-hotspot\bin\java.exe     216
0xcd094e814480  \Windows\System32\en-US\KernelBase.dll.mui     216
0xcd094e814610  \Users\user\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db       216
0xcd094e8147a0  \$Directory    216
0xcd094e814930
\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creati
ves\314559\1677459842      216
0xcd094e814ac0  \$Directory    216
0xcd094e814c50  \CMNotify      216
0xcd094e814de0  \Windows\System32\C_1256.NLS   216
0xcd094e815100  \Windows\System32\BackgroundMediaPolicy.dll    216
0xcd094e815290  \Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4Operational.evtx  216
0xcd094e815420
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133259435822129
572.txt.WNCRYT      216
0xcd094e8155b0  \Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4BackUpKeySvc.evtx 216
0xcd094e815740
\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creati
ves\280811\1677463469      216
0xcd094e8158d0  \Windows\System32\C_1250.NLS   216
0xcd094e815a60  \Windows\System32\Windows.Networking.BackgroundTransfer.BackgroundManagerPolicy.dll     216
0xcd094e815bf0  \$Directory    216
0xcd094e815d80  \Windows\System32\en-US\combase.dll.mui 216
0xcd094e8160a0  \Windows\System32\C_1251.NLS   216
0xcd094e8163c0  \Windows\System32\C_1254.NLS   216
0xcd094e816550  \Windows\System32\C_1253.NLS   216
0xcd094e8166e0  \Windows\System32\winevt\Logs\Microsoft-Windows-CloudStore%4Operational.evtx   216
0xcd094e816870  \Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync%4Operational.evtx   216
0xcd094e816a00  \Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync%4Debug.evtx 216
0xcd094e816b90  \Windows\System32\twinui.appcore.dll   216
0xcd094e816d20  \CMNotify      216
0xcd094e816eb0  \Windows\System32\SmartCardBackgroundPolicy.dll 216
0xcd094e8171d0  \Windows\System32\Windows.System.Launcher.dll   216
0xcd094e817360  \Windows\System32\en-US\winmm.dll.mui   216
0xcd094e8174f0  \Windows\System32\SebBackgroundManagerPolicy.dll       216
0xcd094e817680  \Windows\System32\PackageStateChangeHandler.dll 216
0xcd094e817810  \Windows\System32\InputLocaleManager.dll       216
0xcd094e8179a0  \Windows\System32\ACPBackgroundManagerPolicy.dll       216
0xcd094e817b30  \Windows\System32\Microsoft.Bluetooth.UserService.dll   216
0xcd094e817e50  \Windows\System32\TileDataRepository.dll       216
0xcd094e818170  \Windows\System32\radardt.dll   216
0xcd094e818300
\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133259435106292
286.txt.WNCRYT      21
```

NetScan



```
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xcd0949a14440  UDPv4   0.0.0.0 0       *       0               4428    svchost.exe     2023-04-04 10:35:52.000000
0xcd0949a15160  TCPv4   0.0.0.0 5040    0.0.0.0 0       LISTENING       4428    svchost.exe     2023-04-04 10:35:53.000000
0xcd094d46d440  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1352    svchost.exe     2023-04-04 10:33:47.000000
0xcd094d46d830  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       872     svchost.exe     2023-04-04 10:33:46.000000
0xcd094d46d980  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1352    svchost.exe     2023-04-04 10:33:47.000000
0xcd094d46d980  TCPv6   ::      49667   ::      0       LISTENING       1352    svchost.exe     2023-04-04 10:33:47.000000
0xcd094d46dad0  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       476     wininit.exe     2023-04-04 10:33:46.000000
0xcd094d46dad0  TCPv6   ::      49665   ::      0       LISTENING       476     wininit.exe     2023-04-04 10:33:46.000000
0xcd094d46dd70  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       872     svchost.exe     2023-04-04 10:33:46.000000
0xcd094d46dd70  TCPv6   ::      135     ::      0       LISTENING       872     svchost.exe     2023-04-04 10:33:46.000000
0xcd094d46e010  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       640     lsass.exe       2023-04-04 10:33:46.000000
0xcd094d46e010  TCPv6   ::      49664   ::      0       LISTENING       640     lsass.exe       2023-04-04 10:33:46.000000
0xcd094d46e2b0  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1440    svchost.exe     2023-04-04 10:33:47.000000
0xcd094d46e400  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1440    svchost.exe     2023-04-04 10:33:47.000000
0xcd094d46e400  TCPv6   ::      49666   ::      0       LISTENING       1440    svchost.exe     2023-04-04 10:33:47.000000
0xcd094d46e550  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       640     lsass.exe       2023-04-04 10:33:46.000000
0xcd094d46ea90  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       476     wininit.exe     2023-04-04 10:33:46.000000
0xcd094d877830  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2600    spoolsv.exe     2023-04-04 10:33:49.000000
0xcd094d877980  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2600    spoolsv.exe     2023-04-04 10:33:50.000000
0xcd094d877980  TCPv6   ::      49668   ::      0       LISTENING       2600    spoolsv.exe     2023-04-04 10:33:50.000000
0xcd094d877ec0  UDPv4   0.0.0.0 0       *       0               2980    svchost.exe     2023-04-04 10:33:51.000000
0xcd094d878010  UDPv4   0.0.0.0 0       *       0               2980    svchost.exe     2023-04-04 10:33:50.000000
0xcd094d878010  UDPv6   ::      0       *       0               2980    svchost.exe     2023-04-04 10:33:50.000000
0xcd094d878400  UDPv4   0.0.0.0 0       *       0               2980    svchost.exe     2023-04-04 10:33:50.000000
0xcd094d878400  UDPv6   ::      0       *       0               2980    svchost.exe     2023-04-04 10:33:50.000000
0xcd094dbfe1a0  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       620     services.exe    2023-04-04 10:33:52.000000
0xcd094dbfe440  UDPv4   0.0.0.0 0       *       0               2988    svchost.exe     2023-04-04 10:33:51.000000
0xcd094dbfe440  UDPv6   ::      0       *       0               2988    svchost.exe     2023-04-04 10:33:51.000000
0xcd094dbfe830  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2023-04-04 10:33:52.000000
0xcd094dbfe830  TCPv6   ::      445     ::      0       LISTENING       4       System  2023-04-04 10:33:52.000000
0xcd094dbfec20  UDPv4   0.0.0.0 16576   *       0               2972    svchost.exe     2023-04-04 10:33:51.000000
0xcd094dbff6a0  UDPv4   0.0.0.0 0       *       0               2980    svchost.exe     2023-04-04 10:33:50.000000
0xcd094dbff7f0  UDPv4   0.0.0.0 0       *       0               2988    svchost.exe     2023-04-04 10:33:51.000000
0xcd094dbffbe0  UDPv4   0.0.0.0 0       *       0               2980    svchost.exe     2023-04-04 10:33:51.000000
0xcd094dbffbe0  UDPv6   ::      0       *       0               2980    svchost.exe     2023-04-04 10:33:51.000000
0xcd094dbffd30  UDPv4   0.0.0.0 0       *       0               2980    svchost.exe     2023-04-04 10:33:50.000000
0xcd094ded0050  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       620     services.exe    2023-04-04 10:33:52.000000
0xcd094ded0050  TCPv6   ::      49669   ::      0       LISTENING       620     services.exe    2023-04-04 10:33:52.000000
0xcd094ded1010  TCPv4   0.0.0.0 49670   0.0.0.0 0       LISTENING       2988    svchost.exe     2023-04-04 10:33:54.000000
0xcd094ded16a0  TCPv4   0.0.0.0 49670   0.0.0.0 0       LISTENING       2988    svchost.exe     2023-04-04 10:33:54.000000
0xcd094ded16a0  TCPv6   ::      49670   ::      0       LISTENING       2988    svchost.exe     2023-04-04 10:33:54.000000
0xcd094e3a75b0  UDPv4   0.0.0.0 16576   *       0               4620    svchost.exe     2023-04-04 11:34:32.000000
0xcd094e3a79a0  UDPv4   0.0.0.0 0       *       0               4856    svchost.exe     2023-04-13 11:36:45.000000
0xcd094e3a8ab0  UDPv4   0.0.0.0 16560   *       0               4620    svchost.exe     2023-04-04 11:34:32.000000
0xcd094e3a8ab0  UDPv6   ::      16560   *       0               4620    svchost.exe     2023-04-04 11:34:32.000000
0xcd094e3a8c00  UDPv4   0.0.0.0 0       *       0               2044    svchost.exe     2023-04-04 11:34:31.000000
0xcd094e3a8c00  UDPv6   ::      0       *       0               2044    svchost.exe     2023-04-04 11:34:31.000000
0xcd094e3a9140  UDPv4   0.0.0.0 0       *       0               4856    svchost.exe     2023-04-13 11:36:45.000000
0xcd094e3a9140  UDPv6   ::      0       *       0               4856    svchost.exe     2023-04-13 11:36:45.000000
0xcd094e3a93e0  UDPv4   0.0.0.0 16576   *       0               4620    svchost.exe     2023-04-04 11:34:32.000000
0xcd094e3a9530  UDPv4   0.0.0.0 16560   *       0               4620    svchost.exe     2023-04-04 11:34:32.000000
0xcd094e3a9530  UDPv6   ::      16560   *       0               4620    svchost.exe     2023-04-04 11:34:32.000000
0xcd094e8a5990  UDPv4   0.0.0.0 0       *       0               4856    svchost.exe     2023-04-13 11:36:45.000000
0xcd094e8a5990  UDPv6   ::      0       *       0               4856    svchost.exe     2023-04-13 11:36:45.000000
0xcd094e8a73d0  UDPv4   0.0.0.0 0       *       0               4856    svchost.exe     2023-04-13 11:36:45.000000
0xcd094f6f0810  TCPv4   127.0.0.1       9050    127.0.0.1       49868   CLOSED  7688    taskhsvc.exe    2023-04-17 12:16:59.000000
0xcd09512f8b50  TCPv4   127.0.0.1       49816   127.0.0.1       49817   ESTABLISHED     7688    taskhsvc.exe    2023-04-13 14:06:41.000000
0xcd0951433a20  TCPv4   127.0.0.1       49817   127.0.0.1       49816   ESTABLISHED     7688    taskhsvc.exe    2023-04-13 14:06:41.000000
0xcd0951c04020  TCPv4   127.0.0.1       9050    0.0.0.0 0       LISTENING       7688    taskhsvc.exe    2023-04-13 14:06:41.000000
```

Registry Keys

```
        Volatility 3 Framework 2.0.1
Progress:  100.00       PDB scanning finished
Last Write Time Hive Offset     Type    Key     Name    Data    Volatile

2023-04-04 10:33:31.000000      0xa8892820e000  Key     [NONAME]        A       False
2023-04-04 10:33:31.000000      0xa8892820e000  Key     [NONAME]        MACHINE         False
2023-04-04 10:33:31.000000      0xa8892820e000  Key     [NONAME]        USER            False
2023-04-04 10:33:31.000000      0xa8892820e000  Key     [NONAME]        WC              False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        ActivationBroker                False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        ControlSet001           False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        DriverDatabase          False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        HardwareConfig          False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        Input           False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        Keyboard Layout         False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        Maps            False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        MountedDevices          False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        ResourceManager         False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        ResourcePolicyStore             False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        RNG             False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        Select          False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        Setup           False
2023-04-04 10:33:31.000000      0xa8892824a000  Key     \REGISTRY\MACHINE\SYSTEM        Software                False
```

```
2023-04-04 10:33:31.000000    0xa8892824a000  Key    \REGISTRY\MACHINE\SYSTEM       State          False
2023-04-04 10:33:31.000000    0xa8892824a000  Key    \REGISTRY\MACHINE\SYSTEM       WaaS           False
2023-04-04 10:33:31.000000    0xa8892824a000  Key    \REGISTRY\MACHINE\SYSTEM       WPA            False
2023-04-04 10:33:31.000000    0xa8892824a000  Key    \REGISTRY\MACHINE\SYSTEM       CurrentControlSet            True
2023-04-04 10:33:32.000000    0xa889282a8000  Key    \REGISTRY\MACHINE\HARDWARE     ACPI           False
2023-04-04 10:33:32.000000    0xa889282a8000  Key    \REGISTRY\MACHINE\HARDWARE     DESCRIPTION           False
2023-04-04 10:33:32.000000    0xa889282a8000  Key    \REGISTRY\MACHINE\HARDWARE     DEVICEMAP            False
2023-04-04 10:33:32.000000    0xa889282a8000  Key    \REGISTRY\MACHINE\HARDWARE     RESOURCEMAP           True
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    7-Zip         False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    AutoHotkey           False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    Classes        False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    Clients        False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    CVSM           False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    Cygwin         False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    DefaultUserEnvironment         False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    Google         False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    Microsoft           False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    ODBC           False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    Oracle         False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    Policies             False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    RegisteredApplications         False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    VMware, Inc.          False
2023-02-27 23:59:25.000000    0xa88929766000  Key    \SystemRoot\System32\Config\SOFTWARE    WOW6432Node          False
2023-04-16 13:54:42.000000    0xa88929c61000  Key    \Device\HarddiskVolume1\EFI\Microsoft\Boot\BCD  Description           False
2023-04-16 13:54:42.000000    0xa88929c61000  Key    \Device\HarddiskVolume1\EFI\Microsoft\Boot\BCD  Objects        False
2023-02-27 01:57:16.000000    0xa88929cb9000  Key    \SystemRoot\System32\Config\DEFAULT     Console        False
2023-02-27 01:57:16.000000    0xa88929cb9000  Key    \SystemRoot\System32\Config\DEFAULT     Control Panel         False
2023-02-27 01:57:16.000000    0xa88929cb9000  Key    \SystemRoot\System32\Config\DEFAULT     Environment          False
2023-02-27 01:57:16.000000    0xa88929cb9000  Key    \SystemRoot\System32\Config\DEFAULT     EUDC          False
2023-02-27 01:57:16.000000    0xa88929cb9000  Key    \SystemRoot\System32\Config\DEFAULT     Keyboard Layout       False
2023-02-27 01:57:16.000000    0xa88929cb9000  Key    \SystemRoot\System32\Config\DEFAULT     Printers             False
2023-02-27 01:57:16.000000    0xa88929cb9000  Key    \SystemRoot\System32\Config\DEFAULT     Software             False
2023-02-27 01:57:16.000000    0xa88929cb9000  Key    \SystemRoot\System32\Config\DEFAULT     System         False
2023-04-04 10:33:45.000000    0xa88929d7f000  Key    \SystemRoot\System32\Config\SECURITY    Cache         False
2023-04-04 10:33:45.000000    0xa88929d7f000  Key    \SystemRoot\System32\Config\SECURITY    Policy        False
2023-04-04 10:33:45.000000    0xa88929d7f000  Key    \SystemRoot\System32\Config\SECURITY    RXACT         False
2023-04-04 10:33:45.000000    0xa88929d7f000  Key    \SystemRoot\System32\Config\SECURITY    SAM           True
2023-02-27 08:45:30.000000    0xa88929dac000  Key    \SystemRoot\System32\Config\SAM SAM           False
2023-02-27 08:45:31.000000    0xa88929ea2000  Key    \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT       AppEvents             False
2023-02-27 08:45:31.000000    0xa88929ea2000  Key    \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT       Console        False
2023-02-27 08:45:31.000000    0xa88929ea2000  Key    \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT       Control Panel        False
2023-02-27 08:45:31.000000    0xa88929ea2000  Key    \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT       Environment          False
2023-02-27 08:45:31.000000    0xa88929ea2000  Key    \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT       EUDC          False
2023-02-27 08:45:31.000000    0xa88929ea2000  Key    \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT       Keyboard Layout       False
2023-02-27 08:45:31.000000    0xa88929ea2000  Key    \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT       Network        False
2023-02-27 08:45:31.000000    0xa88929ea2000  Key    \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT       Software             False
2023-02-27 08:45:31.000000    0xa88929ea2000  Key    \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT       System         False
2023-02-27 08:45:39.000000    0xa88929c7a000  Key    \SystemRoot\System32\Config\BBI Events         False
2023-02-27 08:45:39.000000    0xa88929c7a000  Key    \SystemRoot\System32\Config\BBI WorkItems             False
2023-02-27 08:45:39.000000    0xa88929c7a000  REG_DWORD      \SystemRoot\System32\Config\BBI Version 2      False
2023-02-27 08:45:39.000000    0xa88929c7a000  REG_DWORD      \SystemRoot\System32\Config\BBI MinorVersion   2      False
2023-02-27 08:45:32.000000    0xa88929e90000  Key    \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  AppEvents            False
2023-02-27 08:45:32.000000    0xa88929e90000  Key    \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Console        False
2023-02-27 08:45:32.000000    0xa88929e90000  Key    \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Control Panel         False
2023-02-27 08:45:32.000000    0xa88929e90000  Key    \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Environment          False
2023-02-27 08:45:32.000000    0xa88929e90000  Key    \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  EUDC          False
2023-02-27 08:45:32.000000    0xa88929e90000  Key    \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Keyboard Layout       False
2023-02-27 08:45:32.000000    0xa88929e90000  Key    \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Network        False
2023-02-27 08:45:32.000000    0xa88929e90000  Key    \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Software             False
2023-02-27 08:45:32.000000    0xa88929e90000  Key    \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  System         False
2023-04-04 10:41:32.000000    0xa8892d35c000  Key    \??\C:\Users\user\ntuser.dat    AppEvents            False
2023-04-04 10:41:32.000000    0xa8892d35c000  Key    \??\C:\Users\user\ntuser.dat    Console        False
2023-04-04 10:41:32.000000    0xa8892d35c000  Key    \??\C:\Users\user\ntuser.dat    Control Panel         False
2023-04-04 10:41:32.000000    0xa8892d35c000  Key    \??\C:\Users\user\ntuser.dat    Environment          False
2023-04-04 10:41:32.000000    0xa8892d35c000  Key    \??\C:\Users\user\ntuser.dat    EUDC          False
2023-04-04 10:41:32.000000    0xa8892d35c000  Key    \??\C:\Users\user\ntuser.dat    Keyboard Layout       False
2023-04-04 10:41:32.000000    0xa8892d35c000  Key    \??\C:\Users\user\ntuser.dat    Network        False
2023-04-04 10:41:32.000000    0xa8892d35c000  Key    \??\C:\Users\user\ntuser.dat    Printers             False
2023-04-04 10:41:32.000000    0xa8892d35c000  Key    \??\C:\Users\user\ntuser.dat    Software             False
2023-04-04 10:41:32.000000    0xa8892d35c000  Key    \??\C:\Users\user\ntuser.dat    System         False
2023-04-04 10:41:32.000000    0xa8892d35c000  Key    \??\C:\Users\user\ntuser.dat    Volatile Environment          True
2023-04-17 12:00:55.000000    0xa889294b3000  Key    \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  *           False
2023-04-17 12:00:55.000000    0xa889294b3000  Key    \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .3fr          False
2023-04-17 12:00:55.000000    0xa889294b3000  Key    \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .3g2          False
2023-04-17 12:00:55.000000    0xa889294b3000  Key    \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .3gp          False
```

```
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .3gp2         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .3gpp         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .3mf          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .aac          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ac3          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .adt          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .adts         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .all          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .amr          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .appinstaller         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .appx         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .appxbundle           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ari          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .arw          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .asf          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .avi          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .avif         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .bay          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .bmp          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .c5e2524a-ea46-4f67-841f-
6a9465d9d515         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .cap          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .cr2          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .cr3          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .crw          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .dcr          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .dcs          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .dib          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .divx         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .dng          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .drf          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ec3          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .eip          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .eml          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .epub         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .erf          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .fbx          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .fff          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .fh           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .flac         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .gif          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .glb          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .GLTF         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .heic         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .heif         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .hif          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .htm          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .html         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ico          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ics          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .iiq          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .jfif         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .jpe          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .jpeg         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .jpg          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .jxr          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .k25          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .kdc          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .m1v          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .m2t          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .m2ts         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .m2v          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .m3u          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .m4a          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .m4r          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .m4v          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .md           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mdc          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .md_auto_file         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mef          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mka          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mkv          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mod          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mos          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mov          False
```

```
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mp2v          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mp3           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mp4           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mp4v          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mpa           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mpe           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mpeg          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mpg           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mpv2          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mrw           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ms-lockscreencomponent-primary
False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .msix          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .msixbundle            False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .mts           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .nef           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .nrw           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .obj           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .oga           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ogg           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ogm           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ogv           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ogx           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .one           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .onetoc2               False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .opus          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .orf           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ori           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .pdf           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .pef           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ply           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .PML           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .png           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .R3D           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .raf           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .raw           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .res           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .res_auto_file         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .rw2           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .rwl           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .rwz           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .solitairetheme8              False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .sr2           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .srf           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .srw           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .stl           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .svg           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .thumb         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .tif           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .tiff          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .tod           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .ts            False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .tts           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .vcf           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wav           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wdp           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .webm          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wm            False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wma           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wmv           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .WNCRY         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .WNCRY_auto_file              False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wnry          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wnry_auto_file        False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wpl           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .wrl           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .x3f           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .xvid          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  .zpl           False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  ActivatableClasses            False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  AppID          False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX0jr688mrddhm2gsn5y1q8jpx5tfsxk7s         False
2023-04-17 12:00:55.000000     0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX0t69n30jztar4a12pv0h1xh91e8jsacr         False
```

```
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX1apmywg4z9t3tk3nrn9y8ntjc5cg9675            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX2jm25qtmp2qxstv333wv5mne3k5bf4bm            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX3cx04417ybaf9kz7fem54fc937697n6k            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX3p914qnpgw4hwj856jw2y286v7d4qnzh            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX3xxs313wwkfjhythsb8q46xdsq8d2cvv            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX40nx3azkcssh7ybcbzzjpgf1mg561cyz            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX43hnxtbyyps62jhe9sqpdzxn1790zetc            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX47jwqdafzcxw9wm0mbb5cev2eav5b1je            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX4hxtad77fbk3jkkeerkrm0ze94wjf3s9            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX4j5v7692qeayhwcg2qhwgwbcdyrpwsc0            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX4jbzrhvphxte25e0gxha6bq555nrgqzy            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX69r31t6nmawqr1gdamcsndphj2v4a6cx            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX6efkedsh4s4yrd49cf5nmjaza776n10d            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX6hptmm8avg1gnv71j8jda9340qk79w89            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX7rm9drdg8sk7vqndwj3sdjw11x96jc0y            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX85jqyztr8fqc6b7sw64y2mjjrnx59njs            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX8mn6f6acw2d3hves535dpq0zqnxqkec7            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX90nv6nhay5n6a98fnetv7tpk64pp35es            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX9kvz3rdv8t7twanaezbwfcdgrbg3bck0            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX9rkaq77s0jzh1tyccadx9ghba15r6t3h            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppX9vwggs9kbe3mn0w816545e7zs1x6vegr            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXa4x21t18evxksm0kbe6znaz8jjrjvs9e            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXa5q0sm6rab4bbk8faqwhapj4mvw0n9ek            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXak1hygz1tpjjnxhr1pwtcgnkpr24r5e7            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXb6t8194632yvzp2fm989q0bfn7x48r84            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXbfem27ddbf6ebrx72mc6gnaw2e3nkpza            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXcb6e5re383zqpgggd2grt6vrv627a4wt            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXcdh38jxzbcberv50vxg2tg4k84kfnewn            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat  AppXd4nrz8ff68srnhf9t5a8sbjyar1cr723
False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXde74bfzw9j31bzhcvsrxsyjnhhbq66cs            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXdn5b0j699ka5fqvrr3pgjad0evqarm6d            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXdv25x4ndb8r51pbdf6srsknmbkfnkpaq            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXe05qdnx2p14g0mw29139zqs9s5n3wcne            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXe862j7twqs4aww05211jaakwxyfjx4da            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXe8d7fy32jcm7fkx8p2wzxa43pep36805            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXejqz5dpvfxzdkq7rwbwmnn4gyqk3hhb9            False
2023-04-17 12:00:55.000000      0xa889294b3000  Key     \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXf3k2nhftgnncnbzma7c7xf62tm3e4vv2            False
```

```
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXfp6kkvw8823ptbxvr2be691hzfyrsazt	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXfqdap54b29v3w265t548h0wzs1hqega7	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXg280tzrpxnd0t559h02gpd27tgrma246	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXgwsb7drvvkp7jxvqdqst0ajpq6107yzv	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXhhkhyqrpsdn2kgtvr6qf6att22kmtadz	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXk0g4vb8gvt7b93tg50ybcy892pge6jmt	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXnn90p29wc108haje7ahczjhc00h3p5sf	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXnyyfqebxgk8p4scs5cx21tngqn4hwcsq	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXnzh5v9w1s9pv2y889efv7t8bg0msmhca	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXp8e2ntvbtget7f2fw6qec3j54vhd14m4	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXpjsxda6f84877c5f65bm4q3g4qep2rxn	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXq0fevzme2pys62n3e0fbqa7peapykr8v	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXreyvazcs64j2pgtpwyt49g6ce85mwrwg	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXrrebmngeb0a7ggdd6sec1cq49468v8qr	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXsf0d8xs4xz53mhyq7wyajbmrskt080m7	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXtkjk7ve8gcvsz7s2y4kkf56wrmb5edr7	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXvepbp3z66accmsd0x877zbbxjctkpr6t	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXvsddybna5mfqpzfzrh0x2nnv0v7ettv3	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXvvwq6wxamf7qhxd0vn6wm1wwehyxrdd6	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXw3nvmqt363p060ea53qg33er1a0782a8	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXx6a0med6y43gv0vn6qa7r3vdg4cg3bnv	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXxfctf2rqj6c7b4wrvys6zq1bskprrn19	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
AppXzn6aajbcrxx2qvxjawp7v0xnj1zdzdcz	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	armodelviewing	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	bingmaps	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	bingweather	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	calculator	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	callto	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	CLSID	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	com.microsoft.3dviewer	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	com.microsoft.print3d	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	Directory	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	Extensions	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	feedback-hub	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	grvopen	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	http	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	https	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	IE.AssocFile.URL	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	insiderhub	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	Installer	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	Interface	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	JavaPlugin.113612	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	lnkfile	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	Local Settings	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	mailto	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoft-edge	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoft-edge-holographic
False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoft.windows.camera
False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoft.windows.camera.multipicker
False
```

```
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoft.windows.camera.picker
False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoft.windows.photos.crop
False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoft.windows.photos.picker
False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoft.windows.photos.search
False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoft.windows.photos.videoedit
False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoftmusic	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoftsolitairecollection	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	microsoftvideo	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	MIME	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-aad-brokerplugin	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-actioncenter	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-appinstaller	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-apprep	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-calculator	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-chat	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-clock	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-contact-support	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-cortana	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-cxh	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-default-location	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-device-enrollment	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-drive-to	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-edu-secureassessment	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-eyecontrolspeech	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-gamebar	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-gamebarservices	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-gamingoverlay	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-get-started	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-getoffice	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-holographicfirstrun	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-inputapp	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-insights	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-ipmessaging	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-mobileplans	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-officeapp	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-officecmd	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-oobenetwork	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-paint	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-penworkspace	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-people	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-phone	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-photos	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-playto-miracast	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-projection	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-screenclip	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-screensketch	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-search	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-sttoverlay	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-unistore-email	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-voip-call	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-voip-video	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-walk-to	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-wcrv	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-windows-store	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-windows-store-deskext
False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-windows-store2	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-wpc	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-wpdrmv	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-xbet-survey	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-xbl-3d8b930f	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ms-xgpueject	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	msnweather	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	mswindowsmusic	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	mswindowsvideo	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	onenote	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	onenote-cmd	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	outlookaccounts	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	outlookcal	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	outlookmail	False
```

```
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	PackagedCom	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	ProcMon.Logfile.1	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	read	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	skype	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	skype-meetnow	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	skypewin	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	sms	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	tel	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	TypeLib	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	windows-feedback	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	windowsdefender	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	WOW6432Node	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbls	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbox	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbox-arena	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbox-captures	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbox-friendfinder	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbox-gamehub	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbox-lfg	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbox-network	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbox-profile	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbox-settings	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbox-store	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xbox-tcui	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xboxgames	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xboxliveapp-1297287741	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	xboxmusic	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	zune	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	s☻	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	rÓ\☻s4	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	sÓ]☻s5	False
2023-04-17 12:00:55.000000	0xa889294b3000	Key	\??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat	uÓS☻	False
2023-02-27 08:45:52.000000	0xa8892e603000	Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.StartMenuExperienceHost_10.0.18362.387_neutral_neutral_cw5n1h2txyewy\
ActivationStore.dat	ActivatableClassId	False
2023-02-27 08:45:52.000000	0xa8892e603000	Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.StartMenuExperienceHost_10.0.18362.387_neutral_neutral_cw5n1h2txyewy\
ActivationStore.dat	Server	False
2012-05-22 00:00:08.000000	0xa8892e631000	Key
\??\C:\Users\user\AppData\Local\Packages\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\Settings\settings.dat	LocalState	False
2012-05-22 00:00:08.000000	0xa8892e631000	Key
\??\C:\Users\user\AppData\Local\Packages\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\Settings\settings.dat	RoamingState	False
2023-02-27 08:45:44.000000	0xa8892eebc000	Key	\??\C:\Windows\Appcompat\Programs\EncapsulationLogging.hve	Cache	False
2023-02-27 08:45:44.000000	0xa8892eebc000	Key	\??\C:\Windows\Appcompat\Programs\EncapsulationLogging.hve	Events	False
-	0xa8892f08e000	Key	?\	-	-
2023-02-27 08:45:51.000000	0xa8892ebd1000	Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.ShellExperienceHost_10.0.18362.387_neutral_neutral_cw5n1h2txyewy\Activ
ationStore.dat	ActivatableClassId	False
2023-02-27 08:45:51.000000	0xa8892ebd1000	Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.ShellExperienceHost_10.0.18362.387_neutral_neutral_cw5n1h2txyewy\Activ
ationStore.dat	Server	False
2012-05-22 00:00:08.000000	0xa8892ea0a000	Key
\??\C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\settings.dat	LocalState	False
2012-05-22 00:00:08.000000	0xa8892ea0a000	Key
\??\C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\settings.dat	RoamingState	False
2023-02-27 08:45:44.000000	0xa8892f110000	Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\InputApp_1000.18362.387.0_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat
ActivatableClassId	False
2023-02-27 08:45:44.000000	0xa8892f110000	Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\InputApp_1000.18362.387.0_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat	Server
False
2012-05-22 00:00:08.000000	0xa8892e5d0000	Key	\??\C:\Users\user\AppData\Local\Packages\InputApp_cw5n1h2txyewy\Settings\settings.dat	LocalState
False
2012-05-22 00:00:08.000000	0xa8892e5d0000	Key	\??\C:\Users\user\AppData\Local\Packages\InputApp_cw5n1h2txyewy\Settings\settings.dat	RoamingState
False
2023-02-27 00:49:18.000000	0xa8892f3a1000	Key	\??\C:\Windows\AppCompat\Programs\Amcache.hve	Root	False
2023-02-27 01:54:49.000000	0xa889306ef000	Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Photos_2022.30120.12007.0_x64__8wekyb3d8bbwe\ActivationStore.dat
ActivatableClassId	False
2023-02-27 01:54:49.000000	0xa889306ef000	Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Photos_2022.30120.12007.0_x64__8wekyb3d8bbwe\ActivationStore.dat
Server	False
2012-05-22 00:00:08.000000	0xa8892eb50000	Key
\??\C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat	LocalState	False
```

```
2012-05-22 00:00:08.000000      0xa8892eb50000  Key
\??\C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat   RoamingState      False
-      0xa8892ead5000  Key     ?\      -             -
2023-02-27 08:45:49.000000      0xa88930e8e000  Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Cortana_1.13.0.18362_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat
ActivatableClassId             False
2023-02-27 08:45:49.000000      0xa88930e8e000  Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Cortana_1.13.0.18362_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat
Interfaces             False
2023-02-27 08:45:49.000000      0xa88930e8e000  Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Cortana_1.13.0.18362_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat
ProxyStubCLSIDs        False
2023-02-27 08:45:49.000000      0xa88930e8e000  Key
\??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Cortana_1.13.0.18362_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat
Server         False
2012-05-22 00:00:08.000000      0xa8892e6cc000  Key
\??\C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\settings.dat  LocalState        False
2012-05-22 00:00:08.000000      0xa8892e6cc000  Key
\??\C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\settings.dat  RoamingState      False
```