# WANNACRY RANSOMWARE

Raghad Lafe
2111941

Atheer Alotaibi
2111266

Joury Alshelwai
2110772

Retaj Farhan
2110832

# Background on wannacry

WannaCry exploited a vulnerability in the SMB protocol, known as EternalBlue. It quickly spread across networks, encrypting files and demanding Bitcoin payments to restore access.

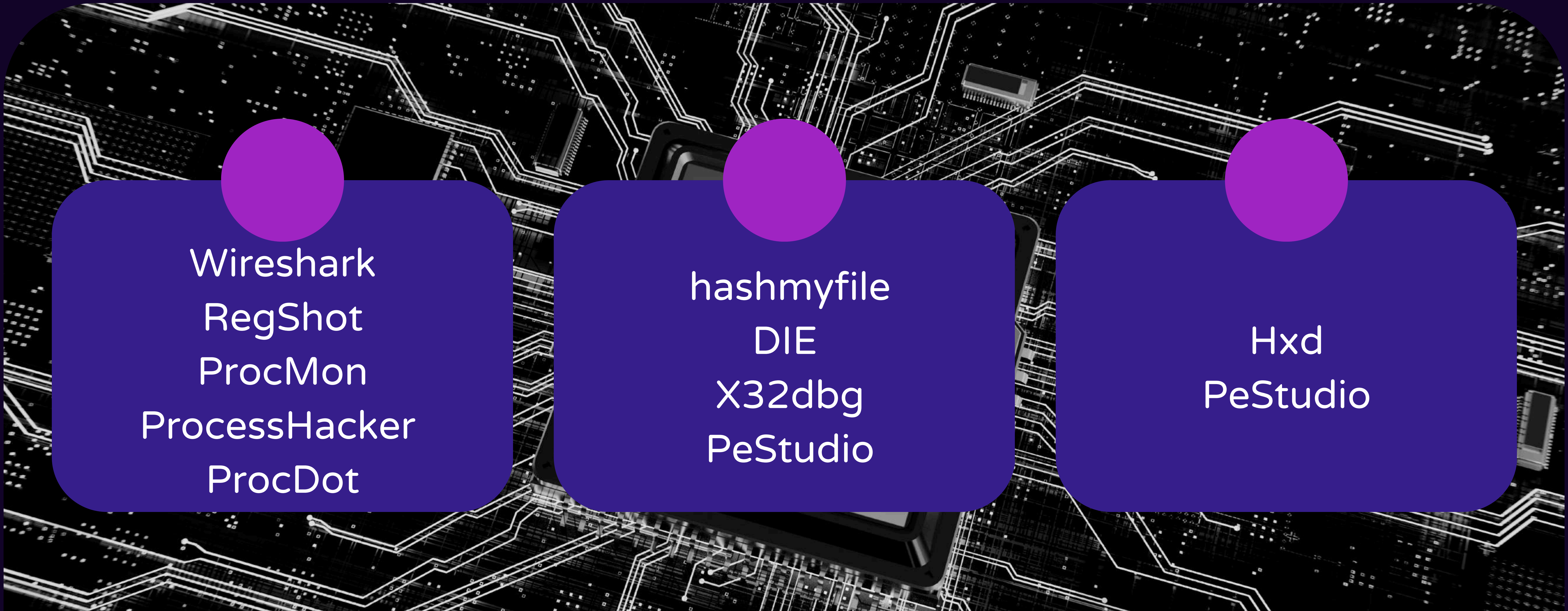
# How it works?

1. Initial Infection
2. Encryption
3. Persistence
4. Kill-Switch Mechanism

# Our Goal

1. Understanding malware behavior
2. Identifying API calls
3. Debugging
4. Dumping

# Overview of tools



Wireshark
RegShot
ProcMon
ProcessHacker
ProcDot

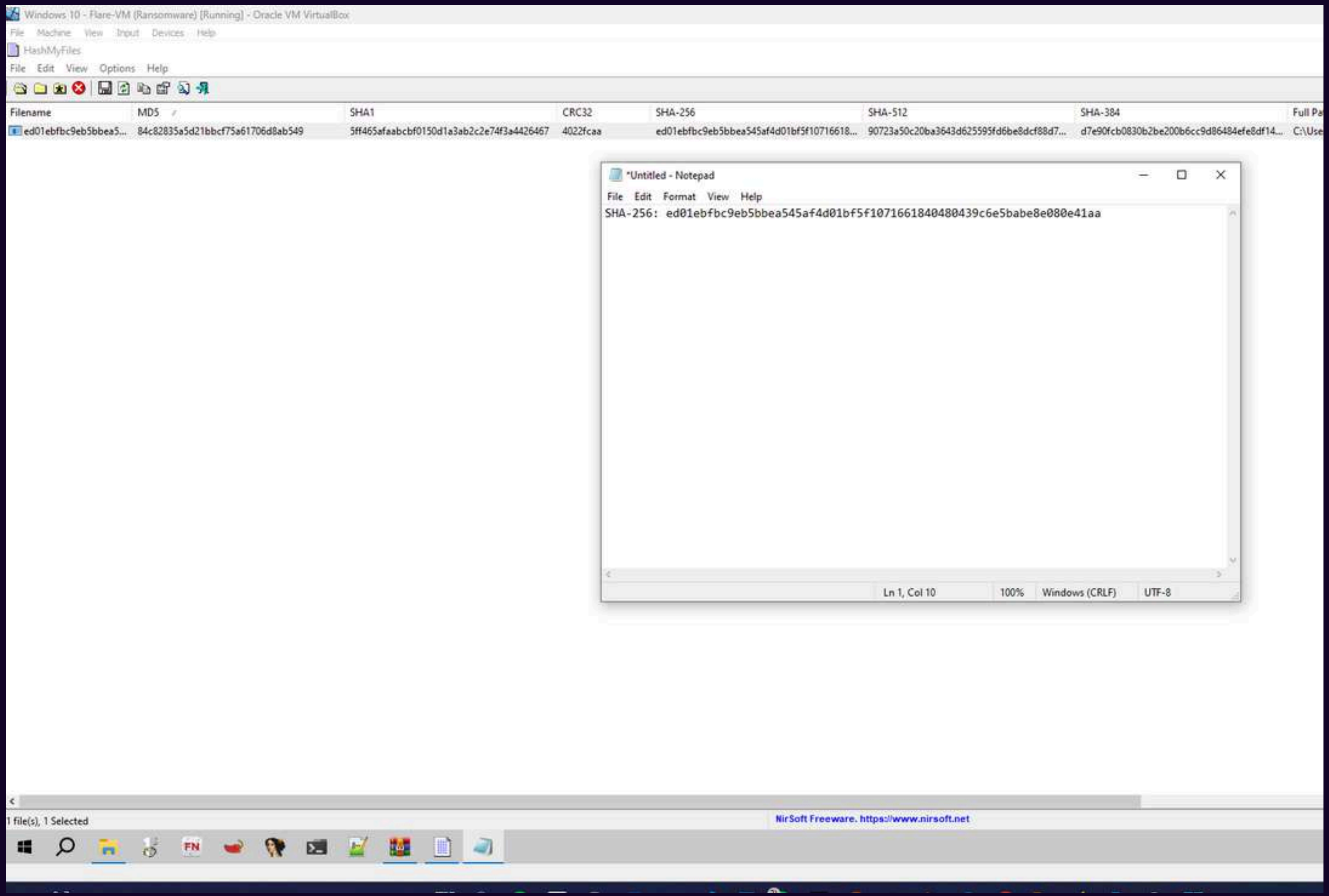
hashmyfile
DIE
X32dbg
PeStudio

Hxd
PeStudio

# Sample used

- Source: GitHub repository by kh4sh3i (Ransomware-Samples)
- Sample Verification: Calculating the file hash with HashMyFiles
- Comparison: Verifying the hash with VirusTotal’s database for integrity and authenticity

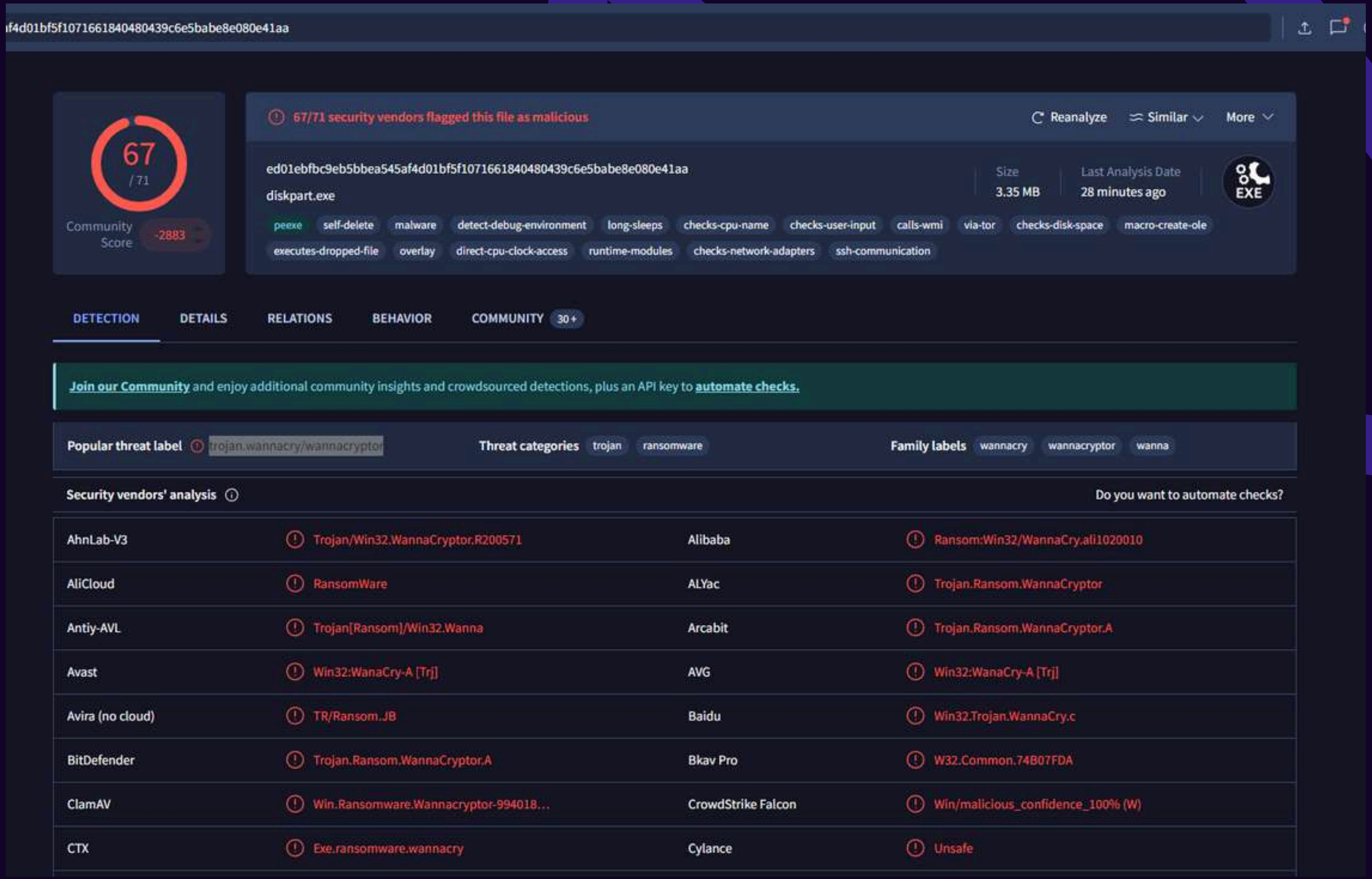
# Sample used


Windows 10 - Flare-VM (Ransomware) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HashMyFiles
File Edit View Options Help

| Filename | MD5 | SHA1 | CRC32 | SHA-256 | SHA-512 | SHA-384 | Full Pa |
|---|---|---|---|---|---|---|---|
| ed01ebfbc9eb5bbea5... | 84c82835a5d21bbcf75a61706d8ab549 | 5ff465afaabcbf0150d1a3ab2c2e74f3a4426467 | 4022fcaa | ed01ebfbc9eb5bbea545af4d01bf5f10716618... | 90723a50c20ba3643d625595fd6be8dcf88d7... | d7e90fcb0830b2be200b6cc9d86484efe8df14... | C:\Use |

*Untitled - Notepad
File Edit Format View Help

```
SHA-256: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
```



67/71 security vendors flagged this file as malicious

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

diskpart.exe

Size 3.35 MB

Last Analysis Date 28 minutes ago

peexe · self-delete · malware · detect-debug-environment · long-sleeps · checks-cpu-name · checks-user-input · calls-wmi · via-tor · checks-disk-space · macro-create-ole · executes-dropped-file · overlay · direct-cpu-clock-access · runtime-modules · checks-network-adapters · ssh-communication

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

Popular threat label trojan.wannacry/wannacryptor

Threat categories trojan · ransomware

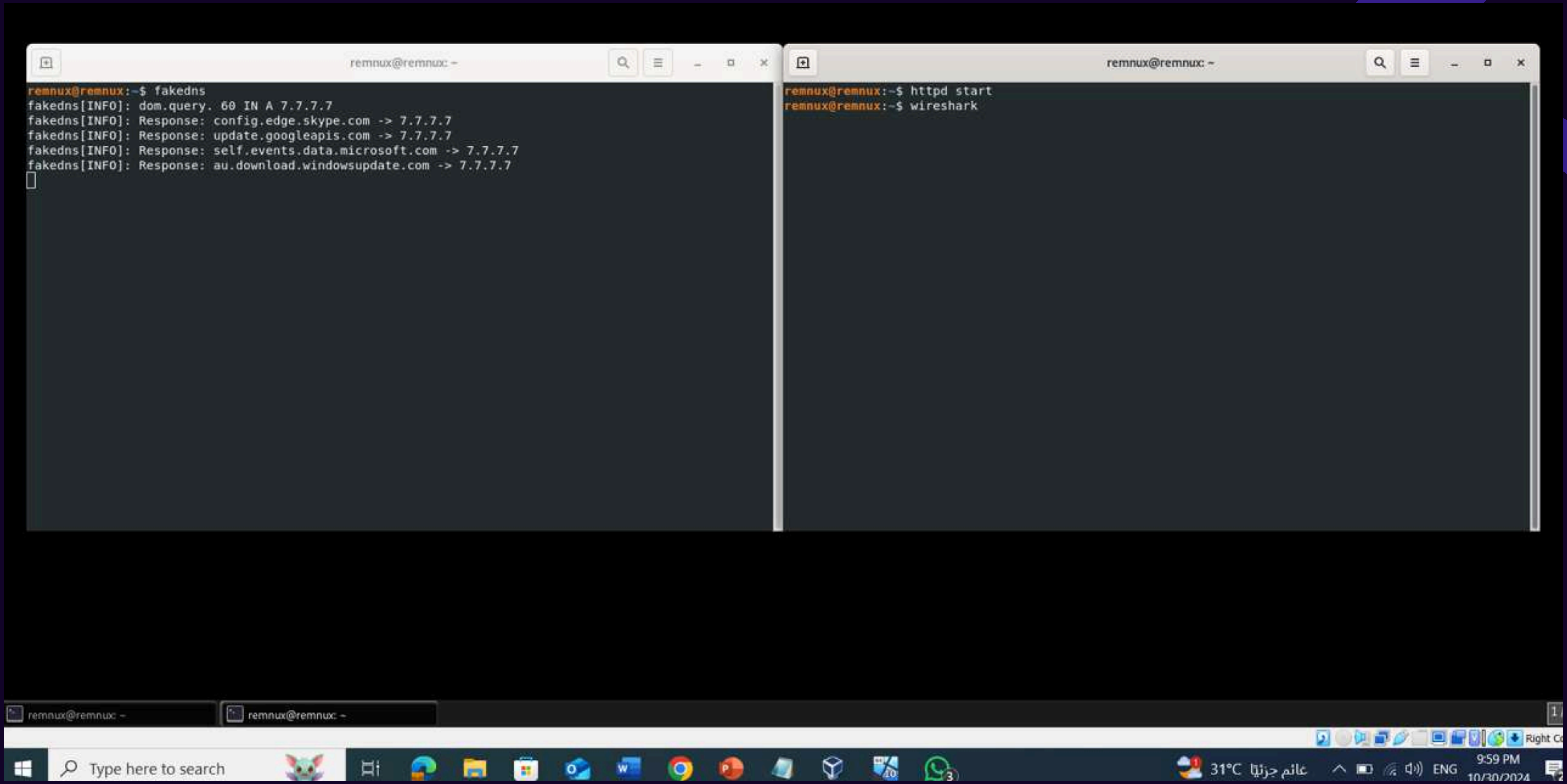
Family labels wannacry · wannacryptor · wanna

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---|---|---|---|
| AhnLab-V3 | Trojan/Win32.WannaCryptor.R200571 | Alibaba | Ransom:Win32/WannaCry.ali1020010 |
| AliCloud | RansomWare | ALYac | Trojan.Ransom.WannaCryptor |
| Antiy-AVL | Trojan[Ransom]/Win32.Wanna | Arcabit | Trojan.Ransom.WannaCryptor.A |
| Avast | Win32:WanaCry-A [Trj] | AVG | Win32:WanaCry-A [Trj] |
| Avira (no cloud) | TR/Ransom.JB | Baidu | Win32.Trojan.WannaCry.c |
| BitDefender | Trojan.Ransom.WannaCryptor.A | Bkav Pro | W32.Common.74B07FDA |
| ClamAV | Win.Ransomware.Wannacryptor-994018... | CrowdStrike Falcon | Win/malicious_confidence_100% (W) |
| CTX | Exe.ransomware.wannacry | Cylance | Unsafe |

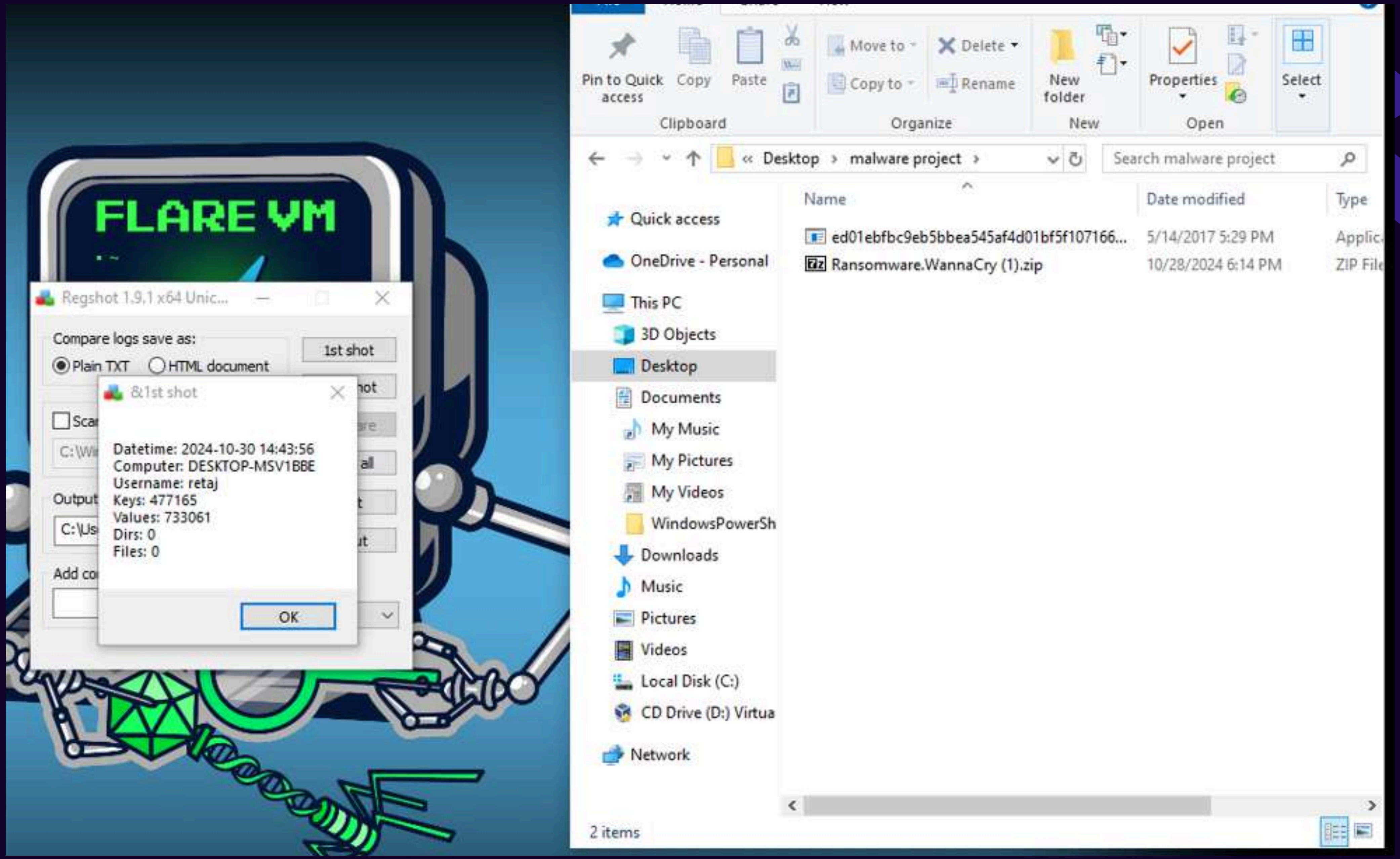
# Behavior Analysis



```
remnux@remnux:~$ fakedns
fakedns[INFO]: dom.query. 60 IN A 7.7.7.7
fakedns[INFO]: Response: config.edge.skype.com -> 7.7.7.7
fakedns[INFO]: Response: update.googleapis.com -> 7.7.7.7
fakedns[INFO]: Response: self.events.data.microsoft.com -> 7.7.7.7
fakedns[INFO]: Response: au.download.windowsupdate.com -> 7.7.7.7
```

```
remnux@remnux:~$ httpd start
remnux@remnux:~$ wireshark
```

# Behavior Analysis



Compare logs save as: ● Plain TXT ○ HTML document

```
Datetime: 2024-10-30 14:43:56
Computer: DESKTOP-MSV1BBE
Username: retaj
Keys: 477165
Values: 733061
Dirs: 0
Files: 0
```

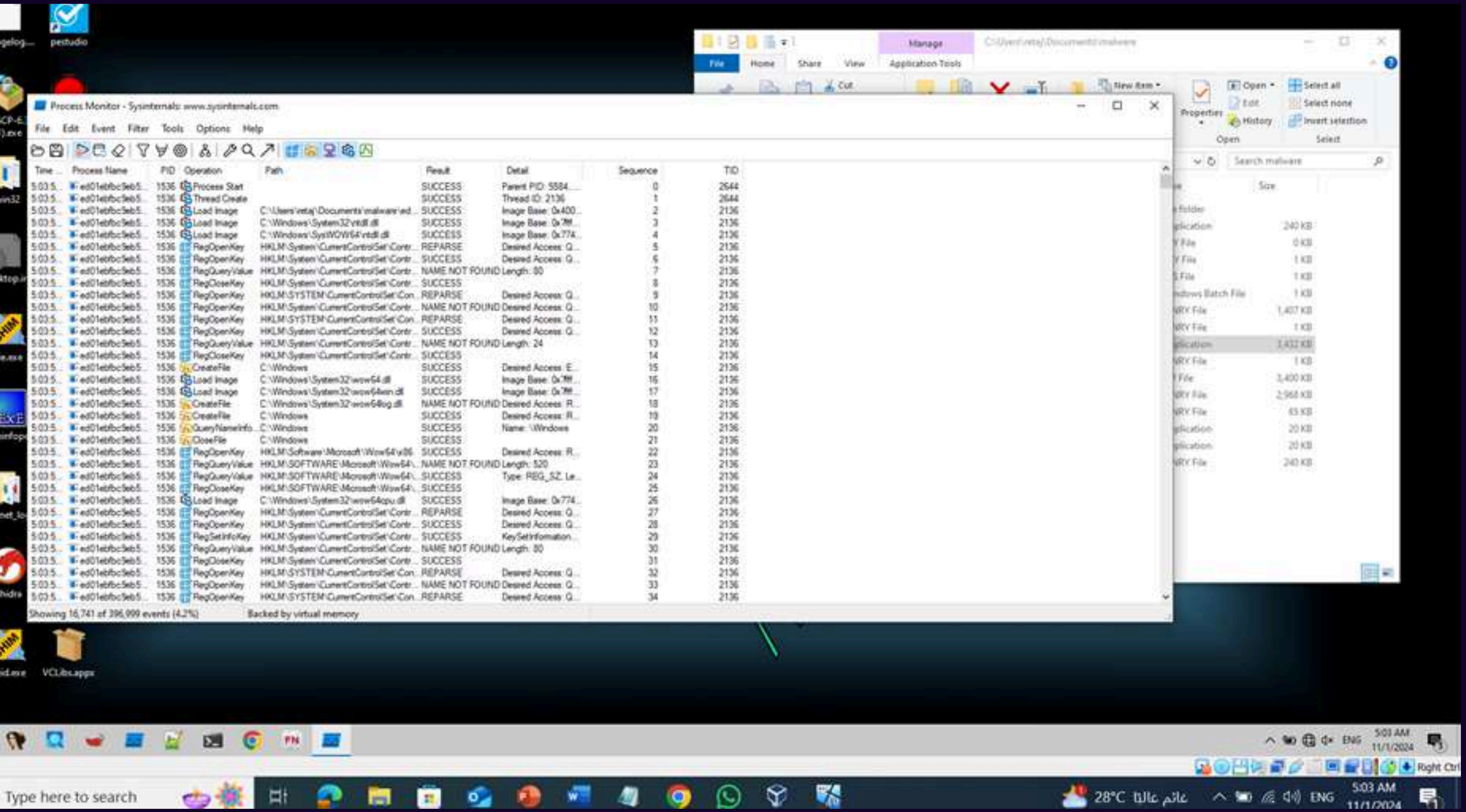
« Desktop › malware project ›

| Name | Date modified | Type |
|---|---|---|
| ed01ebfbc9eb5bbea545af4d01bf5f107166... | 5/14/2017 5:29 PM | Applic |
| Ransomware.WannaCry (1).zip | 10/28/2024 6:14 PM | ZIP File |

first shot

# Behavior Analysis

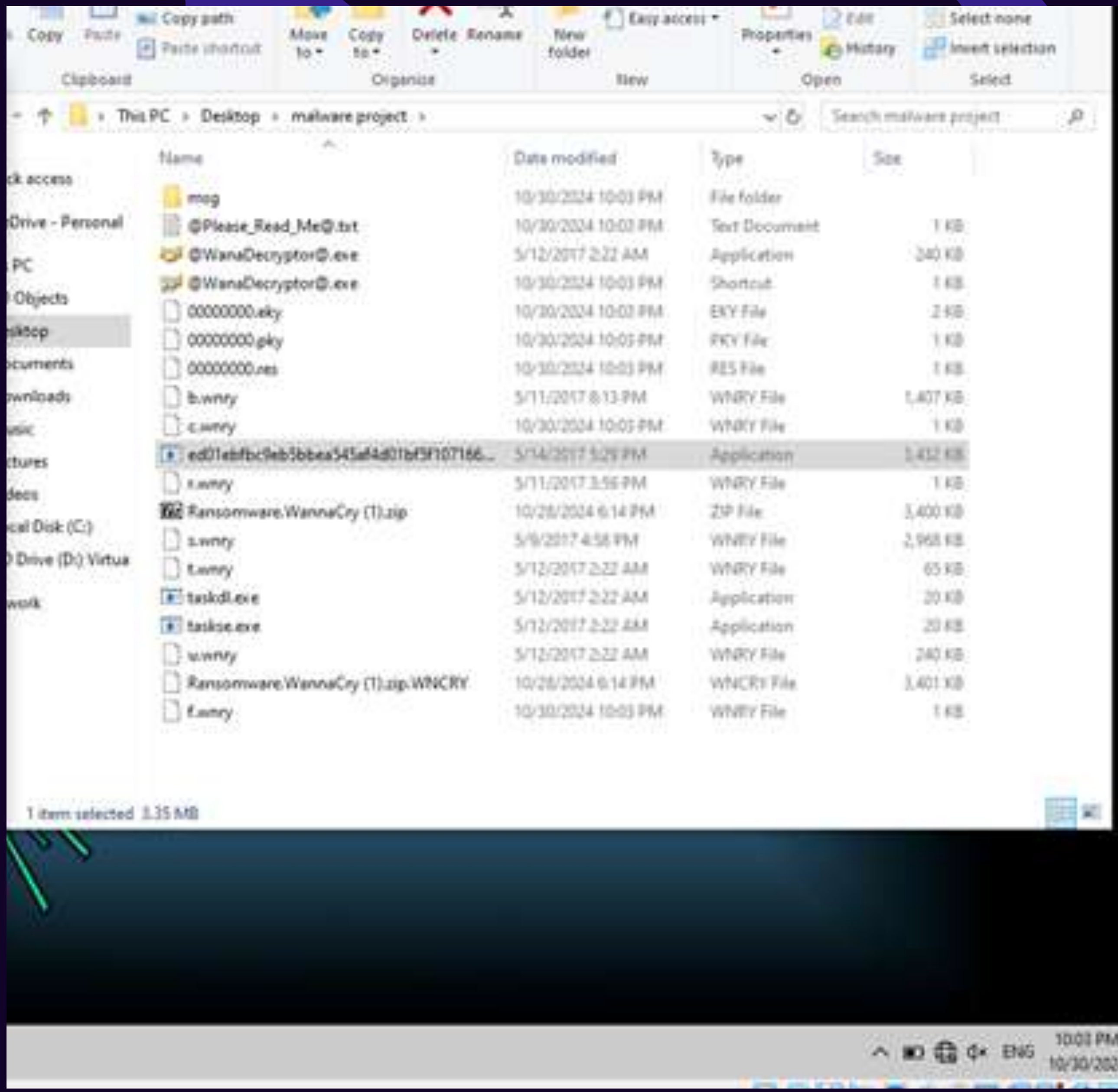
## after running the malware



Process Monitor - Sysinternals: www.sysinternals.com

| Time ... | Process Name | PID | Operation | Path | Result | Detail | Sequence | TID |
|---|---|---|---|---|---|---|---|---|
| 5:03:5... | ed01ebfbc9eb5... | 1536 | Process Start | | SUCCESS | Parent PID: 5584... | 0 | 2644 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | Thread Create | | SUCCESS | Thread ID: 2136 | 1 | 2644 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | Load Image | C:\Users\retaj\Documents\malware\ed... | SUCCESS | Image Base: 0x400... | 2 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | Load Image | C:\Windows\System32\ntdll.dll | SUCCESS | Image Base: 0x7ff... | 3 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | Load Image | C:\Windows\SysWOW64\ntdll.dll | SUCCESS | Image Base: 0x774... | 4 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | REPARSE | Desired Access: Q... | 5 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | Desired Access: Q... | 6 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegQueryValue | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Length: 80 | 7 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegCloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | | 8 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Con... | REPARSE | Desired Access: Q... | 9 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Desired Access: Q... | 10 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Con... | REPARSE | Desired Access: Q... | 11 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | Desired Access: Q... | 12 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegQueryValue | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Length: 24 | 13 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegCloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | | 14 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | CreateFile | C:\Windows | SUCCESS | Desired Access: E... | 15 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | Load Image | C:\Windows\System32\wow64.dll | SUCCESS | Image Base: 0x7ff... | 16 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | Load Image | C:\Windows\System32\wow64win.dll | SUCCESS | Image Base: 0x7ff... | 17 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | CreateFile | C:\Windows\System32\wow64log.dll | NAME NOT FOUND | Desired Access: R... | 18 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | CreateFile | C:\Windows | SUCCESS | Desired Access: R... | 19 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | QueryNameInfo... | C:\Windows | SUCCESS | Name: \Windows | 20 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | CloseFile | C:\Windows | SUCCESS | | 21 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\Software\Microsoft\Wow64\x86 | SUCCESS | Desired Access: R... | 22 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Wow64\... | NAME NOT FOUND | Length: 520 | 23 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Wow64\... | SUCCESS | Type: REG_SZ, Le... | 24 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegCloseKey | HKLM\SOFTWARE\Microsoft\Wow64\... | SUCCESS | | 25 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | Load Image | C:\Windows\System32\wow64cpu.dll | SUCCESS | Image Base: 0x774... | 26 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | REPARSE | Desired Access: Q... | 27 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | Desired Access: Q... | 28 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegSetInfoKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | KeySetInformation... | 29 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegQueryValue | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Length: 80 | 30 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegCloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | | 31 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Con... | REPARSE | Desired Access: Q... | 32 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Desired Access: Q... | 33 | 2136 |
| 5:03:5... | ed01ebfbc9eb5... | 1536 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Con... | REPARSE | Desired Access: Q... | 34 | 2136 |

Showing 16,741 of 396,999 events (4.2%)   Backed by virtual memory



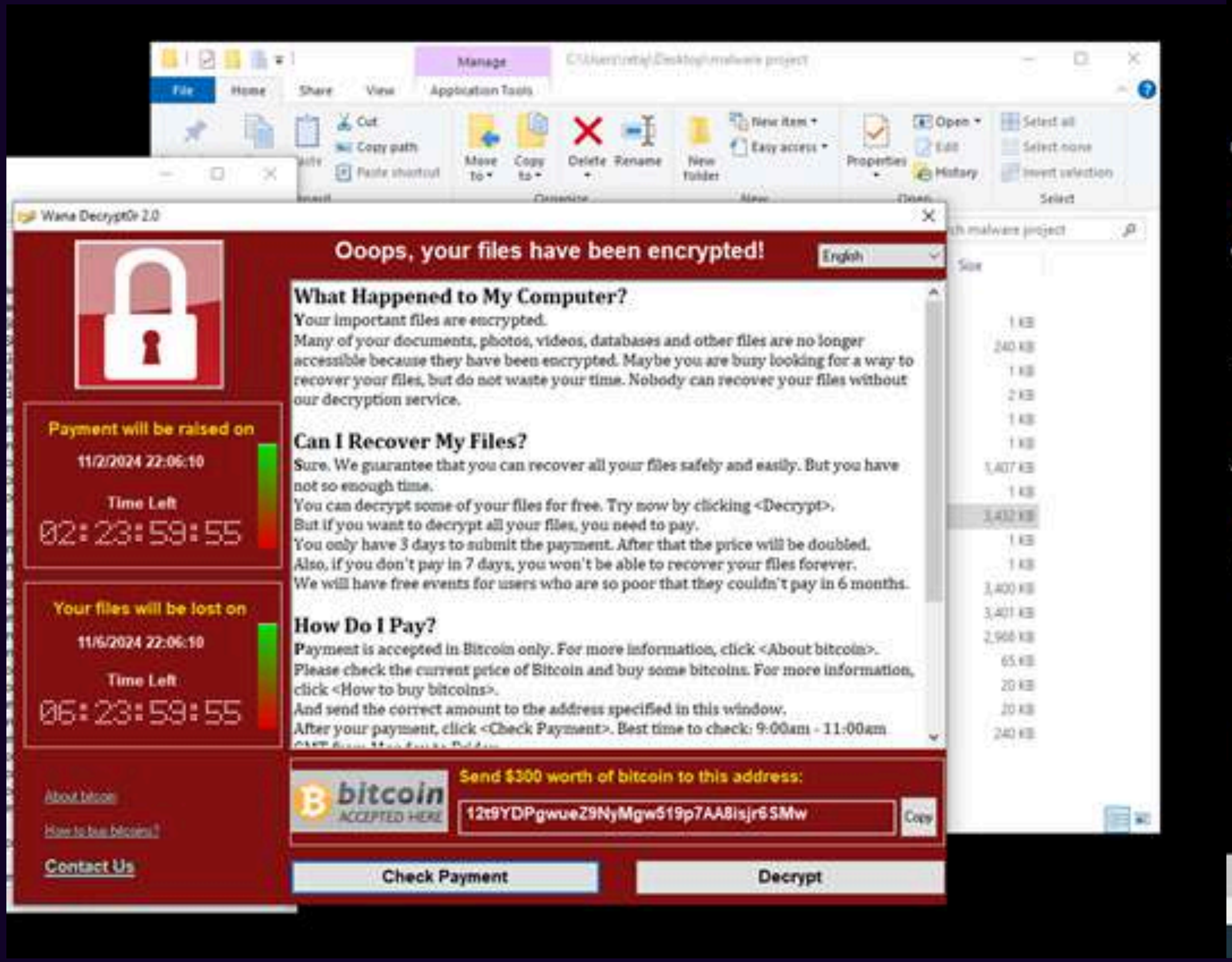
This PC › Desktop › malware project ›

| Name | Date modified | Type | Size |
|---|---|---|---|
| msg | 10/30/2024 10:03 PM | File folder | |
| @Please_Read_Me@.txt | 10/30/2024 10:03 PM | Text Document | 1 KB |
| @WanaDecryptor@.exe | 5/12/2017 2:22 AM | Application | 240 KB |
| @WanaDecryptor@.exe | 10/30/2024 10:03 PM | Shortcut | 1 KB |
| 00000000.eky | 10/30/2024 10:03 PM | EKY File | 2 KB |
| 00000000.pky | 10/30/2024 10:03 PM | PKY File | 1 KB |
| 00000000.res | 10/30/2024 10:03 PM | RES File | 1 KB |
| b.wnry | 5/11/2017 8:13 PM | WNRY File | 1,407 KB |
| c.wnry | 10/30/2024 10:03 PM | WNRY File | 1 KB |
| ed01ebfbc9eb5bbea545af4d01bf5f107166... | 5/14/2017 5:29 PM | Application | 3,432 KB |
| r.wnry | 5/11/2017 3:56 PM | WNRY File | 1 KB |
| Ransomware.WannaCry (1).zip | 10/28/2024 6:14 PM | ZIP File | 3,400 KB |
| s.wnry | 5/9/2017 4:58 PM | WNRY File | 2,968 KB |
| t.wnry | 5/12/2017 2:22 AM | WNRY File | 65 KB |
| taskdl.exe | 5/12/2017 2:22 AM | Application | 20 KB |
| taskse.exe | 5/12/2017 2:22 AM | Application | 20 KB |
| u.wnry | 5/12/2017 2:22 AM | WNRY File | 240 KB |
| Ransomware.WannaCry (1).zip.WNCRY | 10/28/2024 6:14 PM | WNCRY File | 3,401 KB |
| f.wnry | 10/30/2024 10:03 PM | WNRY File | 1 KB |

1 item selected 3.35 MB

# Behavior Analysis

## Ransom note



Ooops, your files have been encrypted!

**What Happened to My Computer?**

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

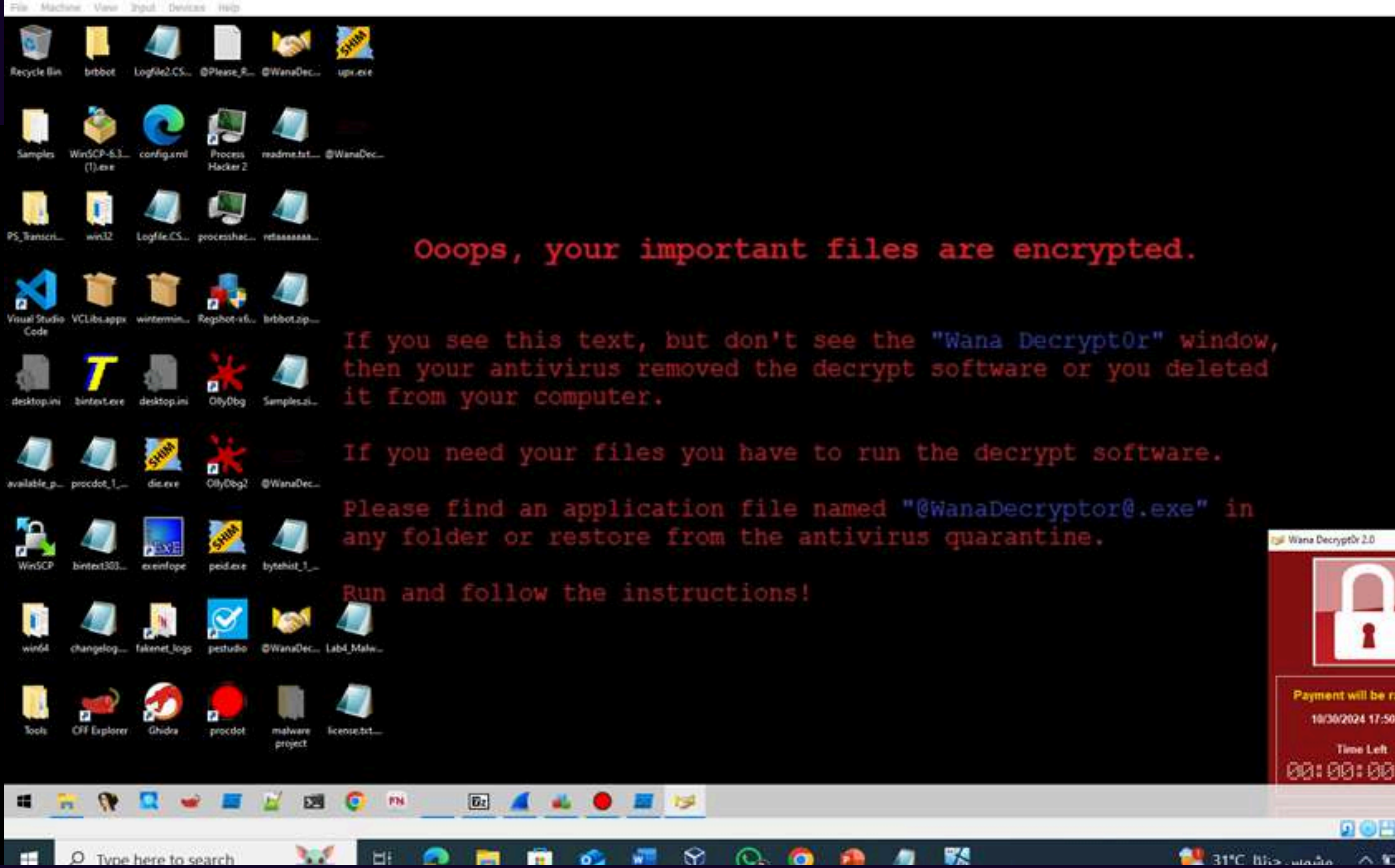
Payment will be raised on
11/2/2024 22:06:10
Time Left
02:23:59:55

Your files will be lost on
11/6/2024 22:06:10
Time Left
06:23:59:55

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

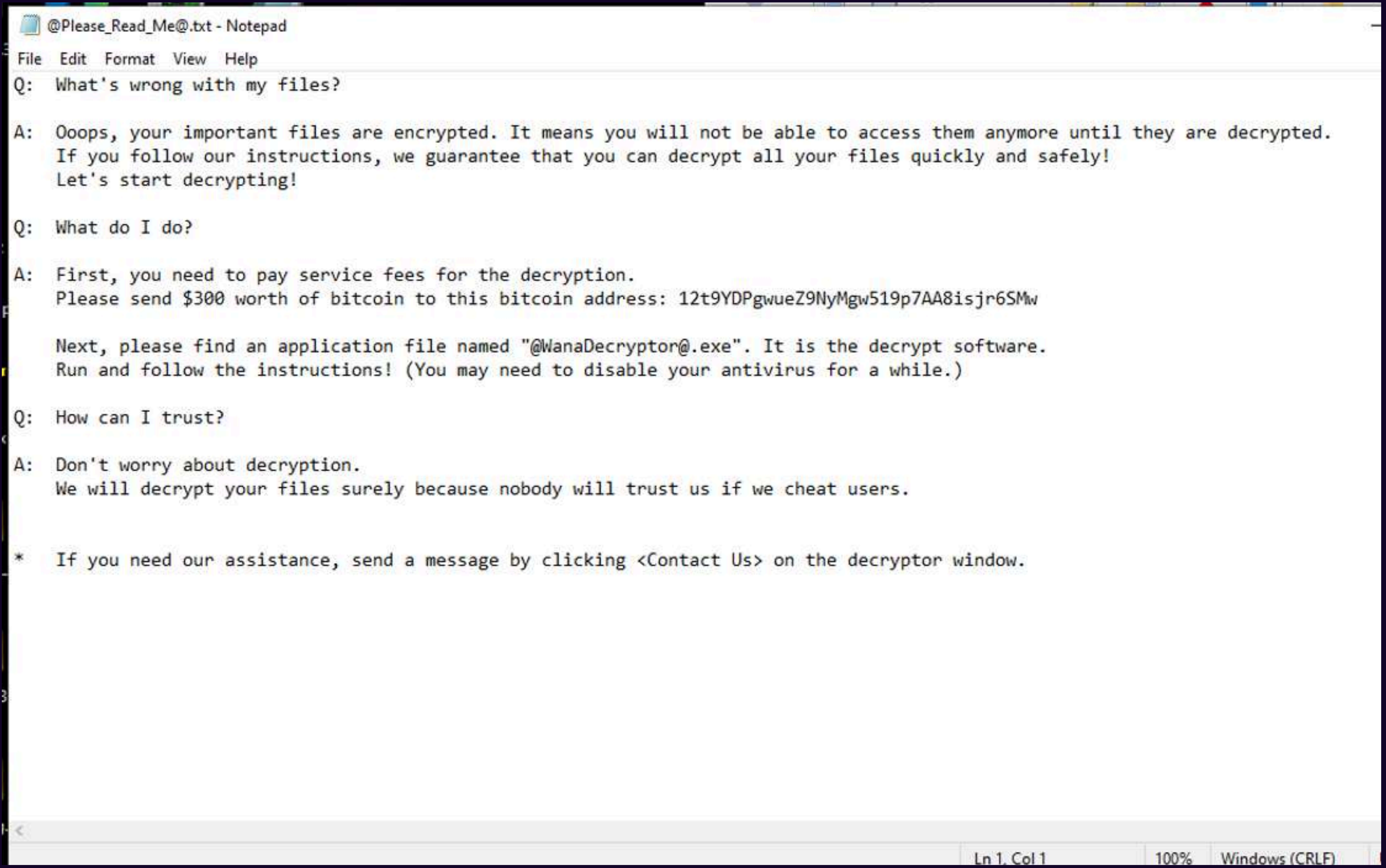


```
Ooops, your important files are encrypted.

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!
```

Payment will be r
10/30/2024 17:50
Time Left
00:00:00

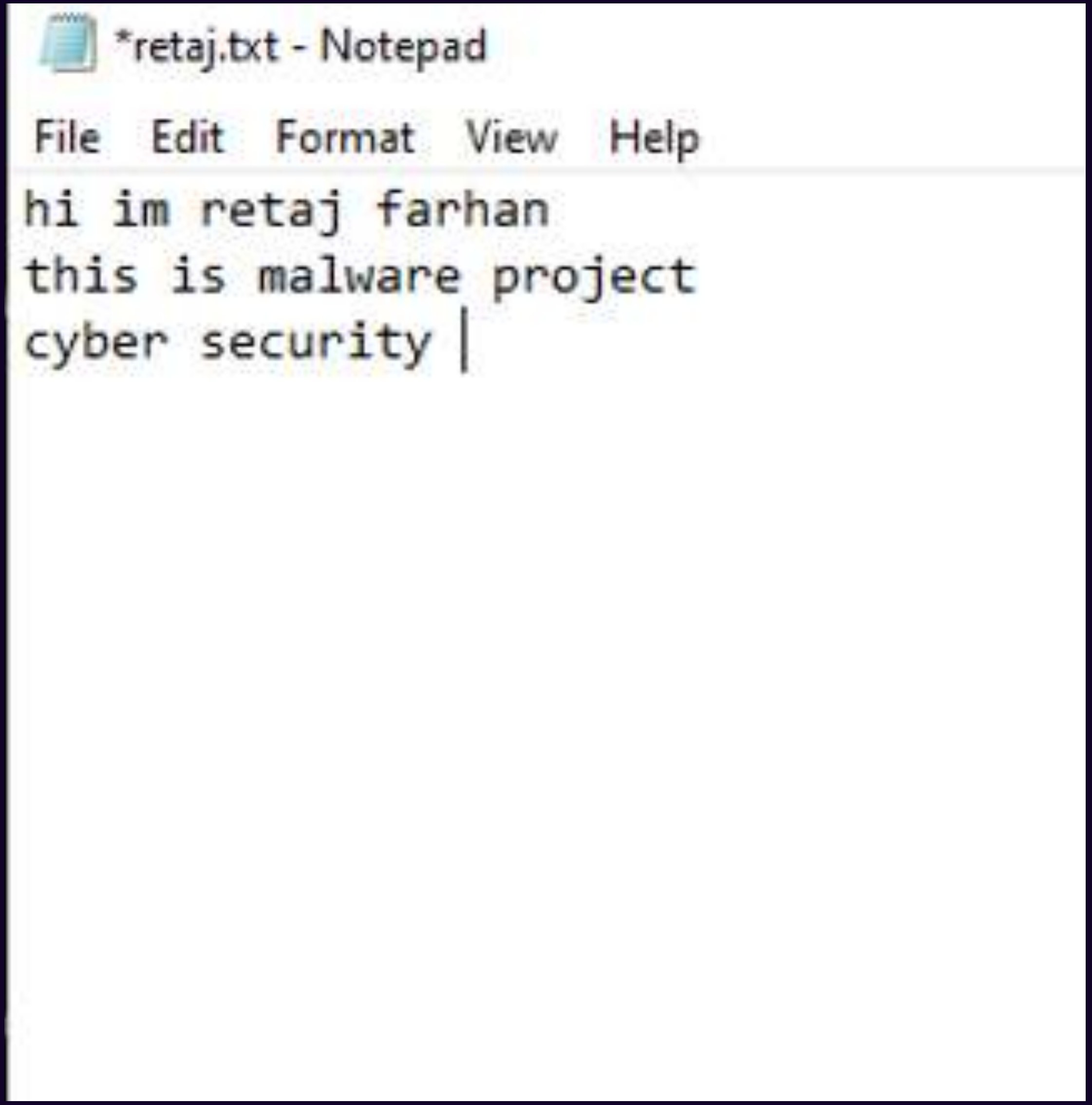
# Behavior Analysis

## ransom note generated by the WannaCry malware.



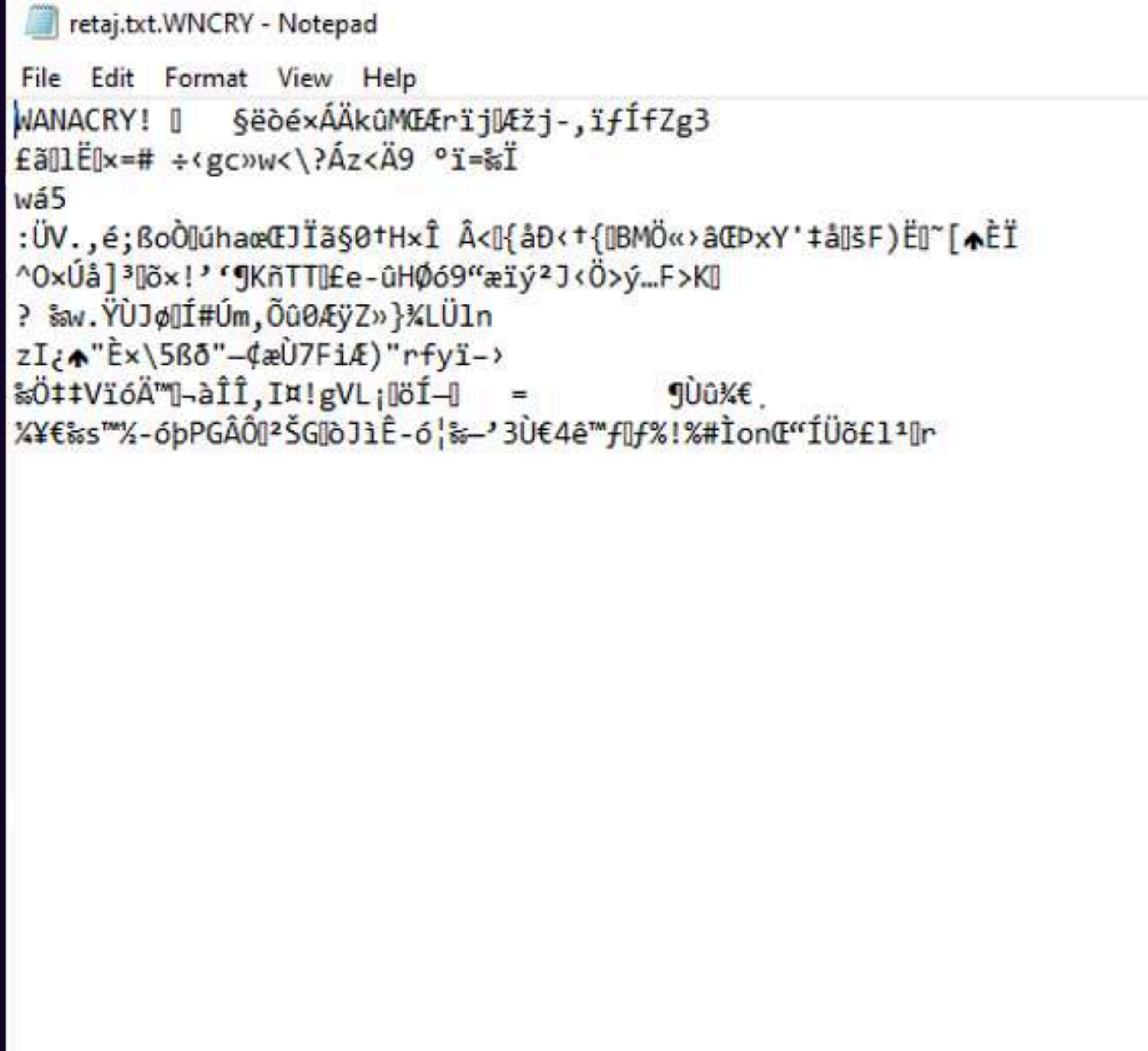
```
Q:  What's wrong with my files?

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 $300 worth of bitcoin to this bitcoin address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

    Next, please find an application file named "@WanaDecryptor@.exe". 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.
```

# Behavior Analysis



```
hi im retaj farhan
this is malware project
cyber security
```

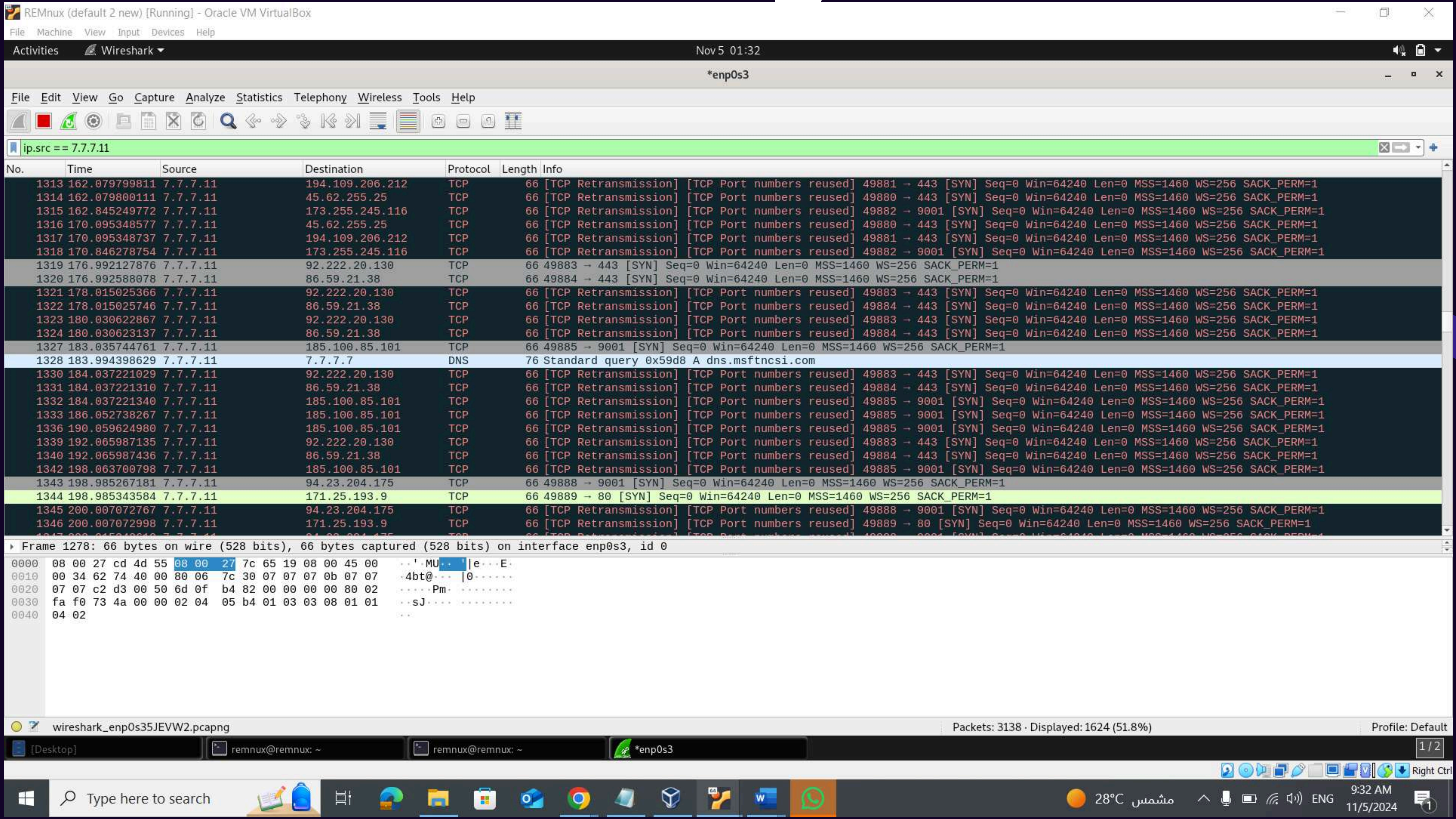
before running the malware



```
WANACRY! ▯   §ëòé×ÁÄkûMŒÆrïj▯Æžj-,ïƒÍfZg3
£ã▯1Ë▯×=# ÷‹gc»w<\?Áz<Ä9 °ï=‰Ï
wá5
:ÜV.,é;ßoÒ▯úhaœŒJÏã§0†H×Î Â<▯{åÐ‹†{▯BMÖ«›âŒÞxY'‡å▯šF)Ë▯˜[↑ÈÏ
^O×Úå]³▯õ×!’‘¶KñTT▯£e-ûHØó9“æïý²J‹Ö>ý…F>K▯
? ‰w.ŸÙJø▯Í#Úm,ÕûØÆÿZ»}¾LÜ1n
zI¿↑"Èx\5ßð"–¢æÙ7FiÆ)"rfyï-›
‰Ö‡‡VïóÄ™▯¬àÎÎ,I¤!gVL¡▯öÍ–▯   =         ¶Ùû¾€
¼¥€‰s™½-óþPGÂÔ▯²ŠG▯òJìÊ-ó¦‰–’3Ù€4ê™ƒ▯ƒ%!%#ÌonŒ“ÍÜõ£1¹▯r
```

after running the malware

# Behavior Analysis


REMnux (default 2 new) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Wireshark
Nov 5 01:32
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[Desktop]
remnux@remnux: ~
remnux@remnux: ~
*enp0s3
1 / 2
Right Ctrl
Type here to search
28°C مشمس
ENG
9:32 AM
11/5/2024

```
ip.src == 7.7.7.11
```

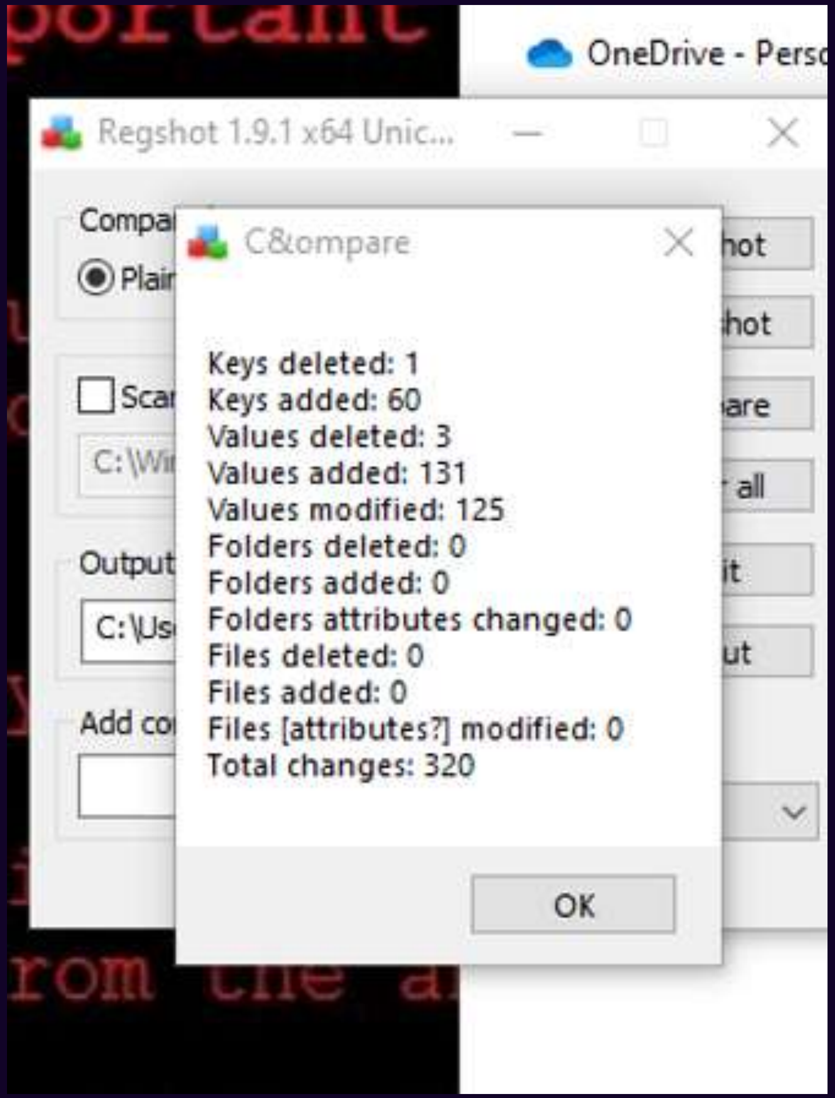
```
No.   Time          Source     Destination      Protocol Length Info
 1313 162.079799811 7.7.7.11   194.109.206.212  TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49881 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1314 162.079800111 7.7.7.11   45.62.255.25     TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49880 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1315 162.845249772 7.7.7.11   173.255.245.116  TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49882 → 9001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1316 170.095348577 7.7.7.11   45.62.255.25     TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49880 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1317 170.095348737 7.7.7.11   194.109.206.212  TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49881 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1318 170.846278754 7.7.7.11   173.255.245.116  TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49882 → 9001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1319 176.992127876 7.7.7.11   92.222.20.130    TCP      66 49883 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1320 176.992588078 7.7.7.11   86.59.21.38      TCP      66 49884 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1321 178.015025366 7.7.7.11   92.222.20.130    TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49883 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1322 178.015025746 7.7.7.11   86.59.21.38      TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49884 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1323 180.030622867 7.7.7.11   92.222.20.130    TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49883 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1324 180.030623137 7.7.7.11   86.59.21.38      TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49884 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1327 183.035744761 7.7.7.11   185.100.85.101   TCP      66 49885 → 9001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1328 183.994398629 7.7.7.11   7.7.7.7          DNS      76 Standard query 0x59d8 A dns.msftncsi.com
 1330 184.037221029 7.7.7.11   92.222.20.130    TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49883 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1331 184.037221310 7.7.7.11   86.59.21.38      TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49884 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1332 184.037221340 7.7.7.11   185.100.85.101   TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49885 → 9001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1333 186.052738267 7.7.7.11   185.100.85.101   TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49885 → 9001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1336 190.059624980 7.7.7.11   185.100.85.101   TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49885 → 9001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1339 192.065987135 7.7.7.11   92.222.20.130    TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49883 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1340 192.065987436 7.7.7.11   86.59.21.38      TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49884 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1342 198.063700798 7.7.7.11   185.100.85.101   TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49885 → 9001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1343 198.985267181 7.7.7.11   94.23.204.175    TCP      66 49888 → 9001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1344 198.985343584 7.7.7.11   171.25.193.9     TCP      66 49889 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1345 200.007072767 7.7.7.11   94.23.204.175    TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49888 → 9001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1346 200.007072998 7.7.7.11   171.25.193.9     TCP      66 [TCP Retransmission] [TCP Port numbers reused] 49889 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
› Frame 1278: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0
```

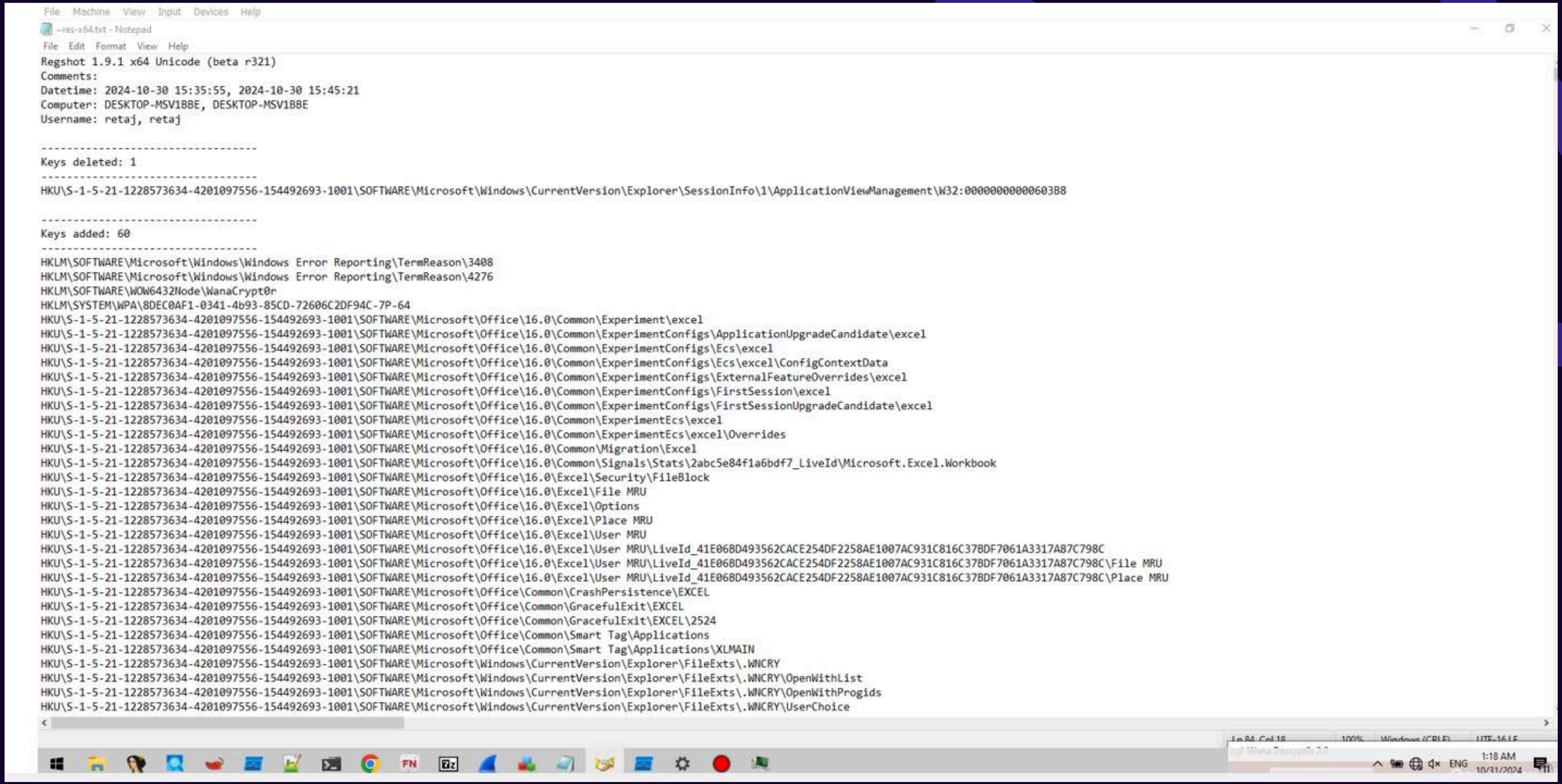
```
0000  08 00 27 cd 4d 55 08 00  27 7c 65 19 08 00 45 00   ··'·MU·· '|e···E·
0010  00 34 62 74 40 00 80 06  7c 30 07 07 07 0b 07 07   ·4bt@··· |0······
0020  07 07 c2 d3 00 50 6d 0f  b4 82 00 00 00 00 80 02   ·····Pm· ········
0030  fa f0 73 4a 00 00 02 04  05 b4 01 03 03 08 01 01   ··sJ···· ········
0040  04 02                                              ··
```

```
wireshark_enp0s35JEVW2.pcapng     Packets: 3138 · Displayed: 1624 (51.8%)     Profile: Default
```

# Behavior Analysis

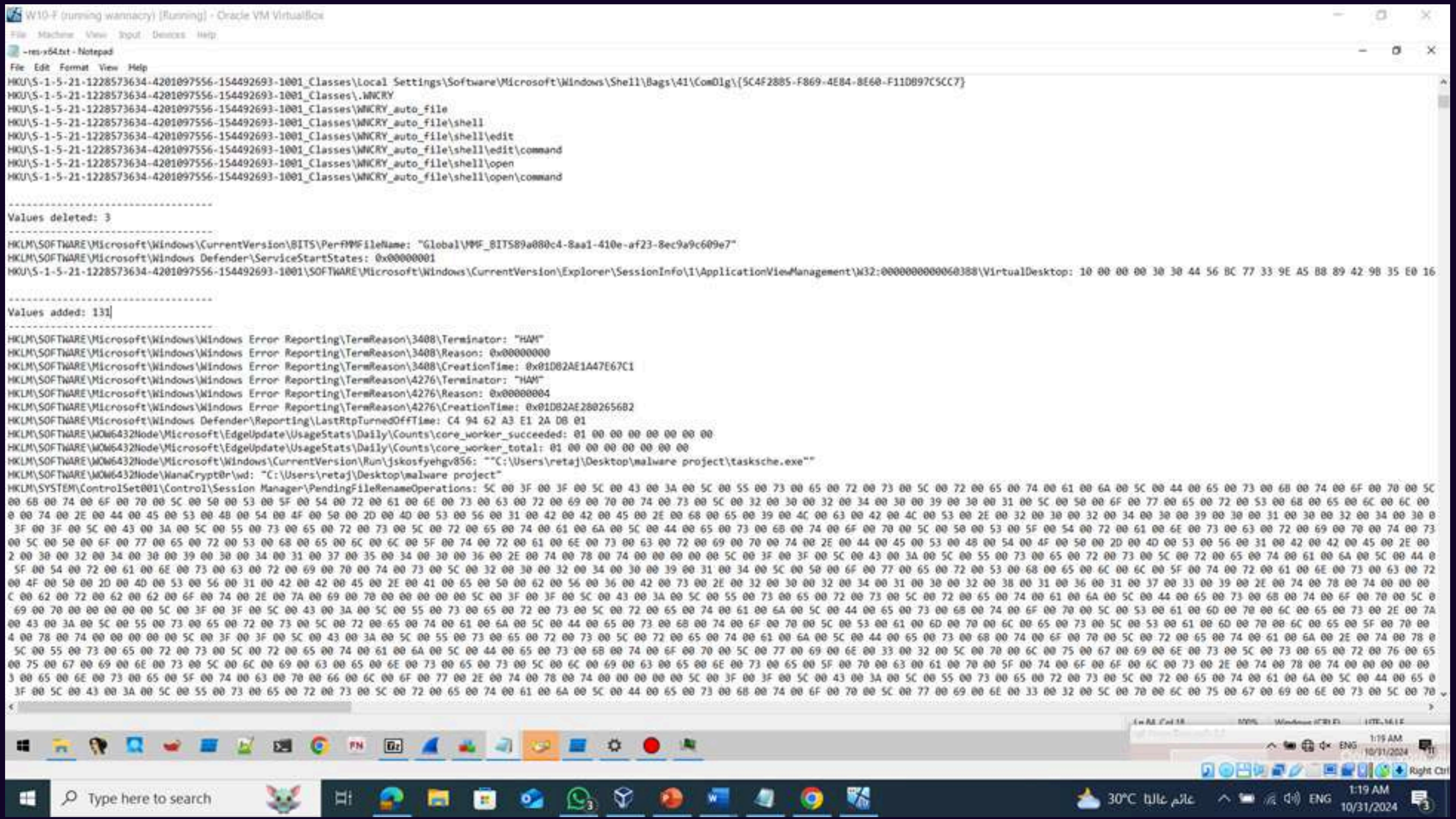


```
Keys deleted: 1
Keys added: 60
Values deleted: 3
Values added: 131
Values modified: 125
Folders deleted: 0
Folders added: 0
Folders attributes changed: 0
Files deleted: 0
Files added: 0
Files [attributes?] modified: 0
Total changes: 320
```

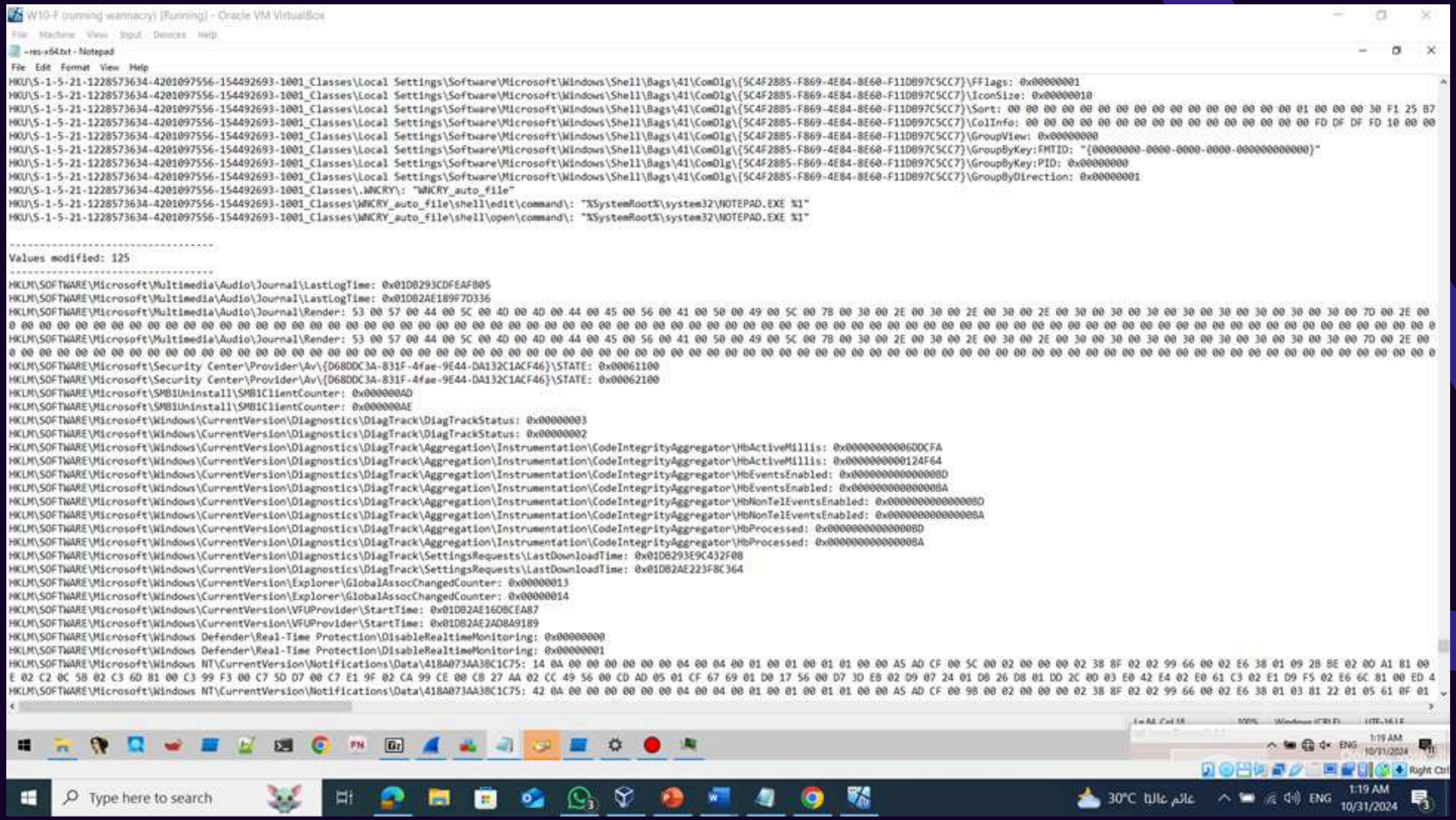

File Machine View Input Devices Help
~res-x64.txt - Notepad
File Edit Format View Help

```
Regshot 1.9.1 x64 Unicode (beta r321)
Comments:
Datetime: 2024-10-30 15:35:55, 2024-10-30 15:45:21
Computer: DESKTOP-MSV1BBE, DESKTOP-MSV1BBE
Username: retaj, retaj

----------------------------------
Keys deleted: 1
----------------------------------
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000603B8

----------------------------------
Keys added: 60
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3408
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4276
HKLM\SOFTWARE\WOW6432Node\WanaCrypt0r
HKLM\SYSTEM\WPA\8DEC0AF1-0341-4b93-85CD-72606C2DF94C-7P-64
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Common\Experiment\excel
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\ApplicationUpgradeCandidate\excel
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\excel
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\excel\ConfigContextData
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\ExternalFeatureOverrides\excel
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\FirstSession\excel
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\FirstSessionUpgradeCandidate\excel
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentEcs\excel
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentEcs\excel\Overrides
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Common\Migration\Excel
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Common\Signals\Stats\2abc5e84f1a6bdf7_LiveId\Microsoft.Excel.Workbook
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Excel\Security\FileBlock
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Excel\File MRU
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Excel\Options
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Excel\Place MRU
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Excel\User MRU
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Excel\User MRU\LiveId_41E06BD493562CACE254DF2258AE1007AC931C816C37BDF7061A3317A87C798C
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Excel\User MRU\LiveId_41E06BD493562CACE254DF2258AE1007AC931C816C37BDF7061A3317A87C798C\File MRU
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\16.0\Excel\User MRU\LiveId_41E06BD493562CACE254DF2258AE1007AC931C816C37BDF7061A3317A87C798C\Place MRU
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\Common\CrashPersistence\EXCEL
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\Common\GracefulExit\EXCEL
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\Common\GracefulExit\EXCEL\2524
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\Common\Smart Tag\Applications
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Office\Common\Smart Tag\Applications\XLMAIN
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.WNCRY
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.WNCRY\OpenWithList
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.WNCRY\OpenWithProgids
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.WNCRY\UserChoice
```

# Behavior Analysis

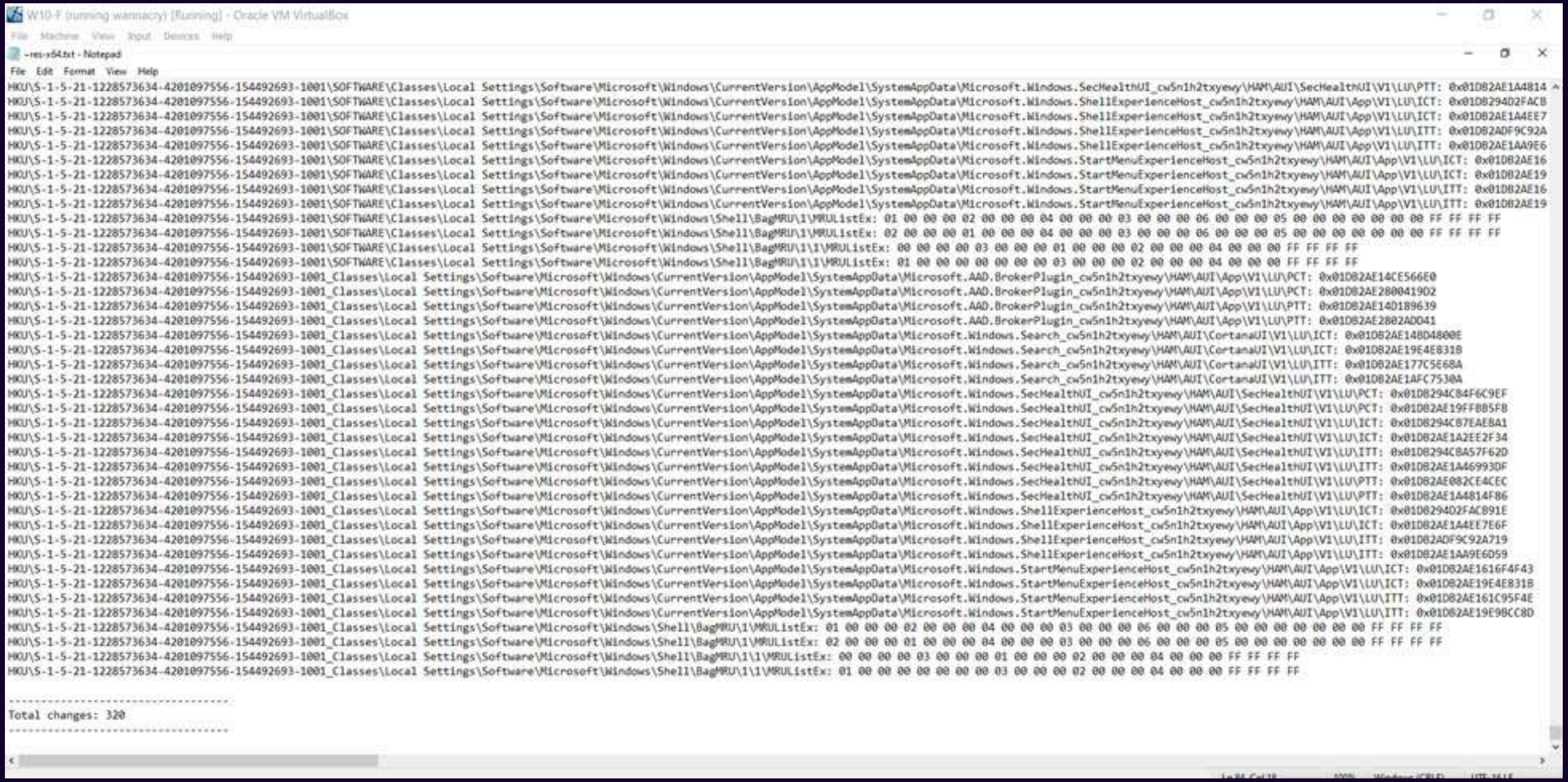

W10-F (running wannacry) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~res-x64.txt - Notepad
File Edit Format View Help
Type here to search
1:19 AM
10/31/2024

```
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\41\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\.WNCRY
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\WNCRY_auto_file
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\WNCRY_auto_file\shell
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\WNCRY_auto_file\shell\edit
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\WNCRY_auto_file\shell\edit\command
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\WNCRY_auto_file\shell\open
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\WNCRY_auto_file\shell\open\command

----------------------------------
Values deleted: 3
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\BITS\PerfMMFileName: "Global\MMF_BITS89a080c4-8aa1-410e-af23-8ec9a9c609e7"
HKLM\SOFTWARE\Microsoft\Windows Defender\ServiceStartStates: 0x00000001
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000060388\VirtualDesktop: 10 00 00 00 30 30 44 56 BC 77 33 9E A5 B8 89 42 9B 35 E0 16

----------------------------------
Values added: 131
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3408\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3408\Reason: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3408\CreationTime: 0x01DB2AE1A47E67C1
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4276\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4276\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4276\CreationTime: 0x01DB2AE280265682
HKLM\SOFTWARE\Microsoft\Windows Defender\Reporting\LastRtpTurnedOffTime: C4 94 62 A3 E1 2A DB 01
HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\UsageStats\Daily\Counts\core_worker_succeeded: 01 00 00 00 00 00 00 00
HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\UsageStats\Daily\Counts\core_worker_total: 01 00 00 00 00 00 00 00
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\jskosfyehgv856: ""C:\Users\retaj\Desktop\malware project\tasksche.exe""
HKLM\SOFTWARE\WOW6432Node\WanaCrypt0r\wd: "C:\Users\retaj\Desktop\malware project"
HKLM\SYSTEM\ControlSet001\Control\Session Manager\PendingFileRenameOperations: 5C 00 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 72 00 65 00 74 00 61 00 6A 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C
00 68 00 74 00 6F 00 70 00 5C 00 50 00 53 00 5F 00 54 00 72 00 61 00 6E 00 73 00 63 00 72 00 69 00 70 00 74 00 73 00 5C 00 32 00 30 00 32 00 34 00 30 00 39 00 30 00 31 00 5C 00 50 00 6F 00 77 00 65 00 72 00 53 00 68 00 65 00 6C 00 6C 00
0 00 74 00 2E 00 44 00 45 00 53 00 4B 00 54 00 4F 00 50 00 2D 00 4D 00 53 00 56 00 31 00 42 00 42 00 45 00 2E 00 68 00 65 00 39 00 4C 00 63 00 42 00 4C 00 53 00 2E 00 32 00 30 00 32 00 34 00 30 00 39 00 30 00 31 00 30 00 32 00 34 00 30 0
 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 72 00 65 00 74 00 61 00 6A 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 50 00 53 00 5F 00 54 00 72 00 61 00 6E 00 73 00 63 00 72 00 69 00 70 00 74 00 73
00 5C 00 50 00 6F 00 77 00 65 00 72 00 53 00 68 00 65 00 6C 00 6C 00 5F 00 74 00 72 00 61 00 6E 00 73 00 63 00 72 00 69 00 70 00 74 00 2E 00 44 00 45 00 53 00 4B 00 54 00 4F 00 50 00 2D 00 4D 00 53 00 56 00 31 00 42 00 42 00 45 00 2E 00
2 00 30 00 32 00 34 00 30 00 39 00 30 00 34 00 31 00 37 00 35 00 34 00 30 00 36 00 2E 00 74 00 78 00 74 00 00 00 00 00 5C 00 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 72 00 65 00 74 00 61 00 6A 00 5C 00 44 0
 5F 00 54 00 72 00 61 00 6E 00 73 00 63 00 72 00 69 00 70 00 74 00 73 00 5C 00 32 00 30 00 32 00 34 00 30 00 39 00 31 00 34 00 5C 00 50 00 6F 00 77 00 65 00 72 00 53 00 68 00 65 00 6C 00 6C 00 5F 00 74 00 72 00 61 00 6E 00 73 00 63 00 72
00 4F 00 50 00 2D 00 4D 00 53 00 56 00 31 00 42 00 42 00 45 00 2E 00 41 00 65 00 50 00 62 00 56 00 36 00 42 00 73 00 2E 00 32 00 30 00 32 00 34 00 31 00 30 00 32 00 38 00 31 00 36 00 31 00 37 00 33 00 39 00 2E 00 74 00 78 00 74 00 00 00
C 00 62 00 72 00 62 00 62 00 6F 00 74 00 2E 00 7A 00 69 00 70 00 00 00 00 00 5C 00 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 72 00 65 00 74 00 61 00 6A 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 0
 69 00 70 00 00 00 00 00 5C 00 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 72 00 65 00 74 00 61 00 6A 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 53 00 61 00 6D 00 70 00 6C 00 65 00 73 00 2E 00 7A
00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 72 00 65 00 74 00 61 00 6A 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 53 00 61 00 6D 00 70 00 6C 00 65 00 73 00 5C 00 53 00 61 00 6D 00 70 00 6C 00 65 00 5F 00 70 00
4 00 78 00 74 00 00 00 00 00 5C 00 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 72 00 65 00 74 00 61 00 6A 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 72 00 65 00 74 00 61 00 6A 00 2E 00 74 00 78 0
 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 72 00 65 00 74 00 61 00 6A 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 77 00 69 00 6E 00 33 00 32 00 5C 00 70 00 6C 00 75 00 67 00 69 00 6E 00 73 00 5C 00 73 00 65 00 72 00 76 00 65
00 75 00 67 00 69 00 6E 00 73 00 5C 00 6C 00 69 00 63 00 65 00 6E 00 73 00 65 00 73 00 5C 00 6C 00 69 00 63 00 65 00 6E 00 73 00 65 00 5F 00 70 00 63 00 61 00 70 00 5F 00 74 00 6F 00 6F 00 6C 00 73 00 2E 00 74 00 78 00 74 00 00 00 00 00
3 00 65 00 6E 00 73 00 65 00 5F 00 74 00 63 00 70 00 66 00 6C 00 6F 00 77 00 2E 00 74 00 78 00 74 00 00 00 00 00 5C 00 3F 00 3F 00 5C 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 72 00 65 00 74 00 61 00 6A 00 5C 00 44 00 65 0
 3F 00 5C 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 72 00 65 00 74 00 61 00 6A 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 77 00 69 00 6E 00 33 00 32 00 5C 00 70 00 6C 00 75 00 67 00 69 00 6E 00 73 00 5C 00 70
```


W10-F (running wannacry) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~res-x64.txt - Notepad
File Edit Format View Help
Type here to search
1:19 AM
10/31/2024

```
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\41\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\FFlags: 0x00000001
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\41\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\IconSize: 0x00000010
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\41\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Sort: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 30 F1 25 B7
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\41\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\ColInfo: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FD DF DF FD 10 00 00
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\41\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupView: 0x00000000
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\41\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey:FMTID: "{00000000-0000-0000-0000-000000000000}"
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\41\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByKey:PID: 0x00000000
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\41\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\GroupByDirection: 0x00000001
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\.WNCRY\: "WNCRY_auto_file"
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\WNCRY_auto_file\shell\edit\command\: "%SystemRoot%\system32\NOTEPAD.EXE %1"
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\WNCRY_auto_file\shell\open\command\: "%SystemRoot%\system32\NOTEPAD.EXE %1"

----------------------------------
Values modified: 125
----------------------------------
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\LastLogTime: 0x01DB293CDFEAFB05
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\LastLogTime: 0x01DB2AE189F7D336
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render: 53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 00 50 00 49 00 5C 00 7B 00 30 00 2E 00 30 00 2E 00 30 00 2E 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 7D 00 2E 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render: 53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 00 50 00 49 00 5C 00 7B 00 30 00 2E 00 30 00 2E 00 30 00 2E 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 7D 00 2E 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
HKLM\SOFTWARE\Microsoft\Security Center\Provider\Av\{D68DDC3A-831F-4fae-9E44-DA132C1ACF46}\STATE: 0x00061100
HKLM\SOFTWARE\Microsoft\Security Center\Provider\Av\{D68DDC3A-831F-4fae-9E44-DA132C1ACF46}\STATE: 0x00062100
HKLM\SOFTWARE\Microsoft\SMB1Uninstall\SMB1ClientCounter: 0x000000AD
HKLM\SOFTWARE\Microsoft\SMB1Uninstall\SMB1ClientCounter: 0x000000AE
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\DiagTrackStatus: 0x00000003
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\DiagTrackStatus: 0x00000002
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\Aggregation\Instrumentation\CodeIntegrityAggregator\HbActiveMillis: 0x00000000006DDCFA
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\Aggregation\Instrumentation\CodeIntegrityAggregator\HbActiveMillis: 0x0000000000124F64
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\Aggregation\Instrumentation\CodeIntegrityAggregator\HbEventsEnabled: 0x000000000000008D
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\Aggregation\Instrumentation\CodeIntegrityAggregator\HbEventsEnabled: 0x000000000000008A
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\Aggregation\Instrumentation\CodeIntegrityAggregator\HbNonTelEventsEnabled: 0x000000000000008D
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\Aggregation\Instrumentation\CodeIntegrityAggregator\HbNonTelEventsEnabled: 0x000000000000008A
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\Aggregation\Instrumentation\CodeIntegrityAggregator\HbProcessed: 0x000000000000008D
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\Aggregation\Instrumentation\CodeIntegrityAggregator\HbProcessed: 0x000000000000008A
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\SettingsRequests\LastDownloadTime: 0x01DB293E9C432F08
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\SettingsRequests\LastDownloadTime: 0x01DB2AE223F8C364
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x00000013
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x00000014
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime: 0x01DB2AE16DBCEA87
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime: 0x01DB2AE2AD8A9189
HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75: 14 0A 00 00 00 00 00 00 04 00 04 00 01 00 01 00 01 01 00 00 A5 AD CF 00 5C 00 02 00 00 00 02 38 8F 02 02 99 66 00 02 E6 38 01 09 2B BE 02 0D A1 81 00
E 02 C2 0C 5B 02 C3 6D 81 00 C3 99 F3 00 C7 5D D7 00 C7 E1 9F 02 CA 99 CE 00 CB 27 AA 02 CC 49 56 00 CD AD 05 01 CF 67 69 01 D0 17 56 00 D7 3D E8 02 D9 07 24 01 DB 26 D8 01 DD 2C 0D 03 E0 42 E4 02 E0 61 C3 02 E1 D9 F5 02 E6 6C 81 00 ED 4
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75: 42 0A 00 00 00 00 00 00 04 00 04 00 01 00 01 00 01 01 00 00 A5 AD CF 00 9B 00 02 00 00 00 02 38 8F 02 02 99 66 00 02 E6 38 01 03 81 22 01 05 61 8F 01
```

# Behavior Analysis

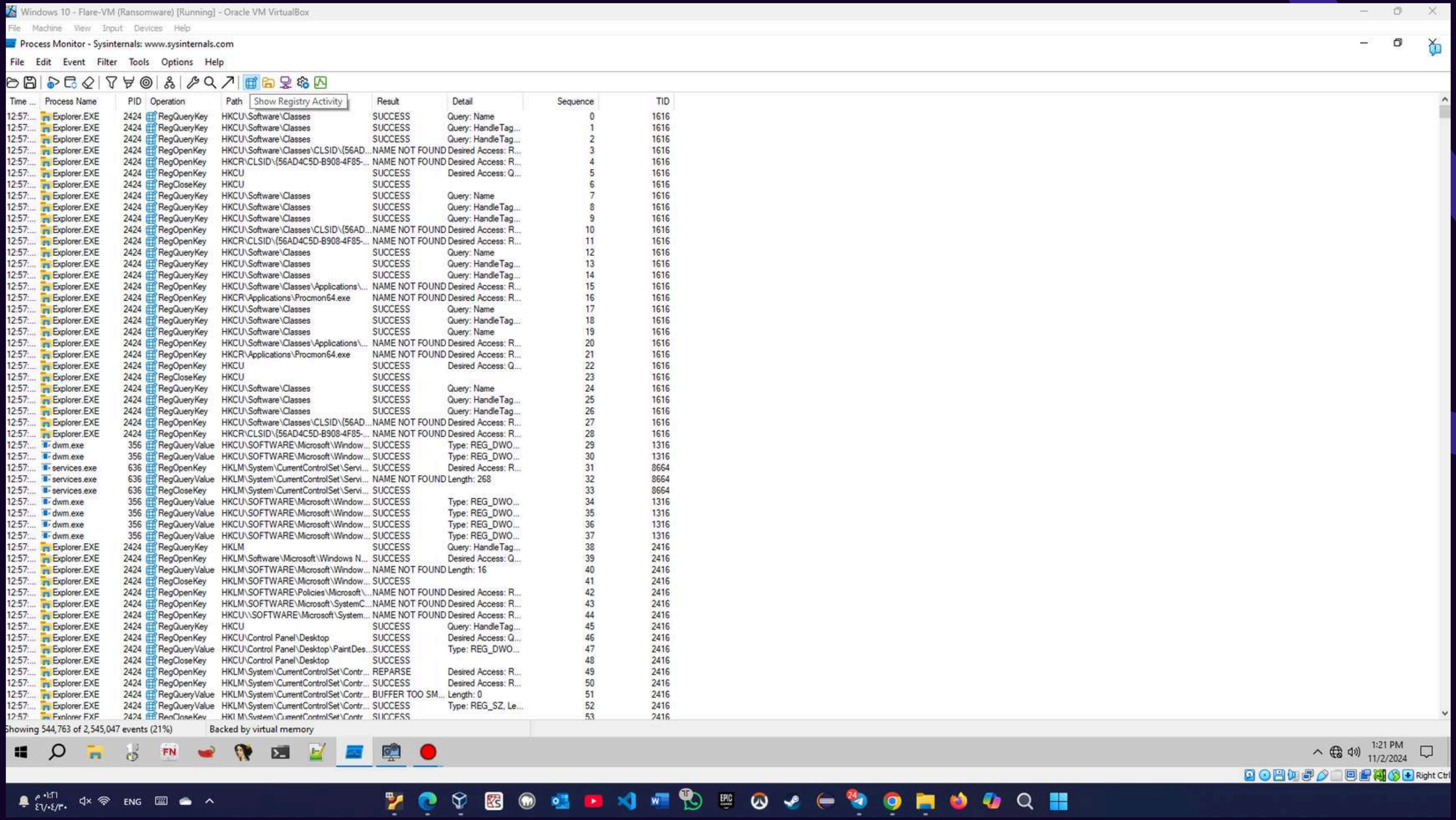


W10-F (running wannacry) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~res-x64.txt - Notepad
File Edit Format View Help

```
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\HAM\AUI\SecHealthUI\V1\LU\PTT: 0x01D82AE1A4814
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 0x01D8294D2FACB
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 0x01D82AE1A4EE7
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 0x01D82ADF9C92A
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 0x01D82AE1AA9E6
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 0x01D82AE16
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 0x01D82AE19
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 0x01D82AE16
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 0x01D82AE19
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\MRUListEx: 01 00 00 00 02 00 00 00 04 00 00 00 03 00 00 00 06 00 00 00 05 00 00 00 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\MRUListEx: 02 00 00 00 01 00 00 00 04 00 00 00 03 00 00 00 06 00 00 00 05 00 00 00 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\MRUListEx: 00 00 00 00 03 00 00 00 01 00 00 00 02 00 00 00 04 00 00 00 FF FF FF FF
HKU\S-1-5-21-1228573634-4201097556-154492693-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\MRUListEx: 01 00 00 00 00 00 00 00 03 00 00 00 02 00 00 00 04 00 00 00 FF FF FF FF
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\HAM\AUI\App\V1\LU\PCT: 0x01D82AE14CE566E0
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\HAM\AUI\App\V1\LU\PCT: 0x01D82AE280041902
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\HAM\AUI\App\V1\LU\PTT: 0x01D82AE14D189639
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\HAM\AUI\App\V1\LU\PTT: 0x01D82AE2802ADD41
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Search_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ICT: 0x01D82AE148D4800E
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Search_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ICT: 0x01D82AE19E4E831B
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Search_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ITT: 0x01D82AE177C5E68A
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Search_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ITT: 0x01D82AE1AFC7530A
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\HAM\AUI\SecHealthUI\V1\LU\PCT: 0x01D8294C84F6C9EF
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\HAM\AUI\SecHealthUI\V1\LU\PCT: 0x01D82AE19FFB85FB
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\HAM\AUI\SecHealthUI\V1\LU\ICT: 0x01D8294C87EAEBA1
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\HAM\AUI\SecHealthUI\V1\LU\ICT: 0x01D82AE1A2EE2F34
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\HAM\AUI\SecHealthUI\V1\LU\ITT: 0x01D8294C8A57F62D
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\HAM\AUI\SecHealthUI\V1\LU\ITT: 0x01D82AE1A46993DF
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\HAM\AUI\SecHealthUI\V1\LU\PTT: 0x01D82AE082CE4CEC
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\HAM\AUI\SecHealthUI\V1\LU\PTT: 0x01D82AE1A4814F86
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 0x01D8294D2FAC891E
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 0x01D82AE1A4EE7E6F
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 0x01D82ADF9C92A719
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 0x01D82AE1AA9E6D59
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 0x01D82AE1616F4F43
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 0x01D82AE19E4E831B
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 0x01D82AE161C95F4E
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 0x01D82AE19E9BCC8D
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\MRUListEx: 01 00 00 00 02 00 00 00 04 00 00 00 03 00 00 00 06 00 00 00 05 00 00 00 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\MRUListEx: 02 00 00 00 01 00 00 00 04 00 00 00 03 00 00 00 06 00 00 00 05 00 00 00 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\MRUListEx: 00 00 00 00 03 00 00 00 01 00 00 00 02 00 00 00 04 00 00 00 FF FF FF FF
HKU\S-1-5-21-1228573634-4201097556-154492693-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\MRUListEx: 01 00 00 00 00 00 00 00 03 00 00 00 02 00 00 00 04 00 00 00 FF FF FF FF

----------------------------------
Total changes: 320
----------------------------------
```

# Behavior Analysis

## Show Registry activity

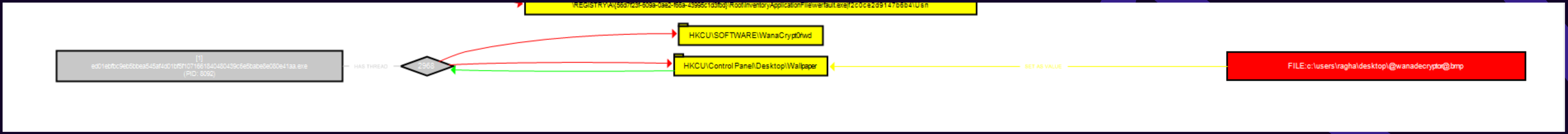

Windows 10 - Flare-VM (Ransomware) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Show Registry Activity
1:21 PM
11/2/2024
ENG
Right Ctrl

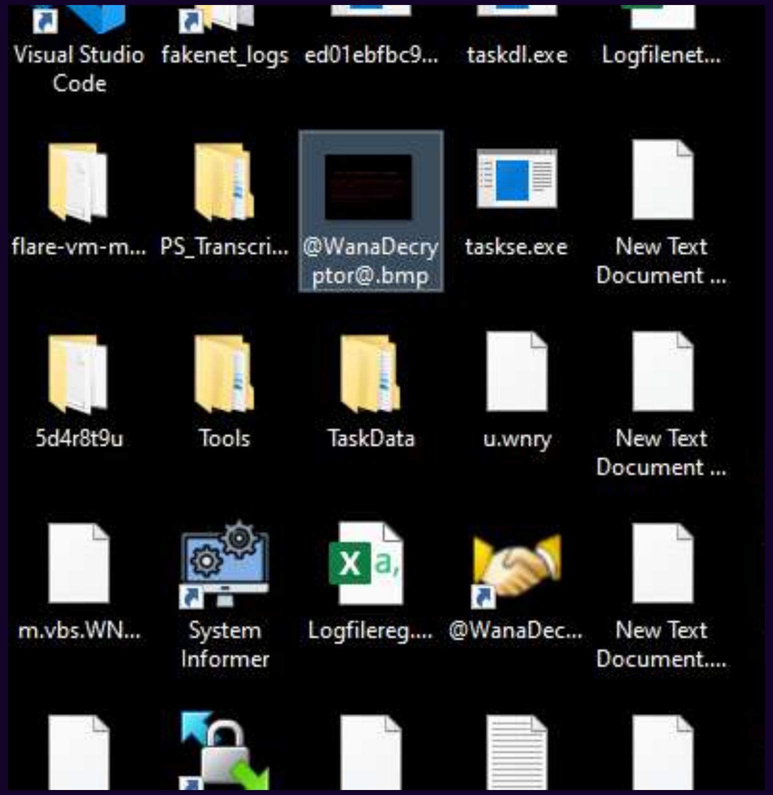
| Time ... | Process Name | PID | Operation | Path | Result | Detail | Sequence | TID |
|---|---|---|---|---|---|---|---|---|
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: Name | 0 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: HandleTag... | 1 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: HandleTag... | 2 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCU\Software\Classes\CLSID\{56AD... | NAME NOT FOUND | Desired Access: R... | 3 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCR\CLSID\{56AD4C5D-B908-4F85-... | NAME NOT FOUND | Desired Access: R... | 4 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCU | SUCCESS | Desired Access: Q... | 5 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegCloseKey | HKCU | SUCCESS |  | 6 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: Name | 7 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: HandleTag... | 8 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: HandleTag... | 9 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCU\Software\Classes\CLSID\{56AD... | NAME NOT FOUND | Desired Access: R... | 10 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCR\CLSID\{56AD4C5D-B908-4F85-... | NAME NOT FOUND | Desired Access: R... | 11 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: Name | 12 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: HandleTag... | 13 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: HandleTag... | 14 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCU\Software\Classes\Applications\... | NAME NOT FOUND | Desired Access: R... | 15 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCR\Applications\Procmon64.exe | NAME NOT FOUND | Desired Access: R... | 16 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: Name | 17 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: HandleTag... | 18 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: Name | 19 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCU\Software\Classes\Applications\... | NAME NOT FOUND | Desired Access: R... | 20 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCR\Applications\Procmon64.exe | NAME NOT FOUND | Desired Access: R... | 21 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCU | SUCCESS | Desired Access: Q... | 22 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegCloseKey | HKCU | SUCCESS |  | 23 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: Name | 24 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: HandleTag... | 25 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU\Software\Classes | SUCCESS | Query: HandleTag... | 26 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCU\Software\Classes\CLSID\{56AD... | NAME NOT FOUND | Desired Access: R... | 27 | 1616 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCR\CLSID\{56AD4C5D-B908-4F85-... | NAME NOT FOUND | Desired Access: R... | 28 | 1616 |
| 12:57:... | dwm.exe | 356 | RegQueryValue | HKCU\SOFTWARE\Microsoft\Window... | SUCCESS | Type: REG_DWO... | 29 | 1316 |
| 12:57:... | dwm.exe | 356 | RegQueryValue | HKCU\SOFTWARE\Microsoft\Window... | SUCCESS | Type: REG_DWO... | 30 | 1316 |
| 12:57:... | services.exe | 636 | RegOpenKey | HKLM\System\CurrentControlSet\Servi... | SUCCESS | Desired Access: R... | 31 | 8664 |
| 12:57:... | services.exe | 636 | RegQueryValue | HKLM\System\CurrentControlSet\Servi... | NAME NOT FOUND | Length: 268 | 32 | 8664 |
| 12:57:... | services.exe | 636 | RegCloseKey | HKLM\System\CurrentControlSet\Servi... | SUCCESS |  | 33 | 8664 |
| 12:57:... | dwm.exe | 356 | RegQueryValue | HKCU\SOFTWARE\Microsoft\Window... | SUCCESS | Type: REG_DWO... | 34 | 1316 |
| 12:57:... | dwm.exe | 356 | RegQueryValue | HKCU\SOFTWARE\Microsoft\Window... | SUCCESS | Type: REG_DWO... | 35 | 1316 |
| 12:57:... | dwm.exe | 356 | RegQueryValue | HKCU\SOFTWARE\Microsoft\Window... | SUCCESS | Type: REG_DWO... | 36 | 1316 |
| 12:57:... | dwm.exe | 356 | RegQueryValue | HKCU\SOFTWARE\Microsoft\Window... | SUCCESS | Type: REG_DWO... | 37 | 1316 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKLM | SUCCESS | Query: HandleTag... | 38 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKLM\Software\Microsoft\Windows N... | SUCCESS | Desired Access: Q... | 39 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Window... | NAME NOT FOUND | Length: 16 | 40 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegCloseKey | HKLM\SOFTWARE\Microsoft\Window... | SUCCESS |  | 41 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKLM\SOFTWARE\Policies\Microsoft\... | NAME NOT FOUND | Desired Access: R... | 42 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKLM\SOFTWARE\Microsoft\SystemC... | NAME NOT FOUND | Desired Access: R... | 43 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCU\\SOFTWARE\Microsoft\System... | NAME NOT FOUND | Desired Access: R... | 44 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryKey | HKCU | SUCCESS | Query: HandleTag... | 45 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKCU\Control Panel\Desktop | SUCCESS | Desired Access: Q... | 46 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryValue | HKCU\Control Panel\Desktop\PaintDes... | SUCCESS | Type: REG_DWO... | 47 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegCloseKey | HKCU\Control Panel\Desktop | SUCCESS |  | 48 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | REPARSE | Desired Access: R... | 49 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | Desired Access: R... | 50 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryValue | HKLM\System\CurrentControlSet\Contr... | BUFFER TOO SM... | Length: 0 | 51 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegQueryValue | HKLM\System\CurrentControlSet\Contr... | SUCCESS | Type: REG_SZ, Le... | 52 | 2416 |
| 12:57:... | Explorer.EXE | 2424 | RegCloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS |  | 53 | 2416 |

Showing 544,763 of 2,545,047 events (21%) Backed by virtual memory

# Behavior Analysis

## ProcDot tool:

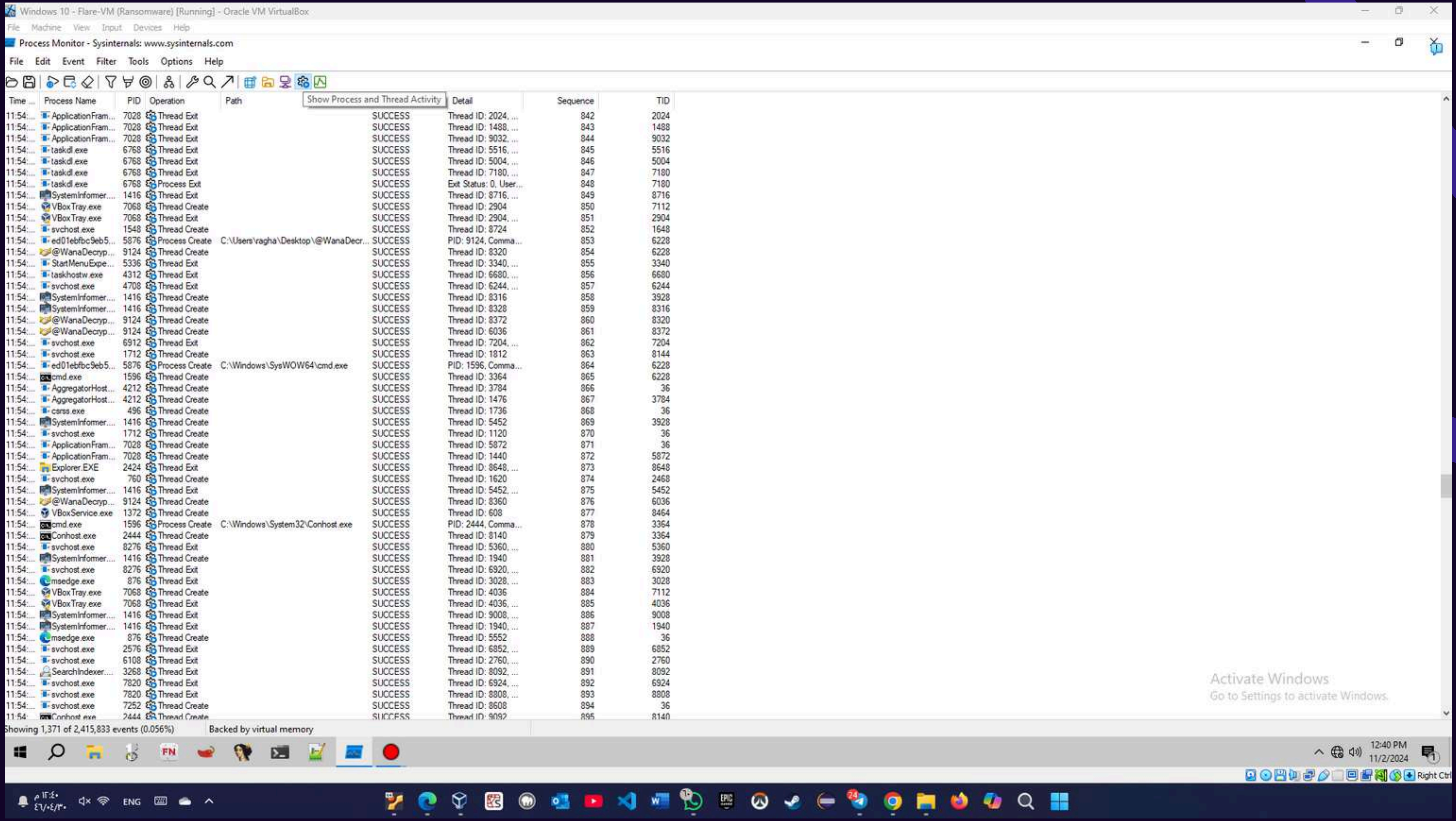

\REGISTRY\A\{56d7f23f-609a-0ae2-f66a-43995c1d3fbd}\Root\InventoryApplicationFile\werfault.exe|f2c0ce2d9147b6b4\Usn
[1]
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
(PID: 8092)
HAS THREAD
2968
HKCU\SOFTWARE\WanaCrypt0r\wd
HKCU\Control Panel\Desktop\Wallpaper
SET AS VALUE
FILE:c:\users\ragha\desktop\@wanadecryptor@.bmp



This is the ransom note image created by WannaCry ransomware.

# Behavior Analysis

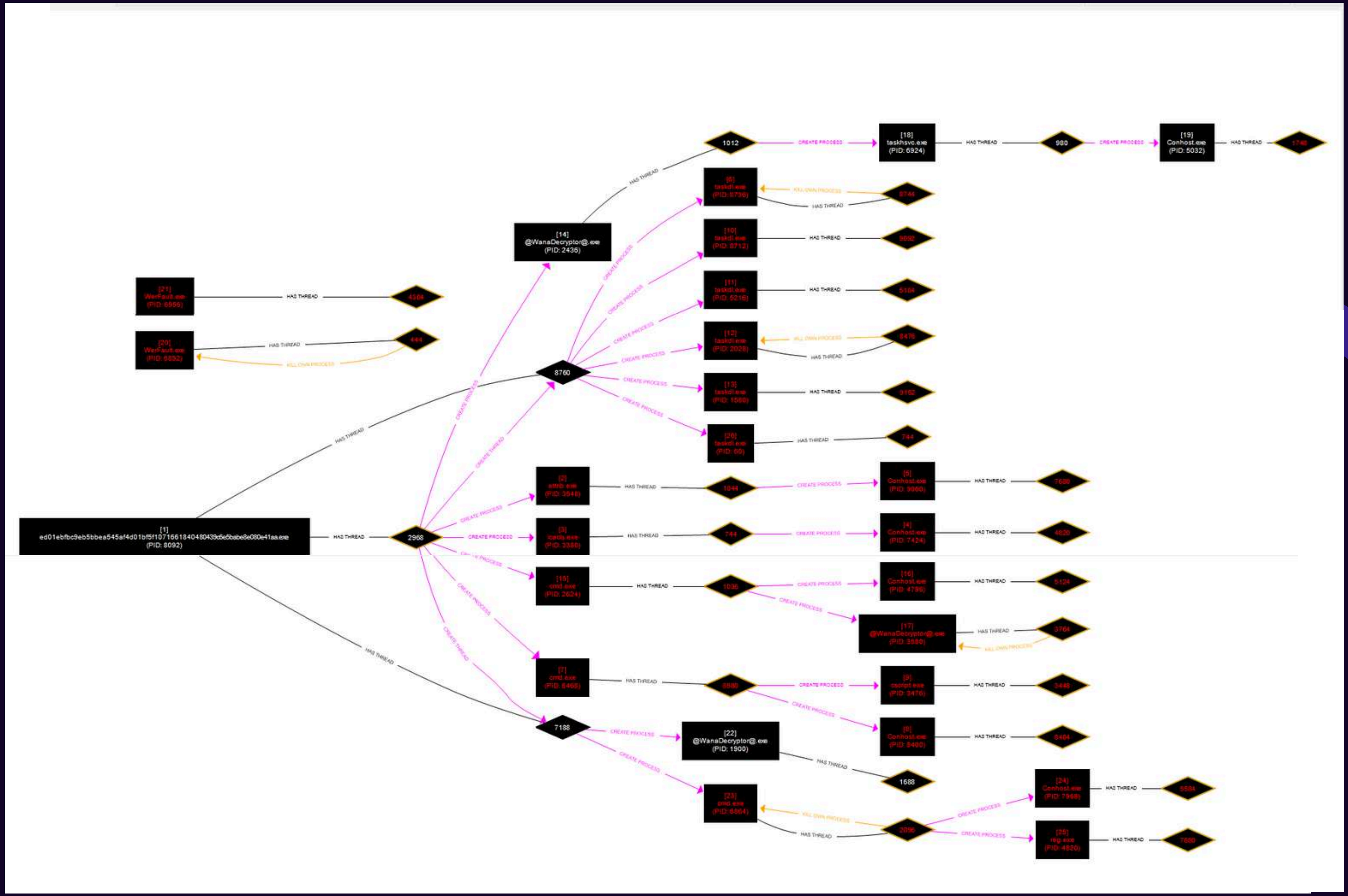
## Show process and thread activity


Windows 10 - Flare-VM (Ransomware) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Show Process and Thread Activity
Activate Windows
Go to Settings to activate Windows.
12:40 PM
11/2/2024
Right Ctrl

| Time ... | Process Name | PID | Operation | Path | | Detail | Sequence | TID |
|---|---|---|---|---|---|---|---|---|
| 11:54:... | ApplicationFram... | 7028 | Thread Exit | | SUCCESS | Thread ID: 2024, ... | 842 | 2024 |
| 11:54:... | ApplicationFram... | 7028 | Thread Exit | | SUCCESS | Thread ID: 1488, ... | 843 | 1488 |
| 11:54:... | ApplicationFram... | 7028 | Thread Exit | | SUCCESS | Thread ID: 9032, ... | 844 | 9032 |
| 11:54:... | taskdl.exe | 6768 | Thread Exit | | SUCCESS | Thread ID: 5516, ... | 845 | 5516 |
| 11:54:... | taskdl.exe | 6768 | Thread Exit | | SUCCESS | Thread ID: 5004, ... | 846 | 5004 |
| 11:54:... | taskdl.exe | 6768 | Thread Exit | | SUCCESS | Thread ID: 7180, ... | 847 | 7180 |
| 11:54:... | taskdl.exe | 6768 | Process Exit | | SUCCESS | Exit Status: 0, User... | 848 | 7180 |
| 11:54:... | SystemInformer.... | 1416 | Thread Exit | | SUCCESS | Thread ID: 8716, ... | 849 | 8716 |
| 11:54:... | VBoxTray.exe | 7068 | Thread Create | | SUCCESS | Thread ID: 2904 | 850 | 7112 |
| 11:54:... | VBoxTray.exe | 7068 | Thread Exit | | SUCCESS | Thread ID: 2904, ... | 851 | 2904 |
| 11:54:... | svchost.exe | 1548 | Thread Create | | SUCCESS | Thread ID: 8724 | 852 | 1648 |
| 11:54:... | ed01ebfbc9eb5... | 5876 | Process Create | C:\Users\ragha\Desktop\@WanaDecr... | SUCCESS | PID: 9124, Comma... | 853 | 6228 |
| 11:54:... | @WanaDecryp... | 9124 | Thread Create | | SUCCESS | Thread ID: 8320 | 854 | 6228 |
| 11:54:... | StartMenuExpe... | 5336 | Thread Exit | | SUCCESS | Thread ID: 3340, ... | 855 | 3340 |
| 11:54:... | taskhostw.exe | 4312 | Thread Exit | | SUCCESS | Thread ID: 6680, ... | 856 | 6680 |
| 11:54:... | svchost.exe | 4708 | Thread Exit | | SUCCESS | Thread ID: 6244, ... | 857 | 6244 |
| 11:54:... | SystemInformer.... | 1416 | Thread Create | | SUCCESS | Thread ID: 8316 | 858 | 3928 |
| 11:54:... | SystemInformer.... | 1416 | Thread Create | | SUCCESS | Thread ID: 8328 | 859 | 8316 |
| 11:54:... | @WanaDecryp... | 9124 | Thread Create | | SUCCESS | Thread ID: 8372 | 860 | 8320 |
| 11:54:... | @WanaDecryp... | 9124 | Thread Create | | SUCCESS | Thread ID: 6036 | 861 | 8372 |
| 11:54:... | svchost.exe | 6912 | Thread Exit | | SUCCESS | Thread ID: 7204, ... | 862 | 7204 |
| 11:54:... | svchost.exe | 1712 | Thread Create | | SUCCESS | Thread ID: 1812 | 863 | 8144 |
| 11:54:... | ed01ebfbc9eb5... | 5876 | Process Create | C:\Windows\SysWOW64\cmd.exe | SUCCESS | PID: 1596, Comma... | 864 | 6228 |
| 11:54:... | cmd.exe | 1596 | Thread Create | | SUCCESS | Thread ID: 3364 | 865 | 6228 |
| 11:54:... | AggregatorHost... | 4212 | Thread Create | | SUCCESS | Thread ID: 3784 | 866 | 36 |
| 11:54:... | AggregatorHost... | 4212 | Thread Create | | SUCCESS | Thread ID: 1476 | 867 | 3784 |
| 11:54:... | csrss.exe | 496 | Thread Create | | SUCCESS | Thread ID: 1736 | 868 | 36 |
| 11:54:... | SystemInformer.... | 1416 | Thread Create | | SUCCESS | Thread ID: 5452 | 869 | 3928 |
| 11:54:... | svchost.exe | 1712 | Thread Create | | SUCCESS | Thread ID: 1120 | 870 | 36 |
| 11:54:... | ApplicationFram... | 7028 | Thread Create | | SUCCESS | Thread ID: 5872 | 871 | 36 |
| 11:54:... | ApplicationFram... | 7028 | Thread Create | | SUCCESS | Thread ID: 1440 | 872 | 5872 |
| 11:54:... | Explorer.EXE | 2424 | Thread Exit | | SUCCESS | Thread ID: 8648, ... | 873 | 8648 |
| 11:54:... | svchost.exe | 760 | Thread Create | | SUCCESS | Thread ID: 1620 | 874 | 2468 |
| 11:54:... | SystemInformer.... | 1416 | Thread Exit | | SUCCESS | Thread ID: 5452, ... | 875 | 5452 |
| 11:54:... | @WanaDecryp... | 9124 | Thread Create | | SUCCESS | Thread ID: 8360 | 876 | 6036 |
| 11:54:... | VBoxService.exe | 1372 | Thread Create | | SUCCESS | Thread ID: 608 | 877 | 8464 |
| 11:54:... | cmd.exe | 1596 | Process Create | C:\Windows\System32\Conhost.exe | SUCCESS | PID: 2444, Comma... | 878 | 3364 |
| 11:54:... | Conhost.exe | 2444 | Thread Create | | SUCCESS | Thread ID: 8140 | 879 | 3364 |
| 11:54:... | svchost.exe | 8276 | Thread Exit | | SUCCESS | Thread ID: 5360, ... | 880 | 5360 |
| 11:54:... | SystemInformer.... | 1416 | Thread Create | | SUCCESS | Thread ID: 1940 | 881 | 3928 |
| 11:54:... | svchost.exe | 8276 | Thread Exit | | SUCCESS | Thread ID: 6920, ... | 882 | 6920 |
| 11:54:... | msedge.exe | 876 | Thread Exit | | SUCCESS | Thread ID: 3028, ... | 883 | 3028 |
| 11:54:... | VBoxTray.exe | 7068 | Thread Create | | SUCCESS | Thread ID: 4036 | 884 | 7112 |
| 11:54:... | VBoxTray.exe | 7068 | Thread Exit | | SUCCESS | Thread ID: 4036, ... | 885 | 4036 |
| 11:54:... | SystemInformer.... | 1416 | Thread Exit | | SUCCESS | Thread ID: 9008, ... | 886 | 9008 |
| 11:54:... | SystemInformer.... | 1416 | Thread Exit | | SUCCESS | Thread ID: 1940, ... | 887 | 1940 |
| 11:54:... | msedge.exe | 876 | Thread Create | | SUCCESS | Thread ID: 5552 | 888 | 36 |
| 11:54:... | svchost.exe | 2576 | Thread Exit | | SUCCESS | Thread ID: 6852, ... | 889 | 6852 |
| 11:54:... | svchost.exe | 6108 | Thread Exit | | SUCCESS | Thread ID: 2760, ... | 890 | 2760 |
| 11:54:... | SearchIndexer.... | 3268 | Thread Exit | | SUCCESS | Thread ID: 8092, ... | 891 | 8092 |
| 11:54:... | svchost.exe | 7820 | Thread Exit | | SUCCESS | Thread ID: 6924, ... | 892 | 6924 |
| 11:54:... | svchost.exe | 7820 | Thread Exit | | SUCCESS | Thread ID: 8808, ... | 893 | 8808 |
| 11:54:... | svchost.exe | 7252 | Thread Create | | SUCCESS | Thread ID: 8608 | 894 | 36 |
| 11:54: | Conhost.exe | 2444 | Thread Create | | SUCCESS | Thread ID: 9092 | 895 | 8140 |

Showing 1,371 of 2,415,833 events (0.056%)    Backed by virtual memory

# Behavior Analysis


[1] ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe (PID: 8092)
HAS THREAD
2968
8760
7188
CREATE PROCESS
CREATE THREAD
KILL OWN PROCESS
[21] WerFault.exe (PID: 6956)
4384
[20] WerFault.exe (PID: 6892)
444
[14] @WanaDecryptor@.exe (PID: 2436)
1012
[18] taskhsvc.exe (PID: 6924)
980
[19] Conhost.exe (PID: 5032)
1748
[6] taskdl.exe (PID: 5736)
8744
[10] taskdl.exe (PID: 8712)
9092
[11] taskdl.exe (PID: 5216)
5184
[12] taskdl.exe (PID: 2028)
8476
[13] taskdl.exe (PID: 1560)
9162
[26] taskdl.exe (PID: 60)
744
[2] attrib.exe (PID: 3548)
1044
[5] Conhost.exe (PID: 9060)
7680
[3] icacls.exe (PID: 3380)
744
[4] Conhost.exe (PID: 7424)
4820
[15] cmd.exe (PID: 2624)
1036
[16] Conhost.exe (PID: 4796)
5124
[17] @WanaDecryptor@.exe (PID: 3580)
3764
[7] cmd.exe (PID: 6468)
5580
[9] cscript.exe (PID: 3476)
3448
[8] Conhost.exe (PID: 8400)
8484
[22] @WanaDecryptor@.exe (PID: 1900)
1688
[23] cmd.exe (PID: 6864)
2096
[24] Conhost.exe (PID: 7968)
5584
[25] reg.exe (PID: 4620)
7680

# Workflow of WannaCry Ransomware

# Identify Malicious API

Purpose:

Understand how the malware interacts with the system to perform harmful actions.

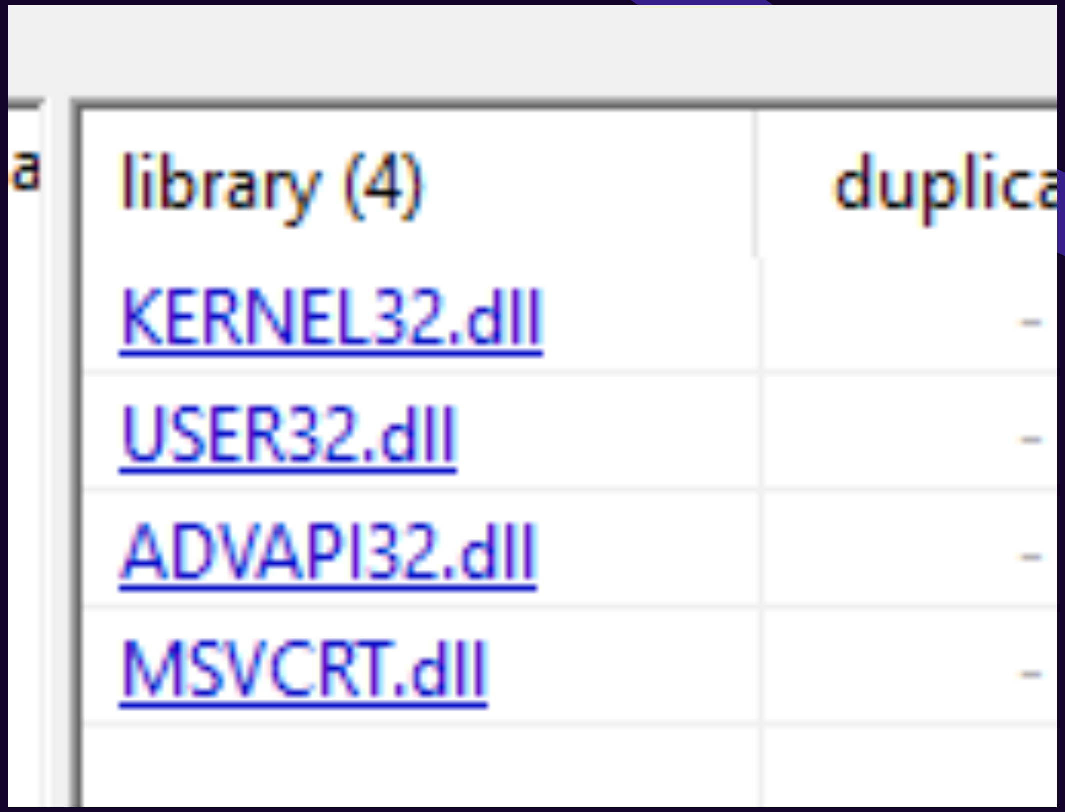
Tool Used:

pestudio

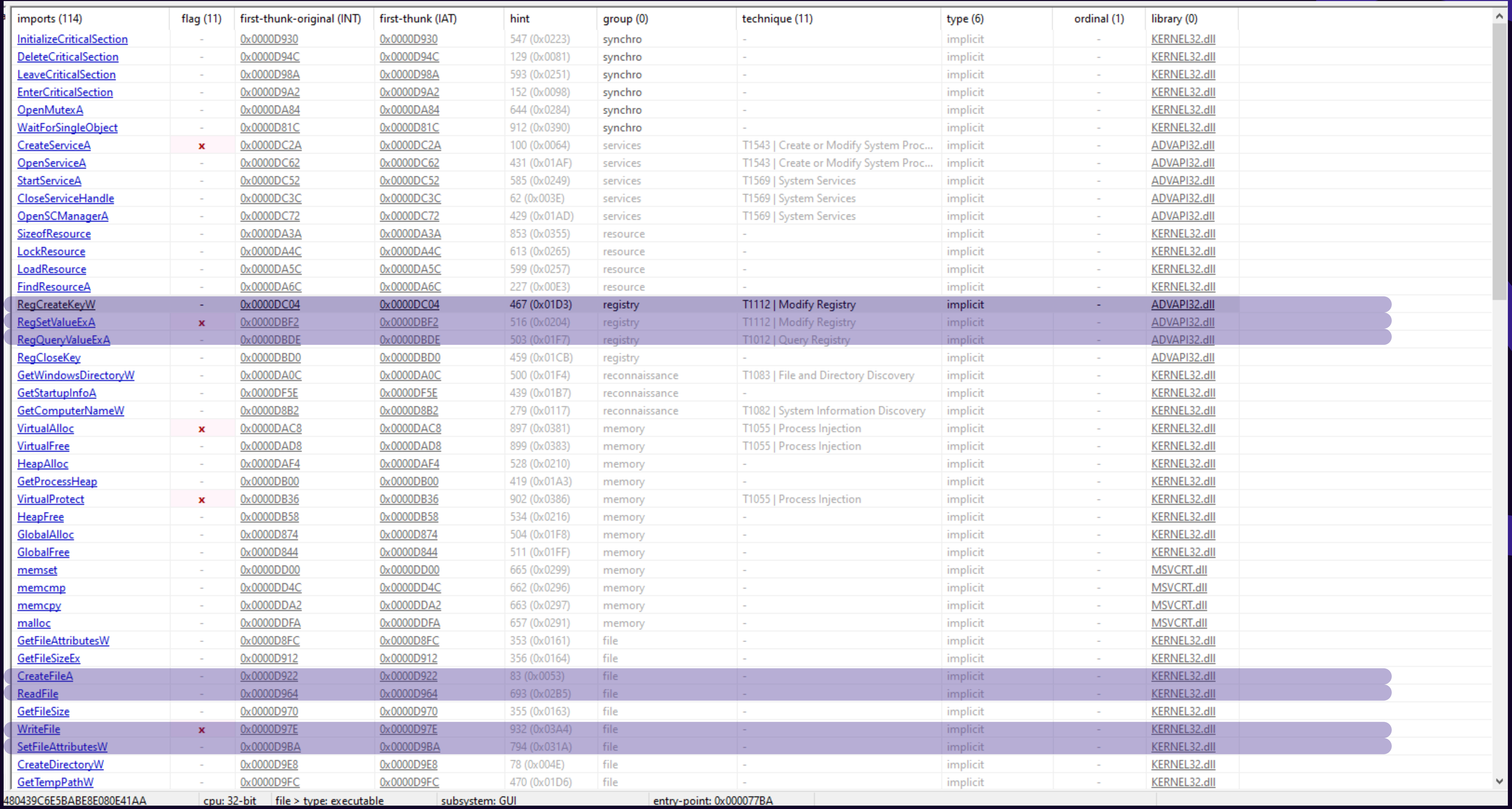
# Overview of the Listed DLLs

kernel32.dll: This library includes the basic and core functionality for all programs, including reading a file and writing a file.

advapi32.dll: This library is used mainly for working with the registry and cryptography

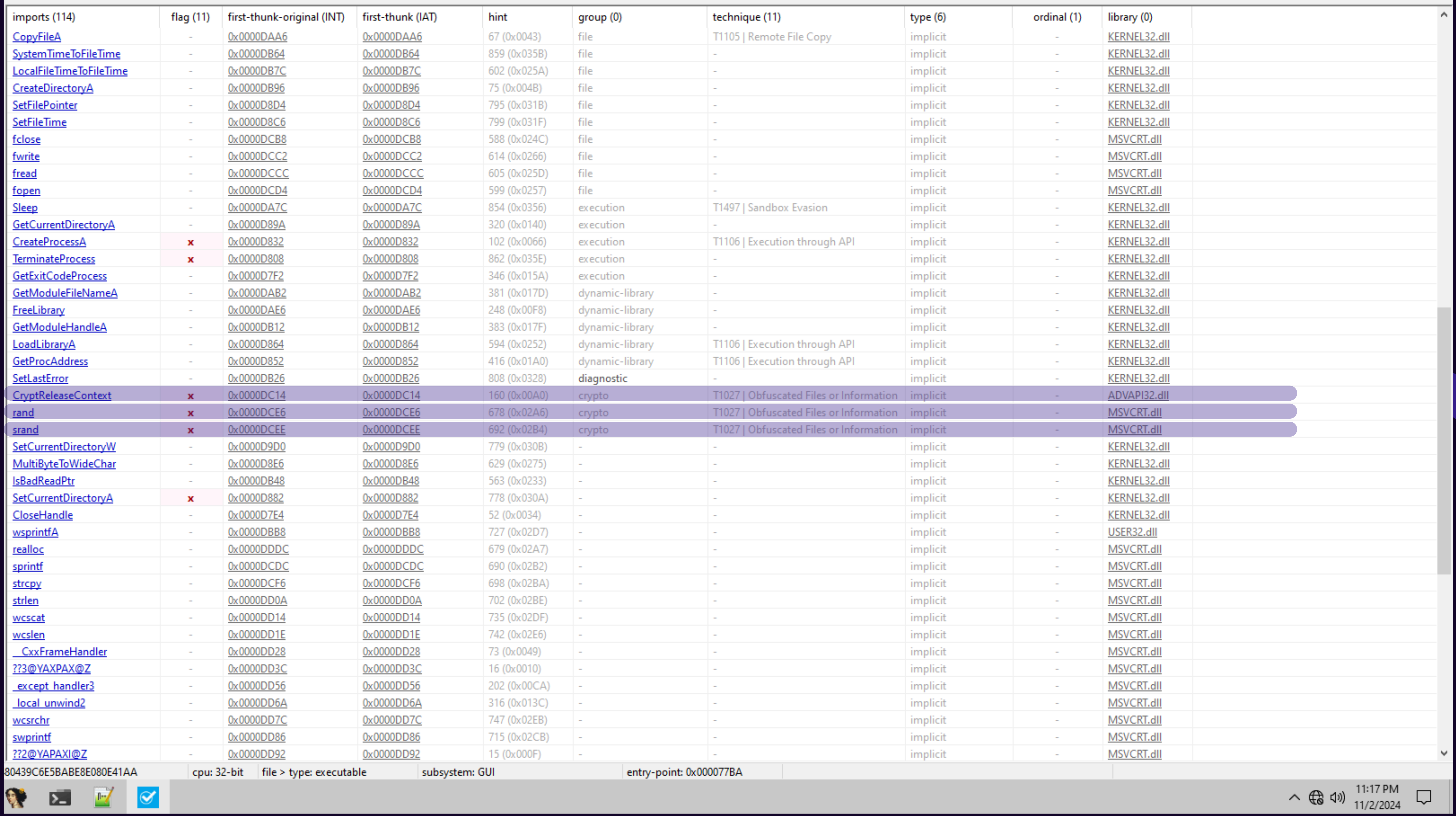


| a | library (4) | duplica |
|---|---|---|
| | KERNEL32.dll | - |
| | USER32.dll | - |
| | ADVAPI32.dll | - |
| | MSVCRT.dll | - |



| imports (114) | flag (11) | first-thunk-original (INT) | first-thunk (IAT) | hint | group (0) | technique (11) | type (6) | ordinal (1) | library (0) |
|---|---|---|---|---|---|---|---|---|---|
| InitializeCriticalSection | - | 0x0000D930 | 0x0000D930 | 547 (0x0223) | synchro | - | implicit | - | KERNEL32.dll |
| DeleteCriticalSection | - | 0x0000D94C | 0x0000D94C | 129 (0x0081) | synchro | - | implicit | - | KERNEL32.dll |
| LeaveCriticalSection | - | 0x0000D98A | 0x0000D98A | 593 (0x0251) | synchro | - | implicit | - | KERNEL32.dll |
| EnterCriticalSection | - | 0x0000D9A2 | 0x0000D9A2 | 152 (0x0098) | synchro | - | implicit | - | KERNEL32.dll |
| OpenMutexA | - | 0x0000DA84 | 0x0000DA84 | 644 (0x0284) | synchro | - | implicit | - | KERNEL32.dll |
| WaitForSingleObject | - | 0x0000D81C | 0x0000D81C | 912 (0x0390) | synchro | - | implicit | - | KERNEL32.dll |
| CreateServiceA | x | 0x0000DC2A | 0x0000DC2A | 100 (0x0064) | services | T1543 \| Create or Modify System Proc... | implicit | - | ADVAPI32.dll |
| OpenServiceA | - | 0x0000DC62 | 0x0000DC62 | 431 (0x01AF) | services | T1543 \| Create or Modify System Proc... | implicit | - | ADVAPI32.dll |
| StartServiceA | - | 0x0000DC52 | 0x0000DC52 | 585 (0x0249) | services | T1569 \| System Services | implicit | - | ADVAPI32.dll |
| CloseServiceHandle | - | 0x0000DC3C | 0x0000DC3C | 62 (0x003E) | services | T1569 \| System Services | implicit | - | ADVAPI32.dll |
| OpenSCManagerA | - | 0x0000DC72 | 0x0000DC72 | 429 (0x01AD) | services | T1569 \| System Services | implicit | - | ADVAPI32.dll |
| SizeofResource | - | 0x0000DA3A | 0x0000DA3A | 853 (0x0355) | resource | - | implicit | - | KERNEL32.dll |
| LockResource | - | 0x0000DA4C | 0x0000DA4C | 613 (0x0265) | resource | - | implicit | - | KERNEL32.dll |
| LoadResource | - | 0x0000DA5C | 0x0000DA5C | 599 (0x0257) | resource | - | implicit | - | KERNEL32.dll |
| FindResourceA | - | 0x0000DA6C | 0x0000DA6C | 227 (0x00E3) | resource | - | implicit | - | KERNEL32.dll |
| RegCreateKeyW | - | 0x0000DC04 | 0x0000DC04 | 467 (0x01D3) | registry | T1112 \| Modify Registry | implicit | - | ADVAPI32.dll |
| RegSetValueExA | x | 0x0000DBF2 | 0x0000DBF2 | 516 (0x0204) | registry | T1112 \| Modify Registry | implicit | - | ADVAPI32.dll |
| RegQueryValueExA | - | 0x0000DBDE | 0x0000DBDE | 503 (0x01F7) | registry | T1012 \| Query Registry | implicit | - | ADVAPI32.dll |
| RegCloseKey | - | 0x0000DBD0 | 0x0000DBD0 | 459 (0x01CB) | registry | - | implicit | - | ADVAPI32.dll |
| GetWindowsDirectoryW | - | 0x0000DA0C | 0x0000DA0C | 500 (0x01F4) | reconnaissance | T1083 \| File and Directory Discovery | implicit | - | KERNEL32.dll |
| GetStartupInfoA | - | 0x0000DF5E | 0x0000DF5E | 439 (0x01B7) | reconnaissance | - | implicit | - | KERNEL32.dll |
| GetComputerNameW | - | 0x0000D8B2 | 0x0000D8B2 | 279 (0x0117) | reconnaissance | T1082 \| System Information Discovery | implicit | - | KERNEL32.dll |
| VirtualAlloc | x | 0x0000DAC8 | 0x0000DAC8 | 897 (0x0381) | memory | T1055 \| Process Injection | implicit | - | KERNEL32.dll |
| VirtualFree | - | 0x0000DAD8 | 0x0000DAD8 | 899 (0x0383) | memory | T1055 \| Process Injection | implicit | - | KERNEL32.dll |
| HeapAlloc | - | 0x0000DAF4 | 0x0000DAF4 | 528 (0x0210) | memory | - | implicit | - | KERNEL32.dll |
| GetProcessHeap | - | 0x0000DB00 | 0x0000DB00 | 419 (0x01A3) | memory | - | implicit | - | KERNEL32.dll |
| VirtualProtect | x | 0x0000DB36 | 0x0000DB36 | 902 (0x0386) | memory | T1055 \| Process Injection | implicit | - | KERNEL32.dll |
| HeapFree | - | 0x0000DB58 | 0x0000DB58 | 534 (0x0216) | memory | - | implicit | - | KERNEL32.dll |
| GlobalAlloc | - | 0x0000D874 | 0x0000D874 | 504 (0x01F8) | memory | - | implicit | - | KERNEL32.dll |
| GlobalFree | - | 0x0000D844 | 0x0000D844 | 511 (0x01FF) | memory | - | implicit | - | KERNEL32.dll |
| memset | - | 0x0000DD00 | 0x0000DD00 | 665 (0x0299) | memory | - | implicit | - | MSVCRT.dll |
| memcmp | - | 0x0000DD4C | 0x0000DD4C | 662 (0x0296) | memory | - | implicit | - | MSVCRT.dll |
| memcpy | - | 0x0000DDA2 | 0x0000DDA2 | 663 (0x0297) | memory | - | implicit | - | MSVCRT.dll |
| malloc | - | 0x0000DDFA | 0x0000DDFA | 657 (0x0291) | memory | - | implicit | - | MSVCRT.dll |
| GetFileAttributesW | - | 0x0000D8FC | 0x0000D8FC | 353 (0x0161) | file | - | implicit | - | KERNEL32.dll |
| GetFileSizeEx | - | 0x0000D912 | 0x0000D912 | 356 (0x0164) | file | - | implicit | - | KERNEL32.dll |
| CreateFileA | - | 0x0000D922 | 0x0000D922 | 83 (0x0053) | file | - | implicit | - | KERNEL32.dll |
| ReadFile | - | 0x0000D964 | 0x0000D964 | 693 (0x02B5) | file | - | implicit | - | KERNEL32.dll |
| GetFileSize | - | 0x0000D970 | 0x0000D970 | 355 (0x0163) | file | - | implicit | - | KERNEL32.dll |
| WriteFile | x | 0x0000D97E | 0x0000D97E | 932 (0x03A4) | file | - | implicit | - | KERNEL32.dll |
| SetFileAttributesW | - | 0x0000D9BA | 0x0000D9BA | 794 (0x031A) | file | - | implicit | - | KERNEL32.dll |
| CreateDirectoryW | - | 0x0000D9E8 | 0x0000D9E8 | 78 (0x004E) | file | - | implicit | - | KERNEL32.dll |
| GetTempPathW | - | 0x0000D9FC | 0x0000D9FC | 470 (0x01D6) | file | - | implicit | - | KERNEL32.dll |

480439C6E5BABE8E080E41AA | cpu: 32-bit | file > type: executable | subsystem: GUI | entry-point: 0x000077BA



| imports (114) | flag (11) | first-thunk-original (INT) | first-thunk (IAT) | hint | group (0) | technique (11) | type (6) | ordinal (1) | library (0) |
|---|---|---|---|---|---|---|---|---|---|
| CopyFileA | - | 0x0000DAA6 | 0x0000DAA6 | 67 (0x0043) | file | T1105 \| Remote File Copy | implicit | - | KERNEL32.dll |
| SystemTimeToFileTime | - | 0x0000DB64 | 0x0000DB64 | 859 (0x035B) | file | - | implicit | - | KERNEL32.dll |
| LocalFileTimeToFileTime | - | 0x0000DB7C | 0x0000DB7C | 602 (0x025A) | file | - | implicit | - | KERNEL32.dll |
| CreateDirectoryA | - | 0x0000DB96 | 0x0000DB96 | 75 (0x004B) | file | - | implicit | - | KERNEL32.dll |
| SetFilePointer | - | 0x0000D8D4 | 0x0000D8D4 | 795 (0x031B) | file | - | implicit | - | KERNEL32.dll |
| SetFileTime | - | 0x0000D8C6 | 0x0000D8C6 | 799 (0x031F) | file | - | implicit | - | KERNEL32.dll |
| fclose | - | 0x0000DCB8 | 0x0000DCB8 | 588 (0x024C) | file | - | implicit | - | MSVCRT.dll |
| fwrite | - | 0x0000DCC2 | 0x0000DCC2 | 614 (0x0266) | file | - | implicit | - | MSVCRT.dll |
| fread | - | 0x0000DCCC | 0x0000DCCC | 605 (0x025D) | file | - | implicit | - | MSVCRT.dll |
| fopen | - | 0x0000DCD4 | 0x0000DCD4 | 599 (0x0257) | file | - | implicit | - | MSVCRT.dll |
| Sleep | - | 0x0000DA7C | 0x0000DA7C | 854 (0x0356) | execution | T1497 \| Sandbox Evasion | implicit | - | KERNEL32.dll |
| GetCurrentDirectoryA | - | 0x0000D89A | 0x0000D89A | 320 (0x0140) | execution | - | implicit | - | KERNEL32.dll |
| CreateProcessA | x | 0x0000D832 | 0x0000D832 | 102 (0x0066) | execution | T1106 \| Execution through API | implicit | - | KERNEL32.dll |
| TerminateProcess | x | 0x0000D808 | 0x0000D808 | 862 (0x035E) | execution | - | implicit | - | KERNEL32.dll |
| GetExitCodeProcess | - | 0x0000D7F2 | 0x0000D7F2 | 346 (0x015A) | execution | - | implicit | - | KERNEL32.dll |
| GetModuleFileNameA | - | 0x0000DAB2 | 0x0000DAB2 | 381 (0x017D) | dynamic-library | - | implicit | - | KERNEL32.dll |
| FreeLibrary | - | 0x0000DAE6 | 0x0000DAE6 | 248 (0x00F8) | dynamic-library | - | implicit | - | KERNEL32.dll |
| GetModuleHandleA | - | 0x0000DB12 | 0x0000DB12 | 383 (0x017F) | dynamic-library | - | implicit | - | KERNEL32.dll |
| LoadLibraryA | - | 0x0000D864 | 0x0000D864 | 594 (0x0252) | dynamic-library | T1106 \| Execution through API | implicit | - | KERNEL32.dll |
| GetProcAddress | - | 0x0000D852 | 0x0000D852 | 416 (0x01A0) | dynamic-library | T1106 \| Execution through API | implicit | - | KERNEL32.dll |
| SetLastError | - | 0x0000DB26 | 0x0000DB26 | 808 (0x0328) | diagnostic | - | implicit | - | KERNEL32.dll |
| CryptReleaseContext | x | 0x0000DC14 | 0x0000DC14 | 160 (0x00A0) | crypto | T1027 \| Obfuscated Files or Information | implicit | - | ADVAPI32.dll |
| rand | x | 0x0000DCE6 | 0x0000DCE6 | 678 (0x02A6) | crypto | T1027 \| Obfuscated Files or Information | implicit | - | MSVCRT.dll |
| srand | x | 0x0000DCEE | 0x0000DCEE | 692 (0x02B4) | crypto | T1027 \| Obfuscated Files or Information | implicit | - | MSVCRT.dll |
| SetCurrentDirectoryW | - | 0x0000D9D0 | 0x0000D9D0 | 779 (0x030B) | - | - | implicit | - | KERNEL32.dll |
| MultiByteToWideChar | - | 0x0000D8E6 | 0x0000D8E6 | 629 (0x0275) | - | - | implicit | - | KERNEL32.dll |
| IsBadReadPtr | - | 0x0000DB48 | 0x0000DB48 | 563 (0x0233) | - | - | implicit | - | KERNEL32.dll |
| SetCurrentDirectoryA | x | 0x0000D882 | 0x0000D882 | 778 (0x030A) | - | - | implicit | - | KERNEL32.dll |
| CloseHandle | - | 0x0000D7E4 | 0x0000D7E4 | 52 (0x0034) | - | - | implicit | - | KERNEL32.dll |
| wsprintfA | - | 0x0000DBB8 | 0x0000DBB8 | 727 (0x02D7) | - | - | implicit | - | USER32.dll |
| realloc | - | 0x0000DDDC | 0x0000DDDC | 679 (0x02A7) | - | - | implicit | - | MSVCRT.dll |
| sprintf | - | 0x0000DCDC | 0x0000DCDC | 690 (0x02B2) | - | - | implicit | - | MSVCRT.dll |
| strcpy | - | 0x0000DCF6 | 0x0000DCF6 | 698 (0x02BA) | - | - | implicit | - | MSVCRT.dll |
| strlen | - | 0x0000DD0A | 0x0000DD0A | 702 (0x02BE) | - | - | implicit | - | MSVCRT.dll |
| wcscat | - | 0x0000DD14 | 0x0000DD14 | 735 (0x02DF) | - | - | implicit | - | MSVCRT.dll |
| wcslen | - | 0x0000DD1E | 0x0000DD1E | 742 (0x02E6) | - | - | implicit | - | MSVCRT.dll |
| __CxxFrameHandler | - | 0x0000DD28 | 0x0000DD28 | 73 (0x0049) | - | - | implicit | - | MSVCRT.dll |
| ??3@YAXPAX@Z | - | 0x0000DD3C | 0x0000DD3C | 16 (0x0010) | - | - | implicit | - | MSVCRT.dll |
| _except_handler3 | - | 0x0000DD56 | 0x0000DD56 | 202 (0x00CA) | - | - | implicit | - | MSVCRT.dll |
| _local_unwind2 | - | 0x0000DD6A | 0x0000DD6A | 316 (0x013C) | - | - | implicit | - | MSVCRT.dll |
| wcsrchr | - | 0x0000DD7C | 0x0000DD7C | 747 (0x02EB) | - | - | implicit | - | MSVCRT.dll |
| swprintf | - | 0x0000DD86 | 0x0000DD86 | 715 (0x02CB) | - | - | implicit | - | MSVCRT.dll |
| ??2@YAPAXI@Z | - | 0x0000DD92 | 0x0000DD92 | 15 (0x000F) | - | - | implicit | - | MSVCRT.dll |

80439C6E5BABE8E080E41AA | cpu: 32-bit | file > type: executable | subsystem: GUI | entry-point: 0x000077BA

11:17 PM
11/2/2024

# Determining the File Architecture

Purpose:

Identifying the file architecture to choose the correct debugger.

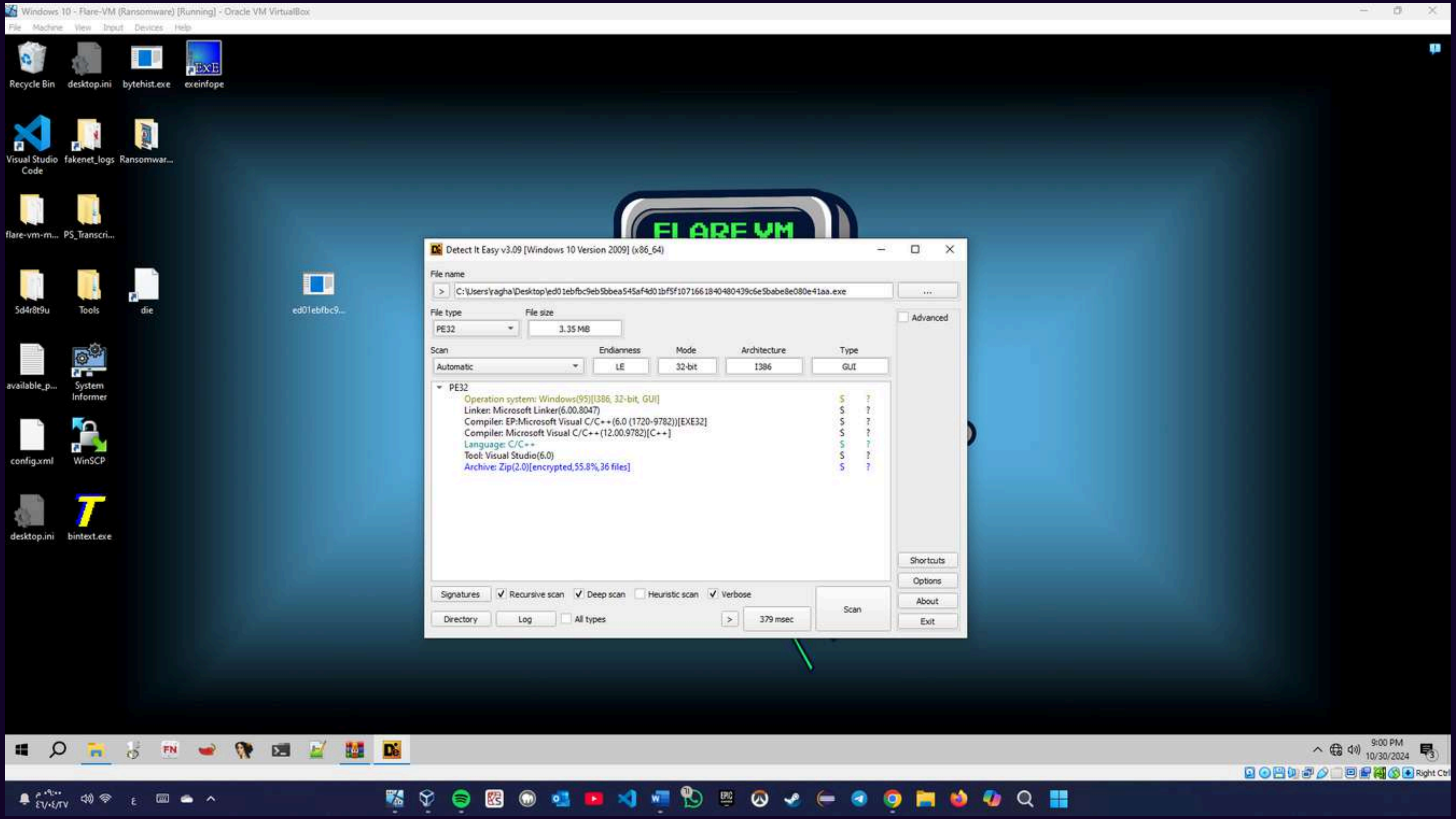
Tool Used:

Detect It Easy (DIE).

Result:

Confirmed the architecture as 32-bit, allowing us to use x32dbg for analysis.

# Determining the File Architecture



File name: C:\Users\ragha\Desktop\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

File type: PE32

File size: 3.35 MB

Scan: Automatic

| Endianness | Mode | Architecture | Type |
|---|---|---|---|
| LE | 32-bit | I386 | GUI |

```
PE32
    Operation system: Windows(95)[I386, 32-bit, GUI]          S   ?
    Linker: Microsoft Linker(6.00.8047)                       S   ?
    Compiler: EP:Microsoft Visual C/C++(6.0 (1720-9782))[EXE32]  S   ?
    Compiler: Microsoft Visual C/C++(12.00.9782)[C++]         S   ?
    Language: C/C++                                           S   ?
    Tool: Visual Studio(6.0)                                  S   ?
    Archive: Zip(2.0)[encrypted,55.8%,36 files]               S   ?
```

□ Advanced

☑ Recursive scan ☑ Deep scan □ Heuristic scan ☑ Verbose

□ All types

379 msec

# Determining Workflow of WannaCry Ransomware

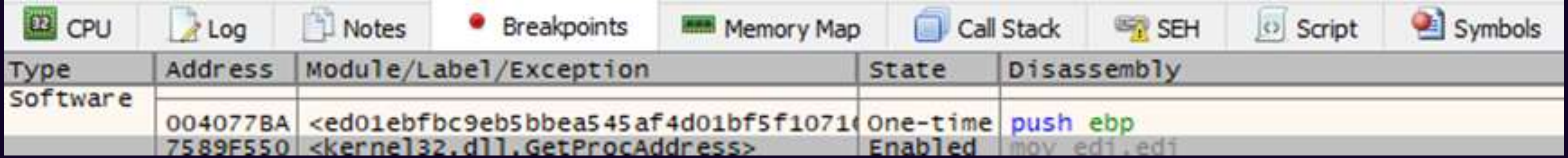
Purpose: Identifying the API used by Wannacry to detrmine the workflow

Tool Used:

dbgx32

# Determining Workflow of WannaCry Ransomware

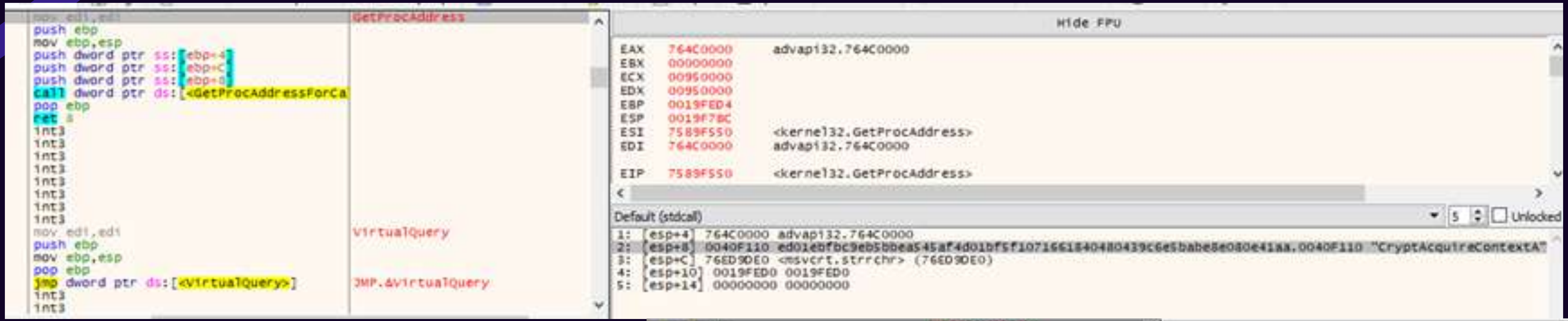
first we made a breakpoint at  GetProcAddress to detrmine what API function WannaCry are using



| Type | Address | Module/Label/Exception | State | Disassembly |
|---|---|---|---|---|
| Software | | | | |
| | 004077BA | <ed01ebfbc9eb5bbea545af4d01bf5f1071( | One-time | push ebp |
| | 7589F550 | <kernel32.dll.GetProcAddress> | Enabled | mov edi,edi |

# Determining Workflow of WannaCry Ransomware

and this some of the calls by the ransomware

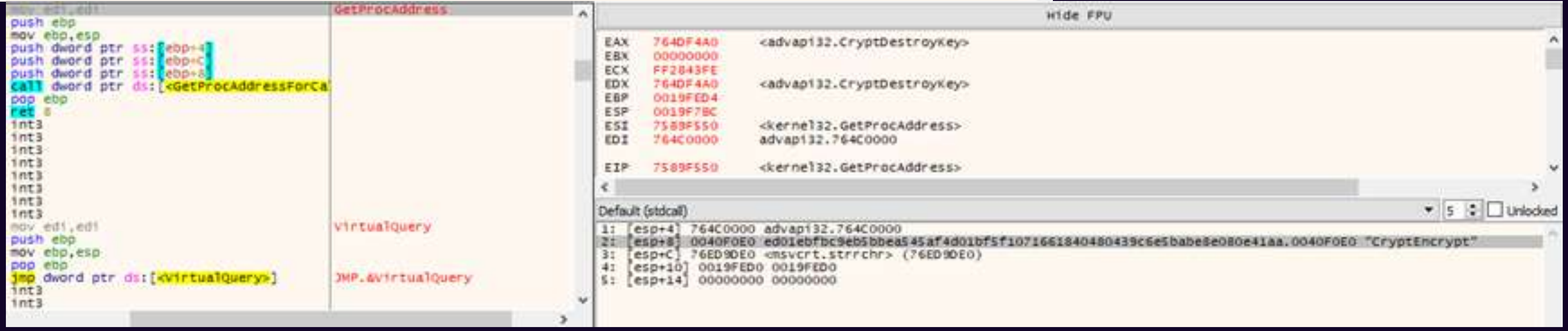


```
mov edi,edi                                      GetProcAddress
push ebp
mov ebp,esp
push dword ptr ss:[ebp+4]
push dword ptr ss:[ebp+C]
push dword ptr ss:[ebp+8]
call dword ptr ds:[<GetProcAddressForCa
pop ebp
ret 8
int3
int3
int3
int3
int3
int3
int3
int3
mov edi,edi                                      VirtualQuery
push ebp
mov ebp,esp
pop ebp
jmp dword ptr ds:[<VirtualQuery>]               JMP.&VirtualQuery
int3
int3
```

```
EAX   764C0000     advapi32.764C0000
EBX   00000000
ECX   00950000
EDX   00950000
EBP   0019FED4
ESP   0019F7BC
ESI   7589F550     <kernel32.GetProcAddress>
EDI   764C0000     advapi32.764C0000

EIP   7589F550     <kernel32.GetProcAddress>
```

Default (stdcall) 5 □ Unlocked

```
1: [esp+4] 764C0000 advapi32.764C0000
2: [esp+8] 0040F110 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.0040F110 "CryptAcquireContextA"
3: [esp+C] 76ED9DE0 <msvcrt.strrchr> (76ED9DE0)
4: [esp+10] 0019FED0 0019FED0
5: [esp+14] 00000000 00000000
```



```
mov edi,edi                                      GetProcAddress
push ebp
mov ebp,esp
push dword ptr ss:[ebp+4]
push dword ptr ss:[ebp+C]
push dword ptr ss:[ebp+8]
call dword ptr ds:[<GetProcAddressForCa
pop ebp
ret 8
int3
int3
int3
int3
int3
int3
int3
int3
mov edi,edi                                      VirtualQuery
push ebp
mov ebp,esp
pop ebp
jmp dword ptr ds:[<VirtualQuery>]               JMP.&VirtualQuery
int3
int3
```

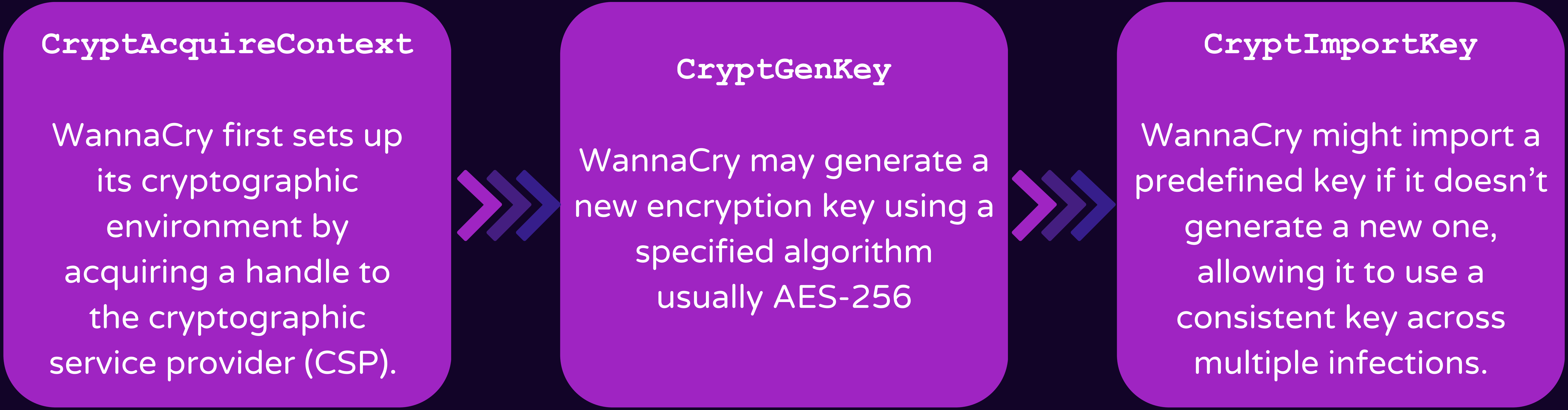
```
EAX   764DF4A0     <advapi32.CryptDestroyKey>
EBX   00000000
ECX   FF2843FE
EDX   764DF4A0     <advapi32.CryptDestroyKey>
EBP   0019FED4
ESP   0019F7BC
ESI   7589F550     <kernel32.GetProcAddress>
EDI   764C0000     advapi32.764C0000

EIP   7589F550     <kernel32.GetProcAddress>
```

Default (stdcall) 5 □ Unlocked

```
1: [esp+4] 764C0000 advapi32.764C0000
2: [esp+8] 0040F0E0 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.0040F0E0 "CryptEncrypt"
3: [esp+C] 76ED9DE0 <msvcrt.strrchr> (76ED9DE0)
4: [esp+10] 0019FED0 0019FED0
5: [esp+14] 00000000 00000000
```

# Initial Steps and Cryptographic Setup

## Prepare for file encryption by establishing cryptographic keys



`CryptAcquireContext`

WannaCry first sets up its cryptographic environment by acquiring a handle to the cryptographic service provider (CSP).

`CryptGenKey`

WannaCry may generate a new encryption key using a specified algorithm usually AES-256

`CryptImportKey`

WannaCry might import a predefined key if it doesn’t generate a new one, allowing it to use a consistent key across multiple infections.

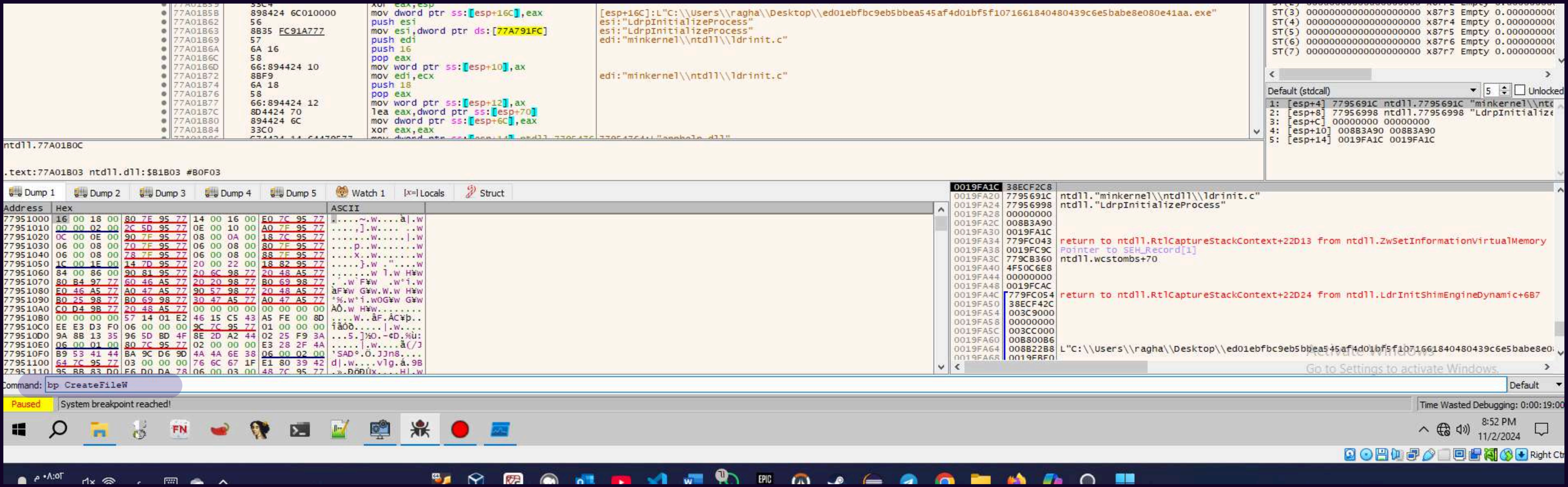
# File Targeting and Access with CreateFileW

`CreateFileW`

WannaCry uses CreateFileW to access and manipulate files for encryption or to leave ransom notes.

setting a breakpoint on CreateFileW, we can view the file paths and names, confirming which files WannaCry targets

# Setting a breakpoint on CreateFileW



```
77A01B5B   898424 6C010000   mov dword ptr ss:[esp+16C],eax     [esp+16C]:L"C:\\Users\\ragha\\Desktop\\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe"
77A01B62   56                push esi                           esi:"LdrpInitializeProcess"
77A01B63   8B35 FC91A777     mov esi,dword ptr ds:[77A791FC]    esi:"LdrpInitializeProcess"
77A01B69   57                push edi                           edi:"minkernel\\ntdll\\ldrinit.c"
77A01B6A   6A 16             push 16
77A01B6C   58                pop eax
77A01B6D   66:894424 10      mov word ptr ss:[esp+10],ax
77A01B72   8BF9              mov edi,ecx                        edi:"minkernel\\ntdll\\ldrinit.c"
77A01B74   6A 18             push 18
77A01B76   58                pop eax
77A01B77   66:894424 12      mov word ptr ss:[esp+12],ax
77A01B7C   8D4424 70         lea eax,dword ptr ss:[esp+70]
77A01B80   894424 6C         mov dword ptr ss:[esp+6C],eax
77A01B84   33C0              xor eax,eax
ntdll.77A01B0C

.text:77A01B03 ntdll.dll:$B1B03 #B0F03
```

```
ST(3) 0000000000000000000 x87r3 Empty 0.00000000(
ST(4) 0000000000000000000 x87r4 Empty 0.00000000(
ST(5) 0000000000000000000 x87r5 Empty 0.00000000(
ST(6) 0000000000000000000 x87r6 Empty 0.00000000(
ST(7) 0000000000000000000 x87r7 Empty 0.00000000(
```

Default (stdcall) 5 □ Unlocked

```
1: [esp+4] 7795691C ntdll.7795691C "minkernel\\ntc
2: [esp+8] 77956998 ntdll.77956998 "LdrpInitialize
3: [esp+C] 00000000 00000000
4: [esp+10] 008B3A90 008B3A90
5: [esp+14] 0019FA1C 0019FA1C
```

```
Address  Hex                                              ASCII
77951000 16 00 18 00 80 7E 95 77 14 00 16 00 E0 7C 95 77 .....~.w....à|.w
77951010 00 00 02 00 2C 5D 95 77 0E 00 10 00 A0 7F 95 77 ....,].w.... ..w
77951020 0C 00 0E 00 90 7F 95 77 08 00 0A 00 18 7C 95 77 .......w.....|.w
77951030 06 00 08 00 70 7F 95 77 06 00 08 00 80 7F 95 77 ....p..w.......w
77951040 06 00 08 00 78 7F 95 77 06 00 08 00 88 7F 95 77 ....x..w.......w
77951050 1C 00 1E 00 14 7D 95 77 20 00 22 00 18 82 95 77 .....}.w .".....w
77951060 84 00 86 00 90 81 95 77 20 6C 98 77 20 48 A5 77 .......w l.w H¥w
77951070 80 B4 97 77 60 46 A5 77 20 20 98 77 B0 69 98 77 .´.w`F¥w  .w°i.w
77951080 E0 46 A5 77 A0 47 A5 77 90 57 98 77 20 48 A5 77 àF¥w G¥w.W.w H¥w
77951090 B0 25 98 77 B0 69 98 77 30 47 A5 77 A0 47 A5 77 °%.w°i.w0G¥w G¥w
779510A0 C0 D4 9B 77 20 48 A5 77 00 00 00 00 00 00 00 00 ÀÔ.w H¥w........
779510B0 00 00 00 00 57 14 01 E2 46 15 C5 43 A5 FE 00 8D ....W..âF.ÅC¥þ..
779510C0 EE E3 D3 F0 06 00 00 00 9C 7C 95 77 01 00 00 00 îãÓð.....|.w....
779510D0 9A 8B 13 35 96 5D BD 4F 8E 2D A2 44 02 25 F9 3A ...5.]½O.-¢D.%ù:
779510E0 06 00 01 00 80 7C 95 77 02 00 00 00 E3 28 2F 4A .....|.w....ã(/J
779510F0 B9 53 41 44 BA 9C D6 9D 4A 4A 6E 38 06 00 02 00 ¹SAD°.Ö.JJn8....
77951100 64 7C 95 77 03 00 00 00 76 6C 67 1F E1 80 39 42 d|.w....vlg.á.9B
```

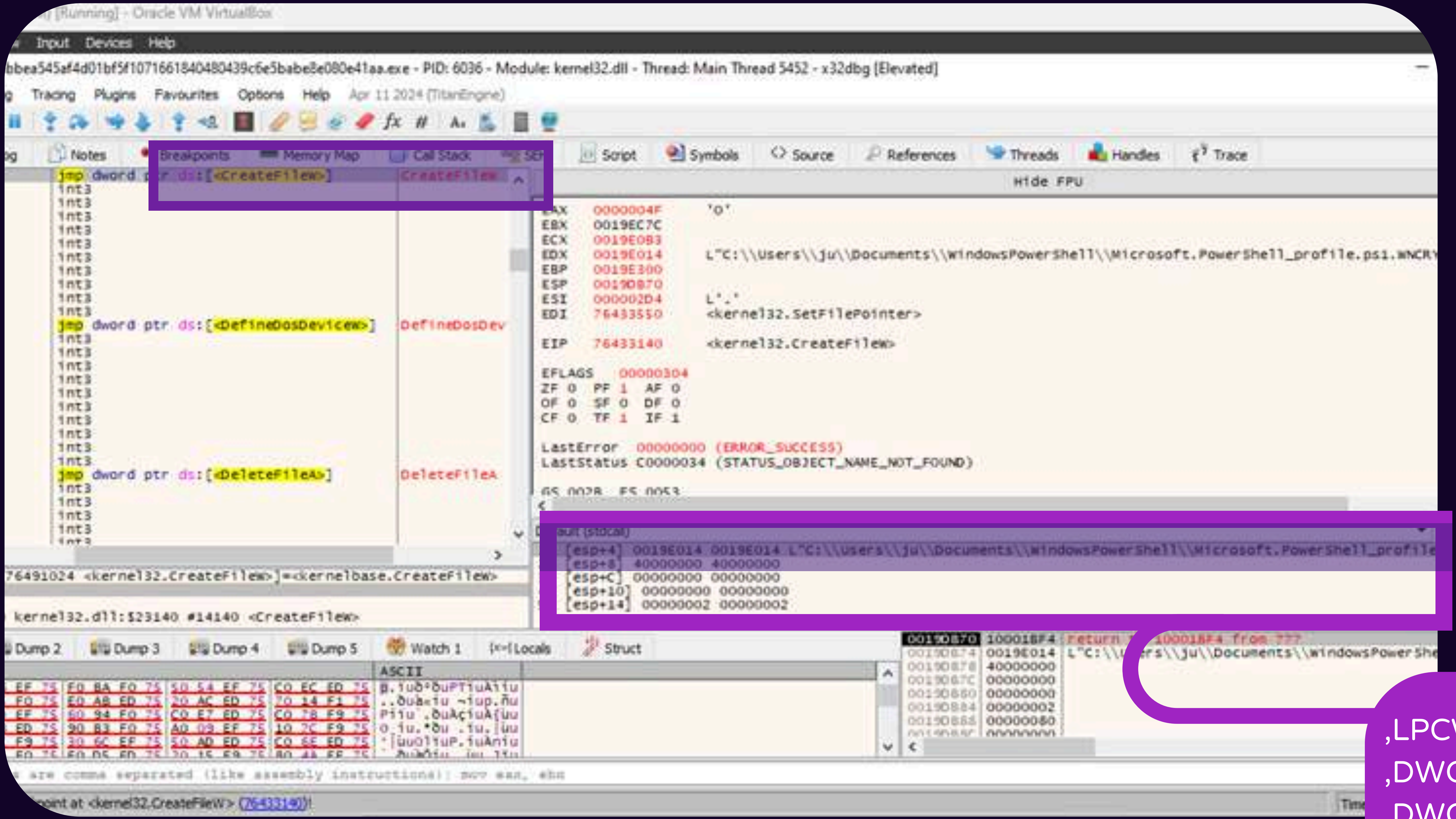
```
0019FA1C 38ECF2C8
0019FA20 7795691C ntdll."minkernel\\ntdll\\ldrinit.c"
0019FA24 77956998 ntdll."LdrpInitializeProcess"
0019FA28 00000000
0019FA2C 008B3A90
0019FA30 0019FA1C
0019FA34 779FC043 return to ntdll.RtlCaptureStackContext+22D13 from ntdll.ZwSetInformationVirtualMemory
0019FA38 0019FC9C Pointer to SEH_Record[1]
0019FA3C 779CB360 ntdll.wcstombs+70
0019FA40 4F50C6E8
0019FA44 00000000
0019FA48 0019FCAC
0019FA4C 779FC054 return to ntdll.RtlCaptureStackContext+22D24 from ntdll.LdrInitShimEngineDynamic+6B7
0019FA50 38ECF42C
0019FA54 003C9000
0019FA58 00000000
0019FA5C 003CC000
0019FA60 00B800B6
0019FA64 008B22B8 L"C:\\Users\\ragha\\Desktop\\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e0
```

Go to Settings to activate Windows.

```
Command: bp CreateFileW
```

Paused | System breakpoint reached! | Time Wasted Debugging: 0:00:19:00

# Debugging Analysis – Observing Targeted Files



```
[Running] - Oracle VM VirtualBox
Input  Devices  Help
bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe - PID: 6036 - Module: kernel32.dll - Thread: Main Thread 5452 - x32dbg [Elevated]
Tracing  Plugins  Favourites  Options  Help  Apr 11 2024 (TitanEngine)
```

```
jmp dword ptr ds:[<CreateFileW>]            CreateFileW
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
jmp dword ptr ds:[<DefineDosDeviceW>]       DefineDosDev
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
jmp dword ptr ds:[<DeleteFileA>]            DeleteFileA
int3
int3
int3
int3

76491024 <kernel32.CreateFileW>]=<kernelbase.CreateFileW>

kernel32.dll:$23140 #14140 <CreateFileW>
```

```
Hide FPU

EAX   0000004F     'O'
EBX   0019EC7C
ECX   0019E0B3
EDX   0019E014     L"C:\\Users\\ju\\Documents\\WindowsPowerShell\\Microsoft.PowerShell_profile.ps1.WNCRY
EBP   0019E300
ESP   0019D870
ESI   000002D4     L'.'
EDI   76433550     <kernel32.SetFilePointer>

EIP   76433140     <kernel32.CreateFileW>

EFLAGS   00000304
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 002B  FS 0053
```

```
Default (stdcall)
[esp+4]  0019E014 0019E014 L"C:\\Users\\ju\\Documents\\WindowsPowerShell\\Microsoft.PowerShell_profile
[esp+8]  40000000 40000000
[esp+C]  00000000 00000000
[esp+10]  00000000 00000000
[esp+14]  00000002 00000002
```

```
0019D870 100018F4 return to 100018F4 from ???
0019D874 0019E014 L"C:\\Users\\ju\\Documents\\WindowsPowerShe
0019D878 40000000
0019D87C 00000000
0019D880 00000000
0019D884 00000002
0019D888 00000080
0019D88C 00000000
```

```
EF 75 | F0 BA F0 75 | 50 54 EF 75 | C0 EC ED 75 | þ.ïuð°ðuPTïuÀìíu
F0 75 | E0 A8 ED 75 | 20 AC ED 75 | 70 14 F1 75 | ..ðuà¨íu ¬íup.ñu
EF 75 | 60 94 F0 75 | C0 E7 ED 75 | C0 78 F9 75 | Pïïu`.ðuÀçíuÀ{ùu
ED 75 | 90 B3 F0 75 | A0 09 EF 75 | 10 2C F9 75 | o íu.³ðu .ïu.,ùu
F9 75 | 30 6C EF 75 | 50 AD ED 75 | C0 6E ED 75 | ·|ùu0lïuP.íuÀníu
```

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

point at <kernel32.CreateFileW> (76433140)!

```
HANDLE CreateFileW(
,LPCWSTR               lpFileName          [in]
,DWORD                 dwDesiredAccess          [in]
,DWORD                 dwShareMode          [in]
LPSECURITY_ATTRIBUTES [in, optional]
,lpSecurityAttributes
,DWORD                 dwCreationDisposition          [in]
,DWORD                 dwFlagsAndAttributes          [in]
HANDLE                 hTemplateFile [in, optional]
```

# Types of Files Created or Modified by WannaCry

Based on the debugging analysis, WannaCry creates and modifies several types of files. These serve different roles in the attack process, from ransom notes to encrypted and temporary files

- Ransom Note Files
- Encrypted Files
- Temporary Files
- Registry Modifications for Persistence

# Ransom Note Files

## @Please_Read_Me@.txt

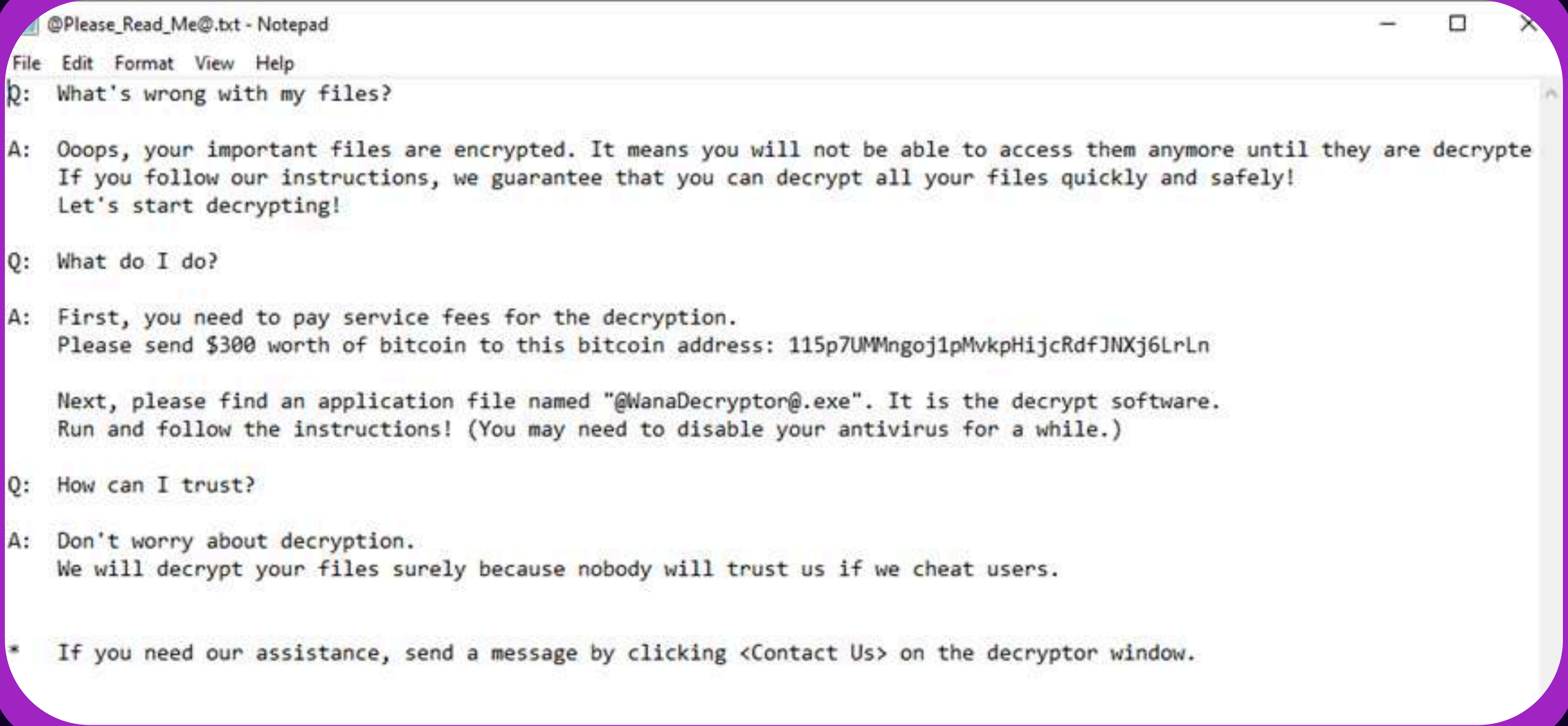
Filename: @Please_Read_Me@.txt – found in each directory with encrypted files.

Purpose: Contains instructions for the victim, including:

- Ransom Demand: Amount of payment required.
- Payment Instructions: How to pay in Bitcoin.

# Ransom Note Files

## @Please_Read_Me@.txt



```
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 decrypte
    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 $300 worth of bitcoin to this bitcoin address: 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

    Next, please find an application file named "@WanaDecryptor@.exe". 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.
```

# Encrypted Files with .WNCRY Extension

Filename Extension: .WNCRY – appended to files post-encryption.

Targeted File Types:

- Documents: .doc, .docx, .xls, .xlsx, .ppt, .pptx.
- Images: .jpg, .png, .bmp.
- Archives: .zip, .rar, .7z.
- Database Files: .sql, .db, .sqlite.

Purpose: Encryption makes the files inaccessible without a decryption key, which is the core function of the ransomware.

# Temporary Files with .tmp Extension

Filename Example: ~SD8F67.tmp – typically used for intermediary data storage during encryption.

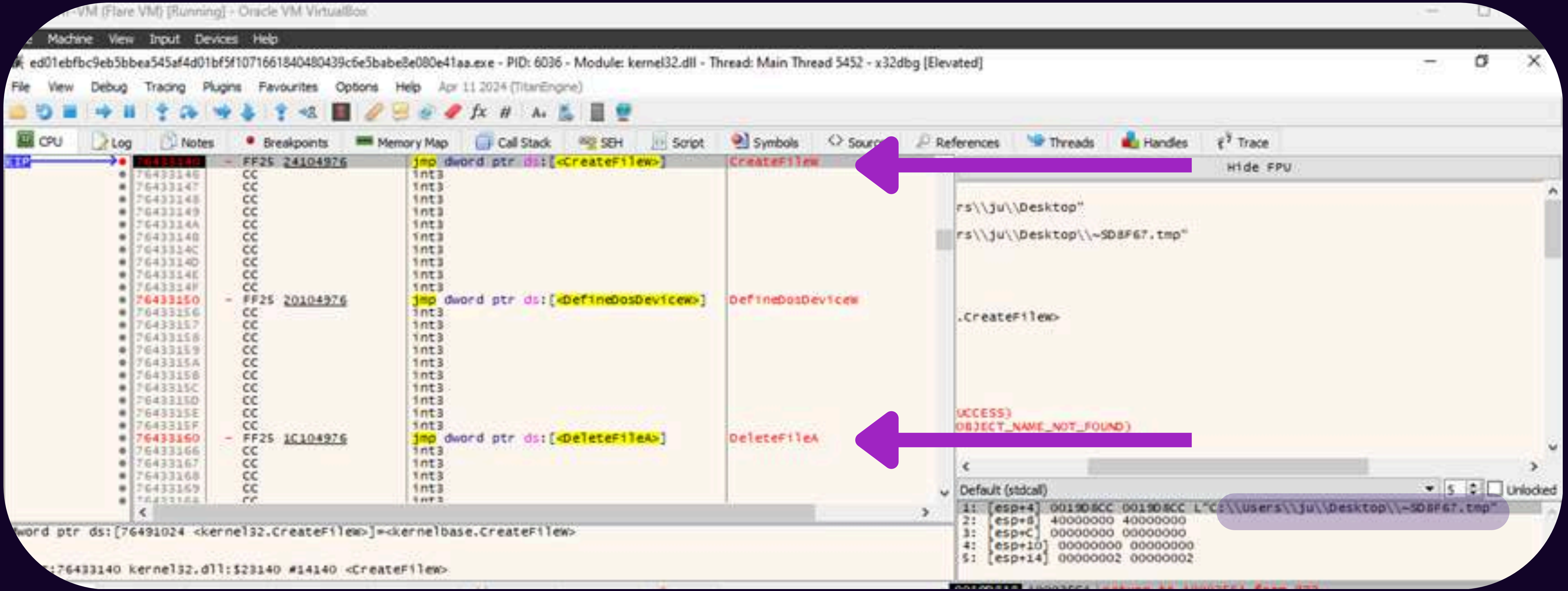
Purpose:

- Holds Unencrypted Data: Prepares data before encryption.
- Encryption Process Storage: Stores intermediate encryption data.

Cleanup Strategy: These temporary files are often deleted after encryption to minimize forensic traces.

# Temporary Files with .tmp Extension

## Cleanup Strategy



ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe - PID: 6036 - Module: kernel32.dll - Thread: Main Thread 5452 - x32dbg [Elevated]

```
76433140  - FF25 24104976   jmp dword ptr ds:[<CreateFileW>]       CreateFileW
76433146    CC              int3
76433147    CC              int3
76433148    CC              int3
76433149    CC              int3
7643314A    CC              int3
7643314B    CC              int3
7643314C    CC              int3
7643314D    CC              int3
7643314E    CC              int3
7643314F    CC              int3
76433150  - FF25 20104976   jmp dword ptr ds:[<DefineDosDeviceW>]  DefineDosDeviceW
76433156    CC              int3
76433157    CC              int3
76433158    CC              int3
76433159    CC              int3
7643315A    CC              int3
7643315B    CC              int3
7643315C    CC              int3
7643315D    CC              int3
7643315E    CC              int3
7643315F    CC              int3
76433160  - FF25 1C104976   jmp dword ptr ds:[<DeleteFileA>]       DeleteFileA
76433166    CC              int3
76433167    CC              int3
76433168    CC              int3
76433169    CC              int3
```

```
word ptr ds:[76491024 <kernel32.CreateFileW>]=<kernelbase.CreateFileW>

:76433140 kernel32.dll:$23140 #14140 <CreateFileW>
```

```
rs\\ju\\Desktop"

rs\\ju\\Desktop\\~SD8F67.tmp"

.CreateFileW>

UCCESS)
OBJECT_NAME_NOT_FOUND)
```

```
1: [esp+4]  0019D8CC 0019D8CC L"C:\\Users\\ju\\Desktop\\~SD8F67.tmp"
2: [esp+8]  40000000 40000000
3: [esp+C]  00000000 00000000
4: [esp+10] 00000000 00000000
5: [esp+14] 00000002 00000002
```

# Registry Modifications for Persistence

Registry Path: WannaCry adds entries under:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Purpose: Ensures WannaCry restarts every time the system boots.

The registry key points to WannaCry's executable, making it difficult to remove the infection without cleaning the registry.

# Read File Contents

**Reads file contents into memory as plaintext**

`ReadFile`

Prepares the file data for encryption, so it can later be overwritten with ciphertext

# Encrypt File Data

`CryptEncrypt`

Encrypts plaintext data in memory using the established cryptographic key, transforming it into ciphertext

**This encryption step makes the file unreadable without a decryption key, fulfilling the ransomware's purpose.**

# Write Encrypted Data to File

`WriteFile`

Writes the ciphertext back to the file, replacing the original content.

**Overwrites the file with encrypted data, enforcing the ransom demand by making the original data inaccessible.**

# Handle closure and Key destruction

`CryptDestroyKey`

Destroys the encryption key handle, preventing key recovery.

`CloseHandle`

Closes all file and cryptographic handles

**By destroying keys and closing handles WannaCry performs a thorough cleanup which prevent any recovery of resources**

# Persistence Mechanism Observed with RegCreateKeyW

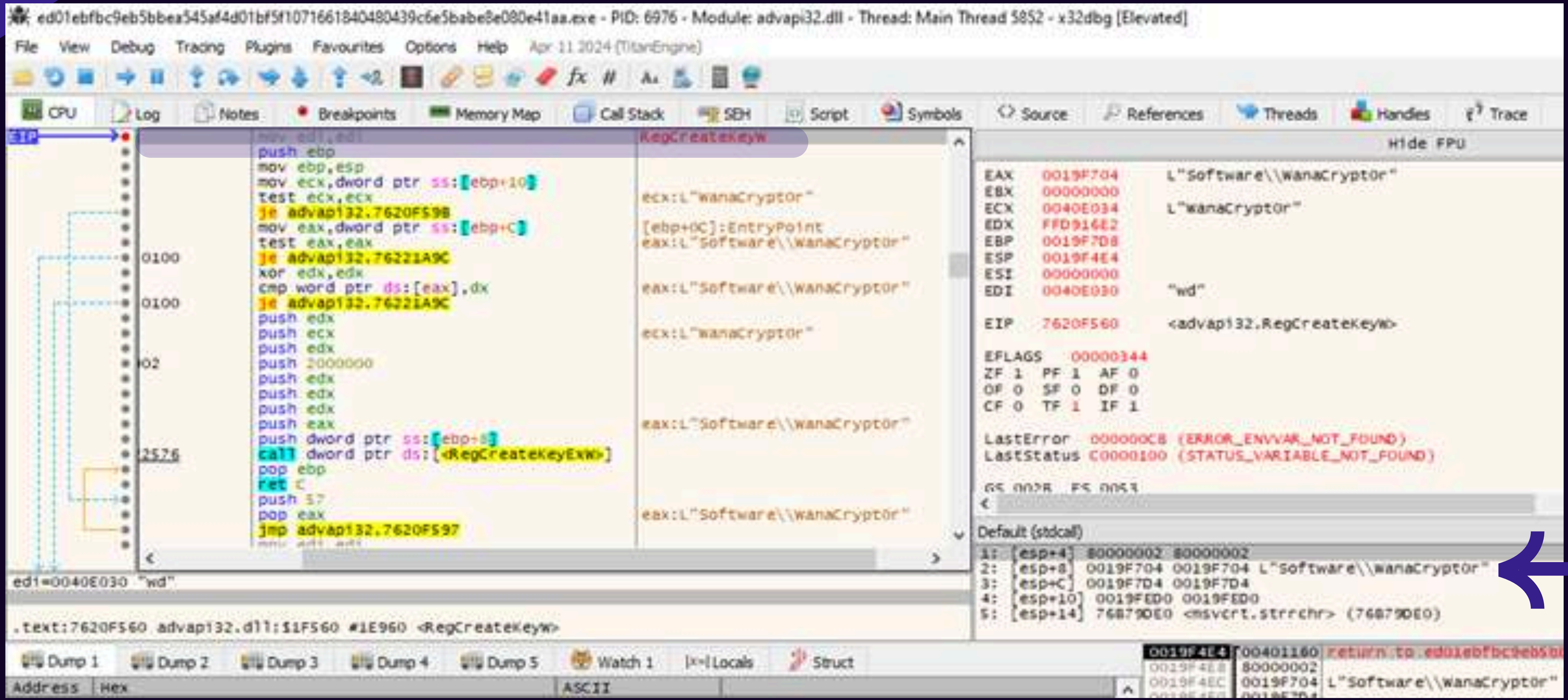
**RegCreateKeyW**

Enables WannaCry to re-establish itself after a system reboot, ensuring it remains active on the infected machine

how???

By createing a specific registry keys to store settings, configurations, or status information to guarantee that WannaCry relaunches on each reboot.

# Persistence Mechanism Observed with RegCreateKeyW


ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe - PID: 6976 - Module: advapi32.dll - Thread: Main Thread 5852 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 11 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Address Hex ASCII

```
EIP →   mov edi,edi                              RegCreateKeyW
        push ebp
        mov ebp,esp
        mov ecx,dword ptr ss:[ebp+10]
        test ecx,ecx                             ecx:L"wanaCryptor"
        je advapi32.7620F59B
        mov eax,dword ptr ss:[ebp+C]             [ebp+0C]:EntryPoint
        test eax,eax                             eax:L"Software\\WanaCryptor"
0100    je advapi32.76221A9C
        xor edx,edx
        cmp word ptr ds:[eax],dx                 eax:L"Software\\WanaCryptor"
0100    je advapi32.76221A9C
        push edx
        push ecx                                 ecx:L"wanaCryptor"
        push edx
02      push 2000000
        push edx
        push edx
        push edx
        push eax                                 eax:L"Software\\WanaCryptor"
        push dword ptr ss:[ebp+8]
2576    call dword ptr ds:[<RegCreateKeyExW>]
        pop ebp
        ret C
        push 57
        pop eax                                  eax:L"Software\\WanaCryptor"
        jmp advapi32.7620F597
```

```
edi=0040E030 "wd"
```

```
.text:7620F560 advapi32.dll:$1F560 #1E960 <RegCreateKeyW>
```

```
EAX   0019F704     L"Software\\WanaCryptor"
EBX   00000000
ECX   0040E034     L"wanaCryptor"
EDX   FFD916E2
EBP   0019F7D8
ESP   0019F4E4
ESI   00000000
EDI   0040E030     "wd"

EIP   7620F560     <advapi32.RegCreateKeyW>

EFLAGS   00000344
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError  000000CB (ERROR_ENVVAR_NOT_FOUND)
LastStatus C0000100 (STATUS_VARIABLE_NOT_FOUND)

GS 002B  FS 0053
```

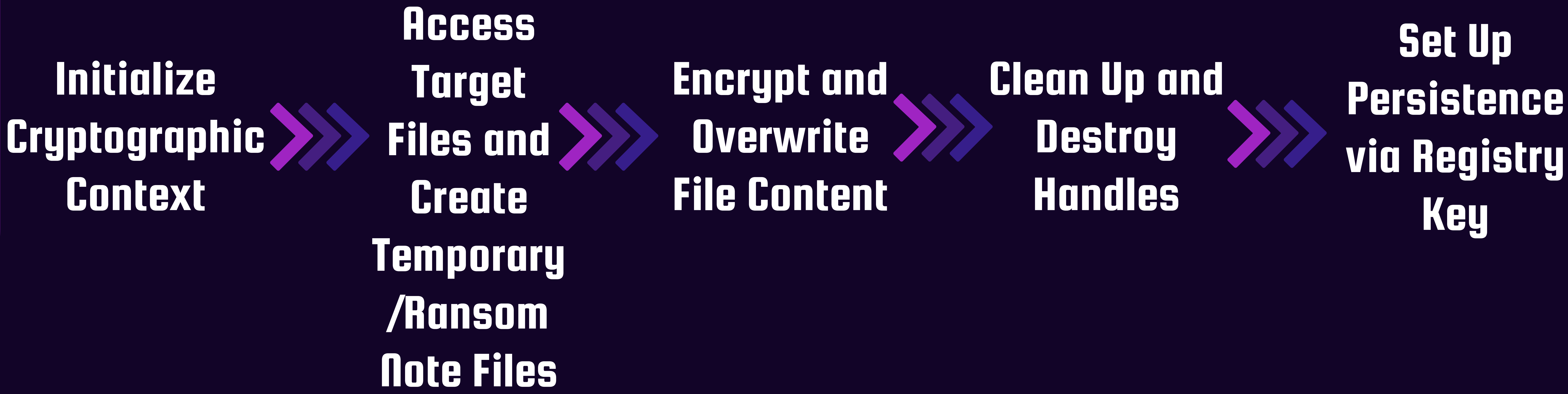
Default (stdcall)

```
1: [esp+4]  80000002 80000002
2: [esp+8]  0019F704 0019F704 L"Software\\wanaCryptor"
3: [esp+C]  0019F7D4 0019F7D4
4: [esp+10] 0019FED0 0019FED0
5: [esp+14] 76879DE0 <msvcrt.strrchr> (76879DE0)
```

```
0019F4E4  00401160  return to ed01ebfbc9eb5b
0019F4E8  80000002
0019F4EC  0019F704  L"Software\\WanaCryptor"
```

By making a breakpoint at `RegCreateKeyW` we can see from lpSubKey set to "software\\wanacryptor"

# Summary of Workflow of WannaCry Ransomware



Initialize Cryptographic Context

Access Target Files and Create Temporary /Ransom Note Files

Encrypt and Overwrite File Content

Clean Up and Destroy Handles

Set Up Persistence via Registry Key

# Dump And Extract

# Importance and Storage of AES Key in WannaCry

Finding the AES key is important because it allows analysts to decrypt files and understand the ransomware's effects. Also Understanding the encryption method used and helps in developing tools to respond to similar ransomware in the future.

WannaCry hides its AES key using functions like CryptGenKey and CryptProtectData, which secure the key in memory. Sometimes, the key is also hidden within DLL files or encrypted with an RSA key, adding extra layers of protection and making it harder to locate.

# Dumping and Extraction Setup

Purpose:

To prepare tools to locate and extract key data , enabling deeper analysis of its encryption methods.

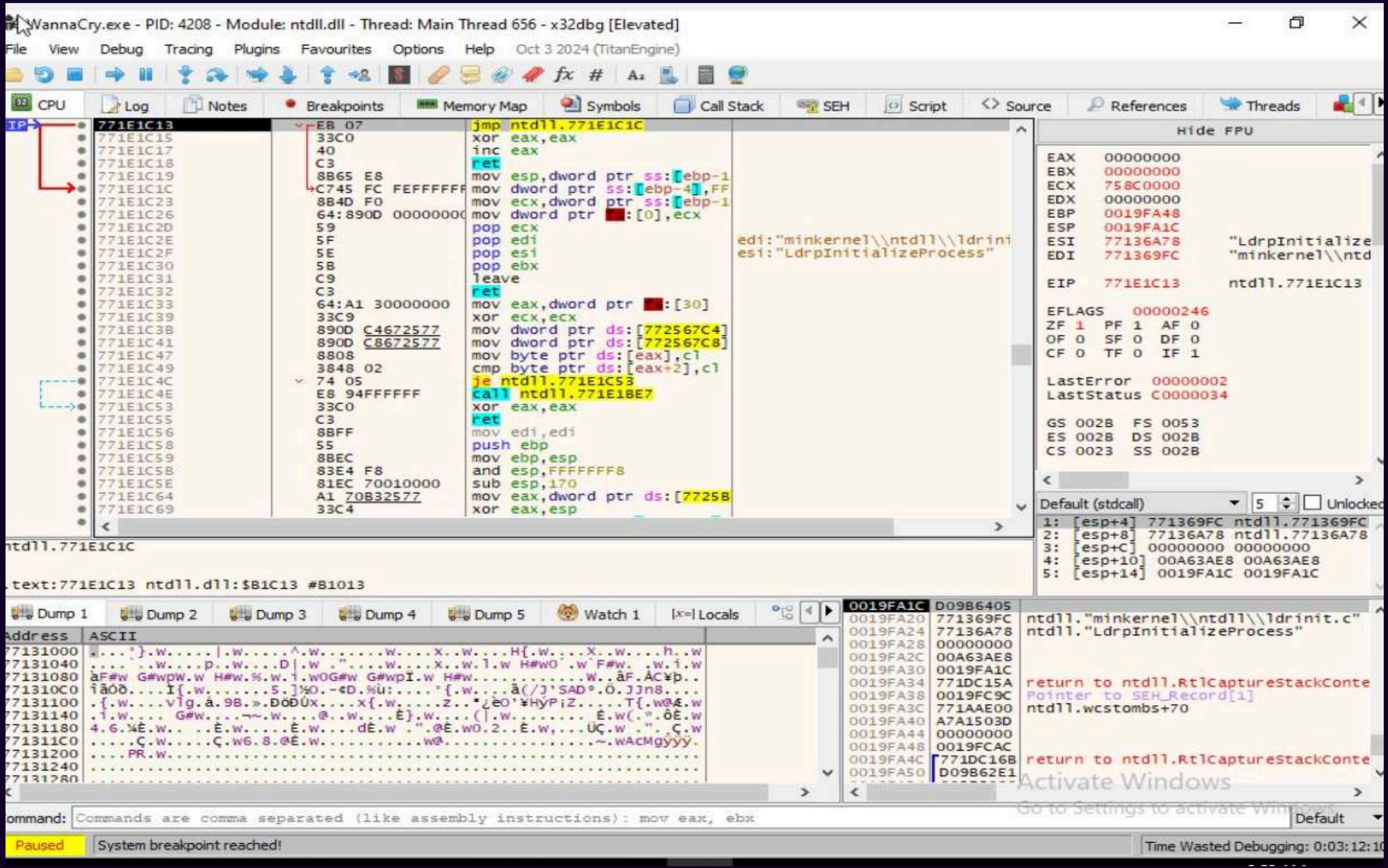
Tool Used:

x32dbg
HxD
PeStudio

Result:

Extracted AES key and relevant data from WannaCry.

# Locating the AES Key


WannaCry.exe - PID: 4208 - Module: ntdll.dll - Thread: Main Thread 656 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Oct 3 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Symbols Call Stack SEH Script Source References Threads
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals
Default (stdcall)
5
Unlocked
Default

```
771E1C13   EB 07               jmp ntdll.771E1C1C
771E1C15   33C0                xor eax,eax
771E1C17   40                  inc eax
771E1C18   C3                  ret
771E1C19   8B65 E8             mov esp,dword ptr ss:[ebp-1
771E1C1C   C745 FC FEFFFFFF    mov dword ptr ss:[ebp-4],FF
771E1C23   8B4D F0             mov ecx,dword ptr ss:[ebp-1
771E1C26   64:890D 00000000    mov dword ptr fs:[0],ecx
771E1C2D   59                  pop ecx
771E1C2E   5F                  pop edi          edi:"minkernel\\ntdll\\ldrini
771E1C2F   5E                  pop esi          esi:"LdrpInitializeProcess"
771E1C30   5B                  pop ebx
771E1C31   C9                  leave
771E1C32   C3                  ret
771E1C33   64:A1 30000000      mov eax,dword ptr fs:[30]
771E1C39   33C9                xor ecx,ecx
771E1C3B   890D C4672577       mov dword ptr ds:[772567C4]
771E1C41   890D C8672577       mov dword ptr ds:[772567C8]
771E1C47   8808                mov byte ptr ds:[eax],cl
771E1C49   3848 02             cmp byte ptr ds:[eax+2],cl
771E1C4C   74 05               je ntdll.771E1C53
771E1C4E   E8 94FFFFFF         call ntdll.771E1BE7
771E1C53   33C0                xor eax,eax
771E1C55   C3                  ret
771E1C56   8BFF                mov edi,edi
771E1C58   55                  push ebp
771E1C59   8BEC                mov ebp,esp
771E1C5B   83E4 F8             and esp,FFFFFFF8
771E1C5E   81EC 70010000       sub esp,170
771E1C64   A1 70B32577         mov eax,dword ptr ds:[7725B
771E1C69   33C4                xor eax,esp

ntdll.771E1C1C

.text:771E1C13 ntdll.dll:$B1C13 #B1013
```

```
EAX     00000000
EBX     00000000
ECX     758C0000
EDX     00000000
EBP     0019FA48
ESP     0019FA1C
ESI     77136A78     "LdrpInitialize
EDI     771369FC     "minkernel\\ntd

EIP     771E1C13     ntdll.771E1C13

EFLAGS    00000246
ZF 1   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1

LastError   00000002
LastStatus  C0000034

GS 002B   FS 0053
ES 002B   DS 002B
CS 0023   SS 002B
```

```
1:  [esp+4]  771369FC ntdll.771369FC
2:  [esp+8]  77136A78 ntdll.77136A78
3:  [esp+C]  00000000 00000000
4:  [esp+10] 00A63AE8 00A63AE8
5:  [esp+14] 0019FA1C 0019FA1C
```

```
Address  ASCII
77131000 ....}.w.....|.w.....^.w.......w....x..w....H{.w....X..w....h..w
77131040 ......w....p..w....D|.w ."....w....x..w.l.w H#wO .w F#w. .w.i.w
77131080 àF#w G#wpW.w H#w.%.w.i.wOG#w G#wpI.w H#w...........W..âF.ÀC¥þ..
771310C0 îãÓð....I{.w.......5.]½O.-¢D.%ù:....'{.w....ã(/J'SAD°.Ö.JJn8....
77131100 .{.w....vìg.á.9B.».ÐõÐÚx....x{.w.....z..•¿èO'¥HýP¡Z.....T{.w@Æ.w
77131140 .ì.w.... G#w....¬~.w....@..w....È}.w....(|.w........ È.w(.".ôÈ.w
77131180 4.6.¼È.w.. ..È.w.....È.w....dÈ.w .".@È.wO.2..È.w,...ÜÇ.w .". Ç.w
771311C0 .....Ç.w.....Ç.w6.8.@È.w............w@...................~.wAcMgÿÿÿ.
77131200 ....PR.w..........................................................
77131240 ..................................................................
77131280 ..................................................................
```

```
0019FA1C  D09B6405
0019FA20  771369FC  ntdll."minkernel\\ntdll\\ldrinit.c"
0019FA24  77136A78  ntdll."LdrpInitializeProcess"
0019FA28  00000000
0019FA2C  00A63AE8
0019FA30  0019FA1C
0019FA34  771DC15A  return to ntdll.RtlCaptureStackConte
0019FA38  0019FC9C  Pointer to SEH_Record[1]
0019FA3C  771AAE00  ntdll.wcstombs+70
0019FA40  A7A1503D
0019FA44  00000000
0019FA48  0019FCAC
0019FA4C  771DC16B  return to ntdll.RtlCaptureStackConte
0019FA50  D09B62E1
```

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

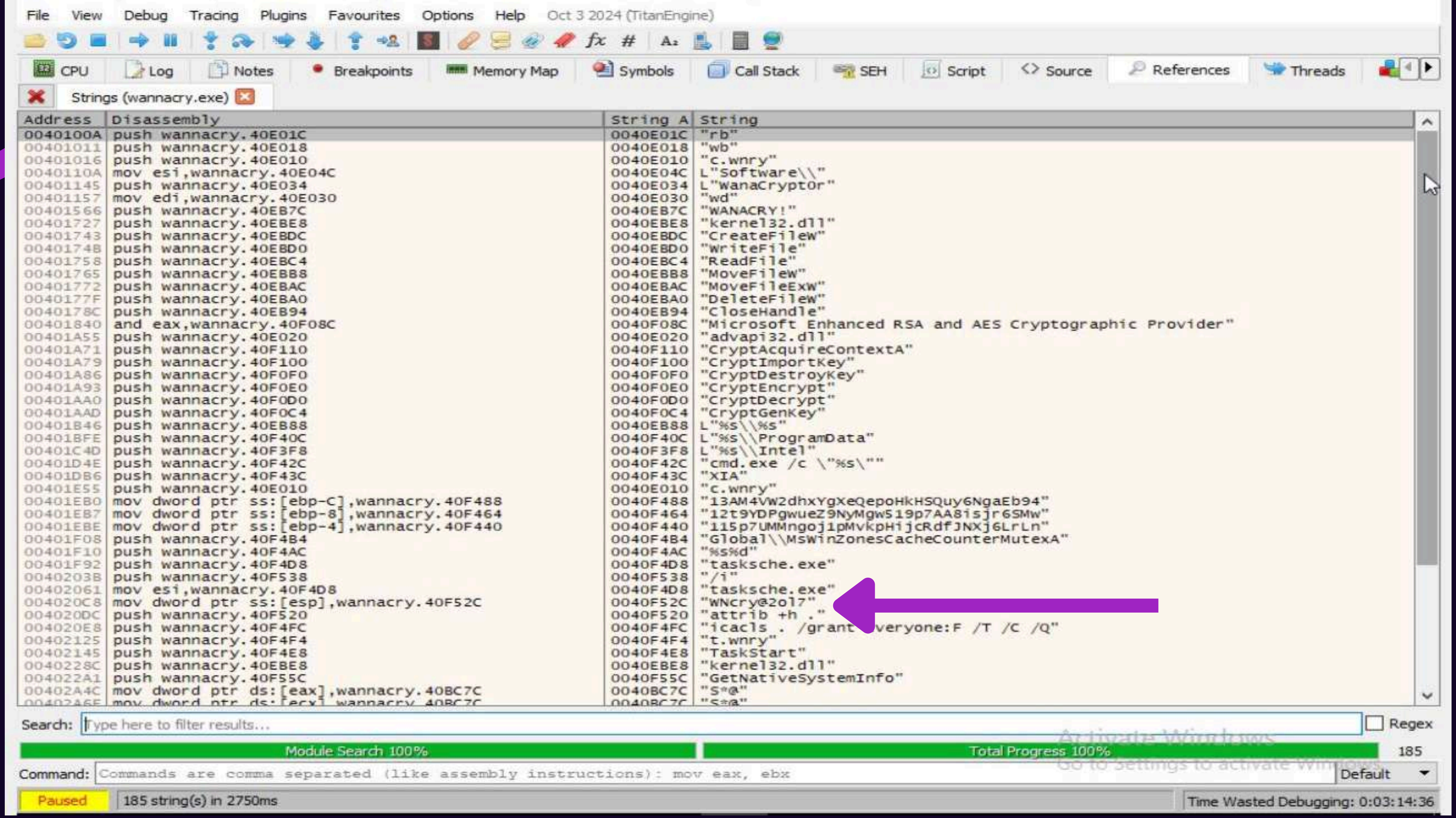
Paused System breakpoint reached!

Time Wasted Debugging: 0:03:12:10

Activate Windows
Go to Settings to activate Windows.

In x32dbg, a breakpoint was set on functions or dlls related to encryption. This allowed us to monitor WannaCry's behavior and track down the AES key location.

# Locating the AES Key



```
Address  Disassembly                                 String A  String
0040100A push wannacry.40E01C                        0040E01C  "rb"
00401011 push wannacry.40E018                        0040E018  "wb"
00401016 push wannacry.40E010                        0040E010  "c.wnry"
0040110A mov esi,wannacry.40E04C                     0040E04C  L"Software\\"
00401145 push wannacry.40E034                        0040E034  L"WanaCrypt0r"
00401157 mov edi,wannacry.40E030                     0040E030  "wd"
00401566 push wannacry.40EB7C                        0040EB7C  "WANACRY!"
00401727 push wannacry.40EBE8                        0040EBE8  "kernel32.dll"
00401743 push wannacry.40EBDC                        0040EBDC  "CreateFileW"
0040174B push wannacry.40EBD0                        0040EBD0  "WriteFile"
00401758 push wannacry.40EBC4                        0040EBC4  "ReadFile"
00401765 push wannacry.40EBB8                        0040EBB8  "MoveFileW"
00401772 push wannacry.40EBAC                        0040EBAC  "MoveFileExW"
0040177F push wannacry.40EBA0                        0040EBA0  "DeleteFileW"
0040178C push wannacry.40EB94                        0040EB94  "CloseHandle"
00401840 and eax,wannacry.40F08C                     0040F08C  "Microsoft Enhanced RSA and AES Cryptographic Provider"
00401A55 push wannacry.40E020                        0040E020  "advapi32.dll"
00401A71 push wannacry.40F110                        0040F110  "CryptAcquireContextA"
00401A79 push wannacry.40F100                        0040F100  "CryptImportKey"
00401A86 push wannacry.40F0F0                        0040F0F0  "CryptDestroyKey"
00401A93 push wannacry.40F0E0                        0040F0E0  "CryptEncrypt"
00401AA0 push wannacry.40F0D0                        0040F0D0  "CryptDecrypt"
00401AAD push wannacry.40F0C4                        0040F0C4  "CryptGenKey"
00401B46 push wannacry.40EB88                        0040EB88  L"%s\\%s"
00401BFE push wannacry.40F40C                        0040F40C  L"%s\\ProgramData"
00401C4D push wannacry.40F3F8                        0040F3F8  L"%s\\Intel"
00401D4E push wannacry.40F42C                        0040F42C  "cmd.exe /c \"%s\""
00401DB6 push wannacry.40F43C                        0040F43C  "XIA"
00401E55 push wannacry.40E010                        0040E010  "c.wnry"
00401EB0 mov dword ptr ss:[ebp-C],wannacry.40F488    0040F488  "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"
00401EB7 mov dword ptr ss:[ebp-8],wannacry.40F464    0040F464  "12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"
00401EBE mov dword ptr ss:[ebp-4],wannacry.40F440    0040F440  "115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn"
00401F08 push wannacry.40F4B4                        0040F4B4  "Global\\MsWinZonesCacheCounterMutexA"
00401F10 push wannacry.40F4AC                        0040F4AC  "%s%d"
00401F92 push wannacry.40F4D8                        0040F4D8  "tasksche.exe"
0040203B push wannacry.40F538                        0040F538  "/i"
00402061 mov esi,wannacry.40F4D8                     0040F4D8  "tasksche.exe"
004020C8 mov dword ptr ss:[esp],wannacry.40F52C      0040F52C  "WNcry@2ol7"
004020DC push wannacry.40F520                        0040F520  "attrib +h ."
004020E8 push wannacry.40F4FC                        0040F4FC  "icacls . /grant Everyone:F /T /C /Q"
00402125 push wannacry.40F4F4                        0040F4F4  "t.wnry"
00402145 push wannacry.40F4E8                        0040F4E8  "TaskStart"
0040228C push wannacry.40EBE8                        0040EBE8  "kernel32.dll"
004022A1 push wannacry.40F55C                        0040F55C  "GetNativeSystemInfo"
00402A4C mov dword ptr ds:[eax],wannacry.40BC7C      0040BC7C  "S*@"
00402A6F mov dword ptr ds:[ecx],wannacry.40BC7C      0040BC7C  "S*@"
```

Search: Type here to filter results...  □ Regex

Module Search 100%  Total Progress 100%  185

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

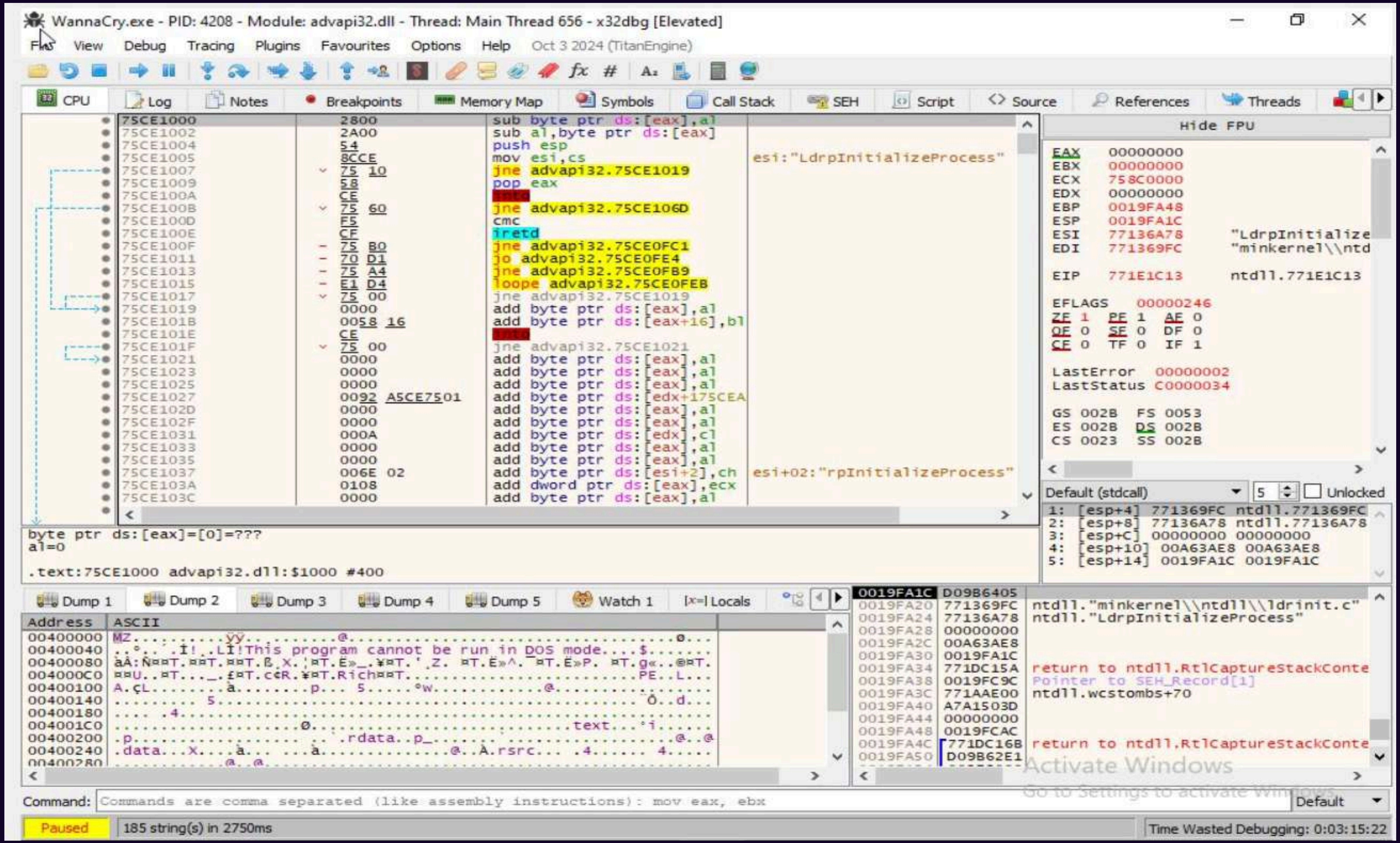
Paused  185 string(s) in 2750ms  Time Wasted Debugging: 0:03:14:36

we found the AES key stored in

ntdll.dll

This shows how WannaCry hides critical data within system DLLs for added security.

# Discovering Key Encryption Algorithm



WannaCry.exe - PID: 4208 - Module: advapi32.dll - Thread: Main Thread 656 - x32dbg [Elevated]

```
75CE1000   2800          sub byte ptr ds:[eax],al
75CE1002   2A00          sub al,byte ptr ds:[eax]
75CE1004   54            push esp
75CE1005   8CCE          mov esi,cs                     esi:"LdrpInitializeProcess"
75CE1007   75 10         jne advapi32.75CE1019
75CE1009   58            pop eax
75CE100A   CE            into
75CE100B   75 60         jne advapi32.75CE106D
75CE100D   F5            cmc
75CE100E   CF            iretd
75CE100F   75 B0         jne advapi32.75CE0FC1
75CE1011   70 D1         jo advapi32.75CE0FE4
75CE1013   75 A4         jne advapi32.75CE0FB9
75CE1015   E1 D4         loope advapi32.75CE0FEB
75CE1017   75 00         jne advapi32.75CE1019
75CE1019   0000          add byte ptr ds:[eax],al
75CE101B   0058 16       add byte ptr ds:[eax+16],bl
75CE101E   CE            into
75CE101F   75 00         jne advapi32.75CE1021
75CE1021   0000          add byte ptr ds:[eax],al
75CE1023   0000          add byte ptr ds:[eax],al
75CE1025   0000          add byte ptr ds:[eax],al
75CE1027   0092 A5CE7501 add byte ptr ds:[edx+175CEA
75CE102D   0000          add byte ptr ds:[eax],al
75CE102F   0000          add byte ptr ds:[eax],al
75CE1031   000A          add byte ptr ds:[edx],cl
75CE1033   0000          add byte ptr ds:[eax],al
75CE1035   0000          add byte ptr ds:[eax],al
75CE1037   006E 02       add byte ptr ds:[esi+2],ch     esi+02:"rpInitializeProcess"
75CE103A   0108          add dword ptr ds:[eax],ecx
75CE103C   0000          add byte ptr ds:[eax],al
```

```
byte ptr ds:[eax]=[0]=???
al=0

.text:75CE1000 advapi32.dll:$1000 #400
```

```
EAX   00000000
EBX   00000000
ECX   758C0000
EDX   00000000
EBP   0019FA48
ESP   0019FA1C
ESI   77136A78      "LdrpInitialize
EDI   771369FC      "minkernel\\ntd

EIP   771E1C13      ntdll.771E1C13

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000002
LastStatus C0000034

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B
```

```
1: [esp+4] 771369FC ntdll.771369FC
2: [esp+8] 77136A78 ntdll.77136A78
3: [esp+C] 00000000 00000000
4: [esp+10] 00A63AE8 00A63AE8
5: [esp+14] 0019FA1C 0019FA1C
```

```
Address   ASCII
00400000  MZ..........ÿÿ........@...........................ø...
00400040  ..º..´.Í!..LÍ!This program cannot be run in DOS mode....$.......
00400080  àÀ:Ñ¤¤T.¤¤T.¤¤T.ß.X.¦¤T.Ë»_.¥¤T.'.Z. ¤T.Ë»^.¯¤T.Ë»P. ¤T.g«..@¤T.
004000C0  ¤¤U..¤T..._.£¤T.c¢R.¥¤T.Rich¤¤T.......................PE..L...
00400100  A.çL........à.......p... 5.....ºw.............@..............
00400140  ......... 5..................................Ö..d...
00400180  .... .4.............................................
004001C0  ...................ø.........................text...°i.....
00400200  .p..................  .rdata..p_.........................@..@
00400240  .data...X....à... ...à..............@..À.rsrc... .4...... 4.....
00400280  ..............@..@.........................................
```

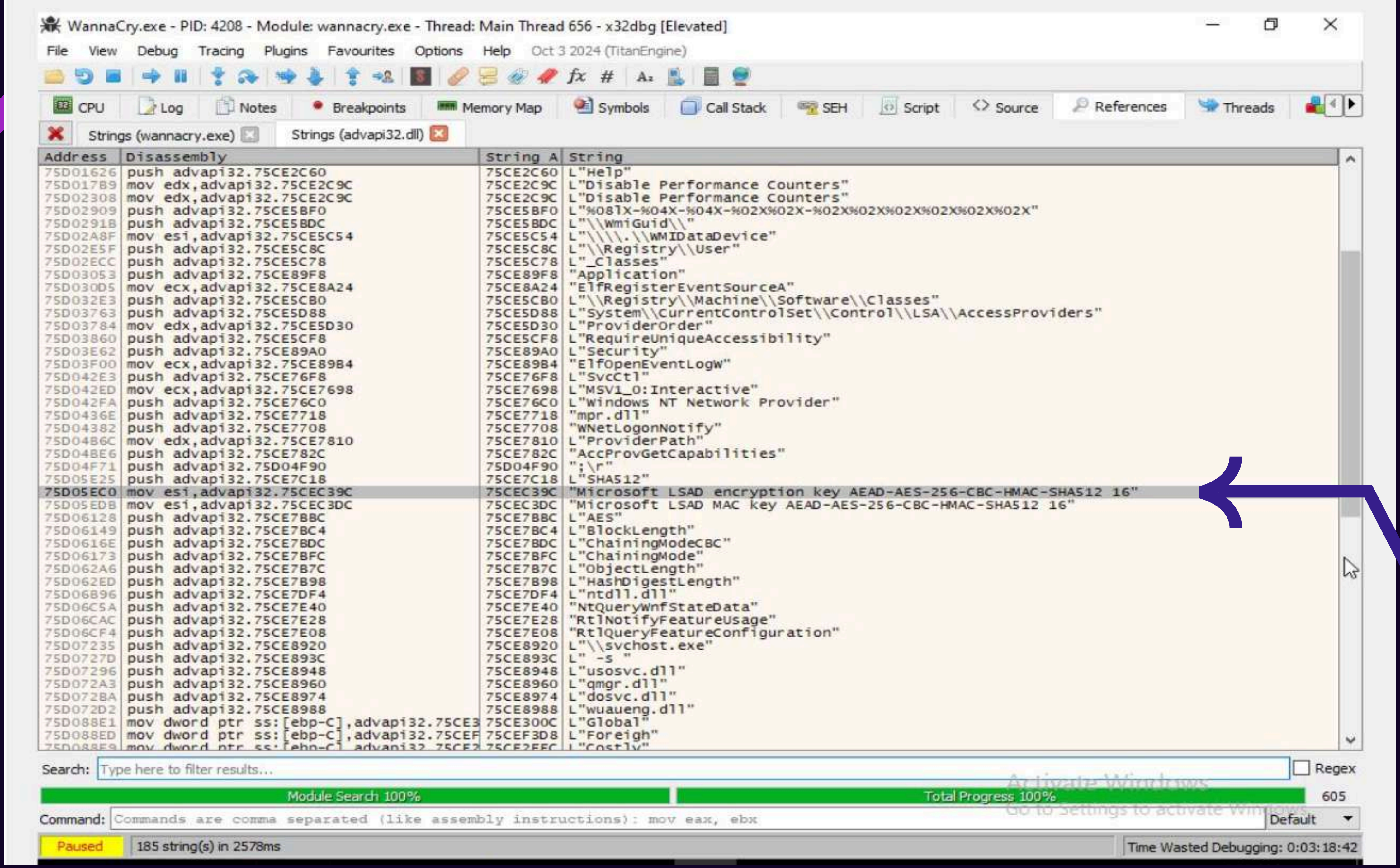
```
0019FA1C  D09B6405
0019FA20  771369FC  ntdll."minkernel\\ntdll\\ldrinit.c"
0019FA24  77136A78  ntdll."LdrpInitializeProcess"
0019FA28  00000000
0019FA2C  00A63AE8
0019FA30  0019FA1C
0019FA34  771DC15A  return to ntdll.RtlCaptureStackConte
0019FA38  0019FC9C  Pointer to SEH_Record[1]
0019FA3C  771AAE00  ntdll.wcstombs+70
0019FA40  A7A1503D
0019FA44  00000000
0019FA48  0019FCAC
0019FA4C  771DC16B  return to ntdll.RtlCaptureStackConte
0019FA50  D09B62E1
```

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

Paused    185 string(s) in 2750ms    Time Wasted Debugging: 0:03:15:22

A breakpoint was set in advapi32.dll, targeting cryptographic functions to identify WannaCry's encryption algorithm.

# Discovering Key Encryption Algorithm



WannaCry.exe - PID: 4208 - Module: wannacry.exe - Thread: Main Thread 656 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Oct 3 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Symbols Call Stack SEH Script Source References Threads
Strings (wannacry.exe) Strings (advapi32.dll)

```
Address  Disassembly                                String A String
75D01626 push advapi32.75CE2C60                     75CE2C60 L"Help"
75D017B9 mov edx,advapi32.75CE2C9C                  75CE2C9C L"Disable Performance Counters"
75D02308 mov edx,advapi32.75CE2C9C                  75CE2C9C L"Disable Performance Counters"
75D02909 push advapi32.75CE5BF0                     75CE5BF0 L"%08lX-%04X-%04X-%02X%02X-%02X%02X%02X%02X%02X%02X"
75D0291B push advapi32.75CE5BDC                     75CE5BDC L"\\WmiGuid\\"
75D02A8F mov esi,advapi32.75CE5C54                  75CE5C54 L"\\\\.\\WMIDataDevice"
75D02E5F push advapi32.75CE5C8C                     75CE5C8C L"\\Registry\\User"
75D02ECC push advapi32.75CE5C78                     75CE5C78 L"_Classes"
75D03053 push advapi32.75CE89F8                     75CE89F8 "Application"
75D030D5 mov ecx,advapi32.75CE8A24                  75CE8A24 "ElfRegisterEventSourceA"
75D032E3 push advapi32.75CE5CB0                     75CE5CB0 L"\\Registry\\Machine\\Software\\Classes"
75D03763 push advapi32.75CE5D88                     75CE5D88 L"System\\CurrentControlSet\\Control\\LSA\\AccessProviders"
75D03784 mov edx,advapi32.75CE5D30                  75CE5D30 L"ProviderOrder"
75D03860 push advapi32.75CE5CF8                     75CE5CF8 L"RequireUniqueAccessibility"
75D03E62 push advapi32.75CE89A0                     75CE89A0 L"Security"
75D03F00 mov ecx,advapi32.75CE89B4                  75CE89B4 "ElfOpenEventLogW"
75D042E3 push advapi32.75CE76F8                     75CE76F8 L"SvcCtl"
75D042ED mov ecx,advapi32.75CE7698                  75CE7698 L"MSV1_0:Interactive"
75D042FA push advapi32.75CE76C0                     75CE76C0 L"Windows NT Network Provider"
75D0436E push advapi32.75CE7718                     75CE7718 "mpr.dll"
75D04382 push advapi32.75CE7708                     75CE7708 "WNetLogonNotify"
75D04B6C mov edx,advapi32.75CE7810                  75CE7810 L"ProviderPath"
75D04BE6 push advapi32.75CE782C                     75CE782C "AccProvGetCapabilities"
75D04F71 push advapi32.75D04F90                     75D04F90 ";\r"
75D05E25 push advapi32.75CE7C18                     75CE7C18 L"SHA512"
75D05EC0 mov esi,advapi32.75CEC39C                  75CEC39C "Microsoft LSAD encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"
75D05EDB mov esi,advapi32.75CEC3DC                  75CEC3DC "Microsoft LSAD MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"
75D06128 push advapi32.75CE7BBC                     75CE7BBC L"AES"
75D06149 push advapi32.75CE7BC4                     75CE7BC4 L"BlockLength"
75D0616E push advapi32.75CE7BDC                     75CE7BDC L"ChainingModeCBC"
75D06173 push advapi32.75CE7BFC                     75CE7BFC L"ChainingMode"
75D062A6 push advapi32.75CE7B7C                     75CE7B7C L"ObjectLength"
75D062ED push advapi32.75CE7B98                     75CE7B98 L"HashDigestLength"
75D06B96 push advapi32.75CE7DF4                     75CE7DF4 L"ntdll.dll"
75D06C5A push advapi32.75CE7E40                     75CE7E40 "NtQueryWnfStateData"
75D06CAC push advapi32.75CE7E28                     75CE7E28 "RtlNotifyFeatureUsage"
75D06CF4 push advapi32.75CE7E08                     75CE7E08 "RtlQueryFeatureConfiguration"
75D07235 push advapi32.75CE8920                     75CE8920 L"\\svchost.exe"
75D0727D push advapi32.75CE893C                     75CE893C L" -s "
75D07296 push advapi32.75CE8948                     75CE8948 L"usosvc.dll"
75D072A3 push advapi32.75CE8960                     75CE8960 L"qmgr.dll"
75D072BA push advapi32.75CE8974                     75CE8974 L"dosvc.dll"
75D072D2 push advapi32.75CE8988                     75CE8988 L"wuaueng.dll"
75D088E1 mov dword ptr ss:[ebp-C],advapi32.75CE3 75CE300C L"Global"
75D088ED mov dword ptr ss:[ebp-C],advapi32.75CEF 75CEF3D8 L"Foreigh"
75D088E9 mov dword ptr ss:[ebp-C],advapi32.75CE2 75CE2FFC L"Costly"
```

Search: Type here to filter results... □ Regex

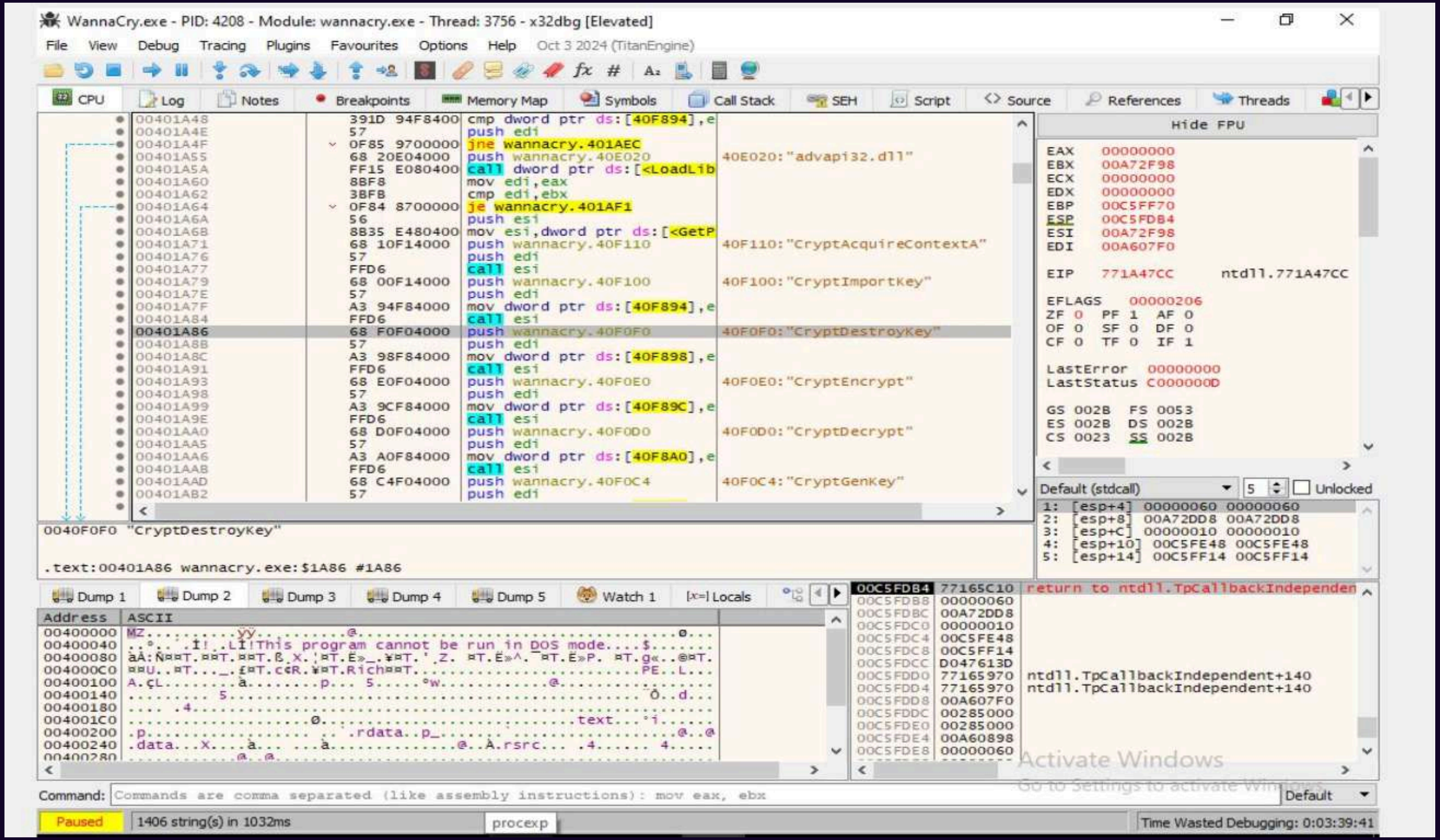
Module Search 100% Total Progress 100% 605

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

Paused 185 string(s) in 2578ms Time Wasted Debugging: 0:03:18:42

After the breakpoint, we found the encryption algorithm used by WannaCry

# Intercepting CryptDestroyKey for Insights


WannaCry.exe - PID: 4208 - Module: wannacry.exe - Thread: 3756 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Oct 3 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Symbols Call Stack SEH Script Source References Threads
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals
Default (stdcall) 5 □ Unlocked
Default

```
00401A48   391D 94F8400   cmp dword ptr ds:[40F894],e
00401A4E   57             push edi
00401A4F   0F85 9700000   jne wannacry.401AEC
00401A55   68 20E04000    push wannacry.40E020           40E020:"advapi32.dll"
00401A5A   FF15 E080400   call dword ptr ds:[<LoadLib
00401A60   8BF8           mov edi,eax
00401A62   3BFB           cmp edi,ebx
00401A64   0F84 8700000   je wannacry.401AF1
00401A6A   56             push esi
00401A6B   8B35 E480400   mov esi,dword ptr ds:[<GetP
00401A71   68 10F14000    push wannacry.40F110           40F110:"CryptAcquireContextA"
00401A76   57             push edi
00401A77   FFD6           call esi
00401A79   68 00F14000    push wannacry.40F100           40F100:"CryptImportKey"
00401A7E   57             push edi
00401A7F   A3 94F84000    mov dword ptr ds:[40F894],e
00401A84   FFD6           call esi
00401A86   68 F0F04000    push wannacry.40F0F0           40F0F0:"CryptDestroyKey"
00401A8B   57             push edi
00401A8C   A3 98F84000    mov dword ptr ds:[40F898],e
00401A91   FFD6           call esi
00401A93   68 E0F04000    push wannacry.40F0E0           40F0E0:"CryptEncrypt"
00401A98   57             push edi
00401A99   A3 9CF84000    mov dword ptr ds:[40F89C],e
00401A9E   FFD6           call esi
00401AA0   68 D0F04000    push wannacry.40F0D0           40F0D0:"CryptDecrypt"
00401AA5   57             push edi
00401AA6   A3 A0F84000    mov dword ptr ds:[40F8A0],e
00401AAB   FFD6           call esi
00401AAD   68 C4F04000    push wannacry.40F0C4           40F0C4:"CryptGenKey"
00401AB2   57             push edi

0040F0F0 "CryptDestroyKey"

.text:00401A86 wannacry.exe:$1A86 #1A86
```

```
EAX     00000000
EBX     00A72F98
ECX     00000000
EDX     00000000
EBP     00C5FF70
ESP     00C5FDB4
ESI     00A72F98
EDI     00A607F0

EIP     771A47CC      ntdll.771A47CC

EFLAGS    00000206
ZF 0   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1

LastError   00000000
LastStatus  C000000D

GS 002B   FS 0053
ES 002B   DS 002B
CS 0023   SS 002B
```

```
1:  [esp+4]  00000060 00000060
2:  [esp+8]  00A72DD8 00A72DD8
3:  [esp+C]  00000010 00000010
4:  [esp+10] 00C5FE48 00C5FE48
5:  [esp+14] 00C5FF14 00C5FF14
```

```
Address   ASCII
00400000  MZ..........ÿÿ.........@..............................ø...
00400040  ..º..´.Í!..LÍ!This program cannot be run in DOS mode....$.......
00400080  àÀ:Ñ¤¤T.¤¤T.¤¤T.ß X.¦¤T.È»_.¥¤T.'.Z. ¤T.È»^.¯¤T.È»P. ¤T.g«..@¤T.
004000C0  ¤¤U..¤T..._.£¤T.c¢R.¥¤T.Rich¤¤T.......................PE..L...
00400100  A.çL.......à........p... 5.....°w...........@..............
00400140  .........5.........................................Ô..d...
00400180  .... .4...................................................
004001C0  .....................ø...........................text...`i.....
00400200  .p......................rdata..p_...........................@..@
00400240  .data...X....à......à.............@..À.rsrc... .4...... 4.....
00400280  ..............@..@.........................................
```

```
00C5FDB4  77165C10  return to ntdll.TpCallbackIndependen
00C5FDB8  00000060
00C5FDBC  00A72DD8
00C5FDC0  00000010
00C5FDC4  00C5FE48
00C5FDC8  00C5FF14
00C5FDCC  D047613D
00C5FDD0  77165970  ntdll.TpCallbackIndependent+140
00C5FDD4  77165970  ntdll.TpCallbackIndependent+140
00C5FDD8  00A607F0
00C5FDDC  00285000
00C5FDE0  00285000
00C5FDE4  00A60898
00C5FDE8  00000060
```

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

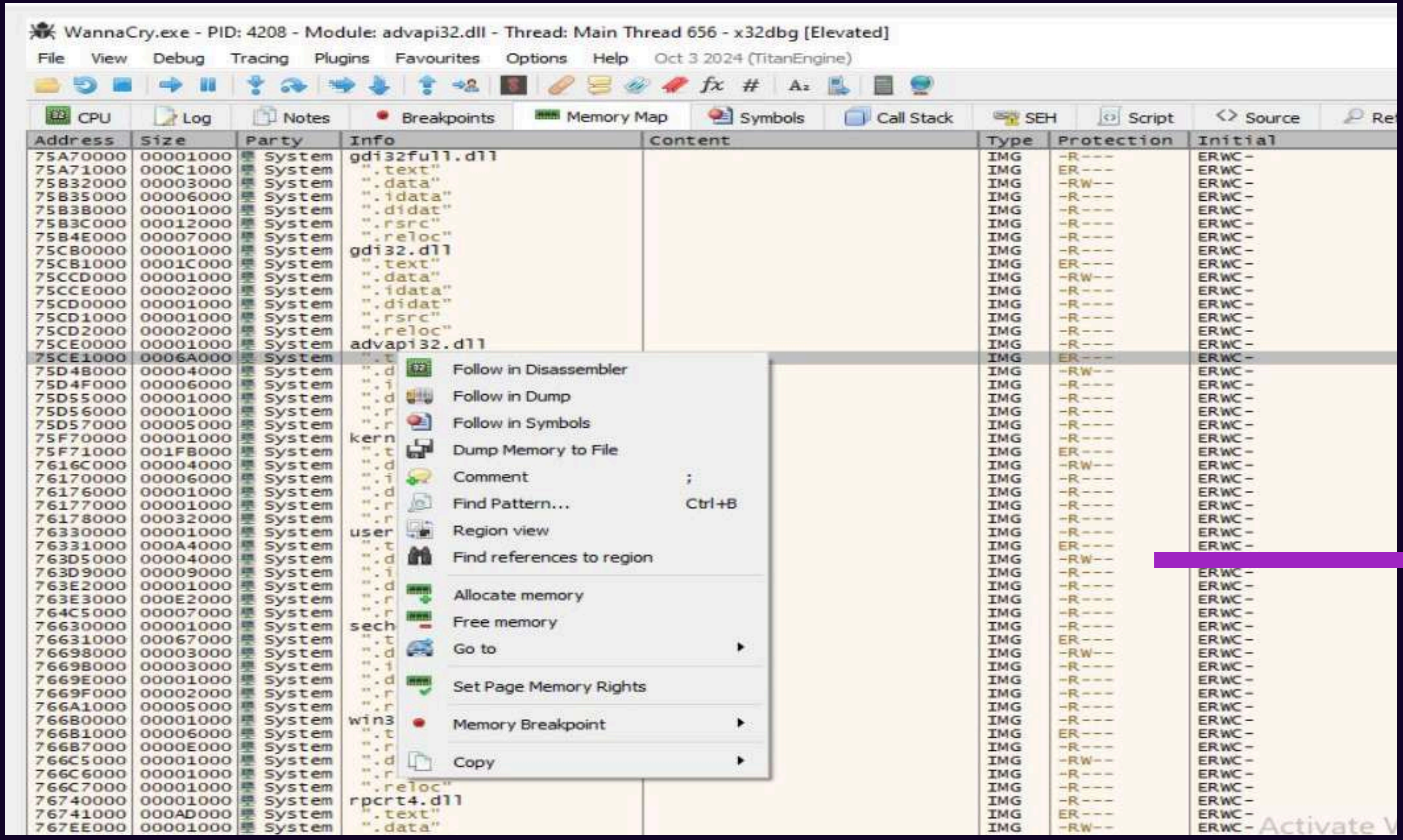
Paused | 1406 string(s) in 1032ms | procexp | Time Wasted Debugging: 0:03:39:41

Activate Windows
Go to Settings to activate Windows.

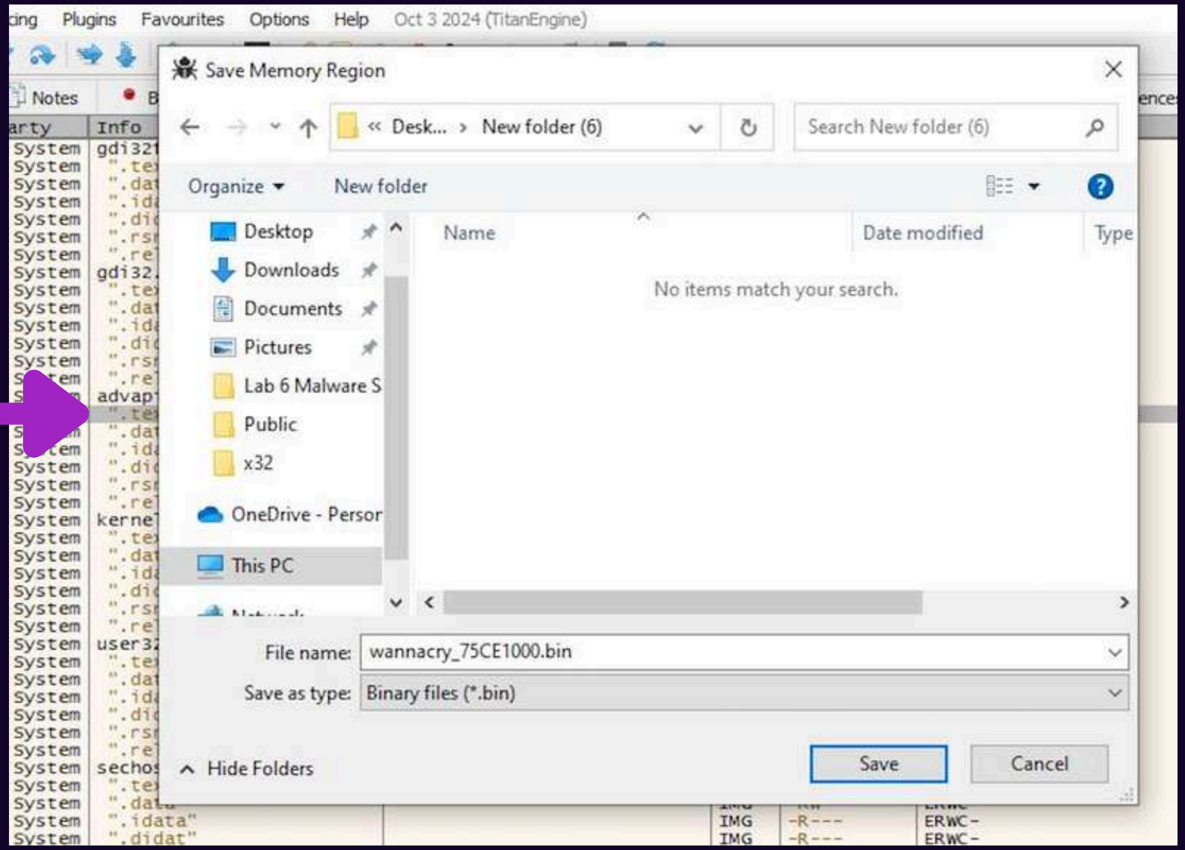
We use CryptDestroyKey as a breakpoint to capture the AES key and other valuable information before they are erased, providing crucial insights for analysis.

# Dumping Key Data

After hitting the CryptDestroyKey and also advapi breakpoint, we saved a memory dump from dll,  This dump includes decrypted data and essential information



```
Address   Size      Party   Info            Content  Type  Protection  Initial
75A70000  00001000  System  gdi32full.dll            IMG   -R---       ERWC-
75A71000  000C1000  System   ".text"                 IMG   ER---       ERWC-
75B32000  00003000  System   ".data"                 IMG   -RW--       ERWC-
75B35000  00006000  System   ".idata"                IMG   -R---       ERWC-
75B3B000  00001000  System   ".didat"                IMG   -R---       ERWC-
75B3C000  00012000  System   ".rsrc"                 IMG   -R---       ERWC-
75B4E000  00007000  System   ".reloc"                IMG   -R---       ERWC-
75CB0000  00001000  System  gdi32.dll                IMG   -R---       ERWC-
75CB1000  0001C000  System   ".text"                 IMG   ER---       ERWC-
75CCD000  00001000  System   ".data"                 IMG   -RW--       ERWC-
75CCE000  00002000  System   ".idata"                IMG   -R---       ERWC-
75CD0000  00001000  System   ".didat"                IMG   -R---       ERWC-
75CD1000  00001000  System   ".rsrc"                 IMG   -R---       ERWC-
75CD2000  00002000  System   ".reloc"                IMG   -R---       ERWC-
75CE0000  00001000  System  advapi32.dll             IMG   -R---       ERWC-
75CE1000  0006A000  System   ".t                     IMG   ER---       ERWC-
75D4B000  00004000  System   ".d                     IMG   -RW--       ERWC-
75D4F000  00006000  System   ".i                     IMG   -R---       ERWC-
75D55000  00001000  System   ".d                     IMG   -R---       ERWC-
75D56000  00001000  System   ".r                     IMG   -R---       ERWC-
75D57000  00005000  System   ".r                     IMG   -R---       ERWC-
75F70000  00001000  System  kern                     IMG   -R---       ERWC-
75F71000  001FB000  System   ".t                     IMG   ER---       ERWC-
7616C000  00004000  System   ".d                     IMG   -RW--       ERWC-
76170000  00006000  System   ".i                     IMG   -R---       ERWC-
76176000  00001000  System   ".d                     IMG   -R---       ERWC-
76177000  00001000  System   ".r                     IMG   -R---       ERWC-
76178000  00032000  System   ".r                     IMG   -R---       ERWC-
76330000  00001000  System  user                     IMG   -R---       ERWC-
76331000  000A4000  System   ".t                     IMG   ER---       ERWC-
763D5000  00004000  System   ".d                     IMG   -RW--       ERWC-
763D9000  00009000  System   ".i                     IMG   -R---       ERWC-
763E2000  00001000  System   ".d                     IMG   -R---       ERWC-
763E3000  000E2000  System   ".r                     IMG   -R---       ERWC-
764C5000  00007000  System   ".r                     IMG   -R---       ERWC-
76630000  00001000  System  sech                     IMG   -R---       ERWC-
76631000  00067000  System   ".t                     IMG   ER---       ERWC-
76698000  00003000  System   ".d                     IMG   -RW--       ERWC-
7669B000  00003000  System   ".i                     IMG   -R---       ERWC-
7669E000  00001000  System   ".d                     IMG   -R---       ERWC-
7669F000  00002000  System   ".r                     IMG   -R---       ERWC-
766A1000  00005000  System   ".r                     IMG   -R---       ERWC-
766B0000  00001000  System  win3                     IMG   -R---       ERWC-
766B1000  00006000  System   ".t                     IMG   ER---       ERWC-
766B7000  0000E000  System   ".r                     IMG   -R---       ERWC-
766C5000  00001000  System   ".d                     IMG   -RW--       ERWC-
766C6000  00001000  System   ".r                     IMG   -R---       ERWC-
766C7000  00001000  System   ".reloc"                IMG   -R---       ERWC-
76740000  00001000  System  rpcrt4.dll               IMG   -R---       ERWC-
76741000  000AD000  System   ".text"                 IMG   ER---       ERWC-
767EE000  00001000  System   ".data"                 IMG   -RW--       ERWC-
```



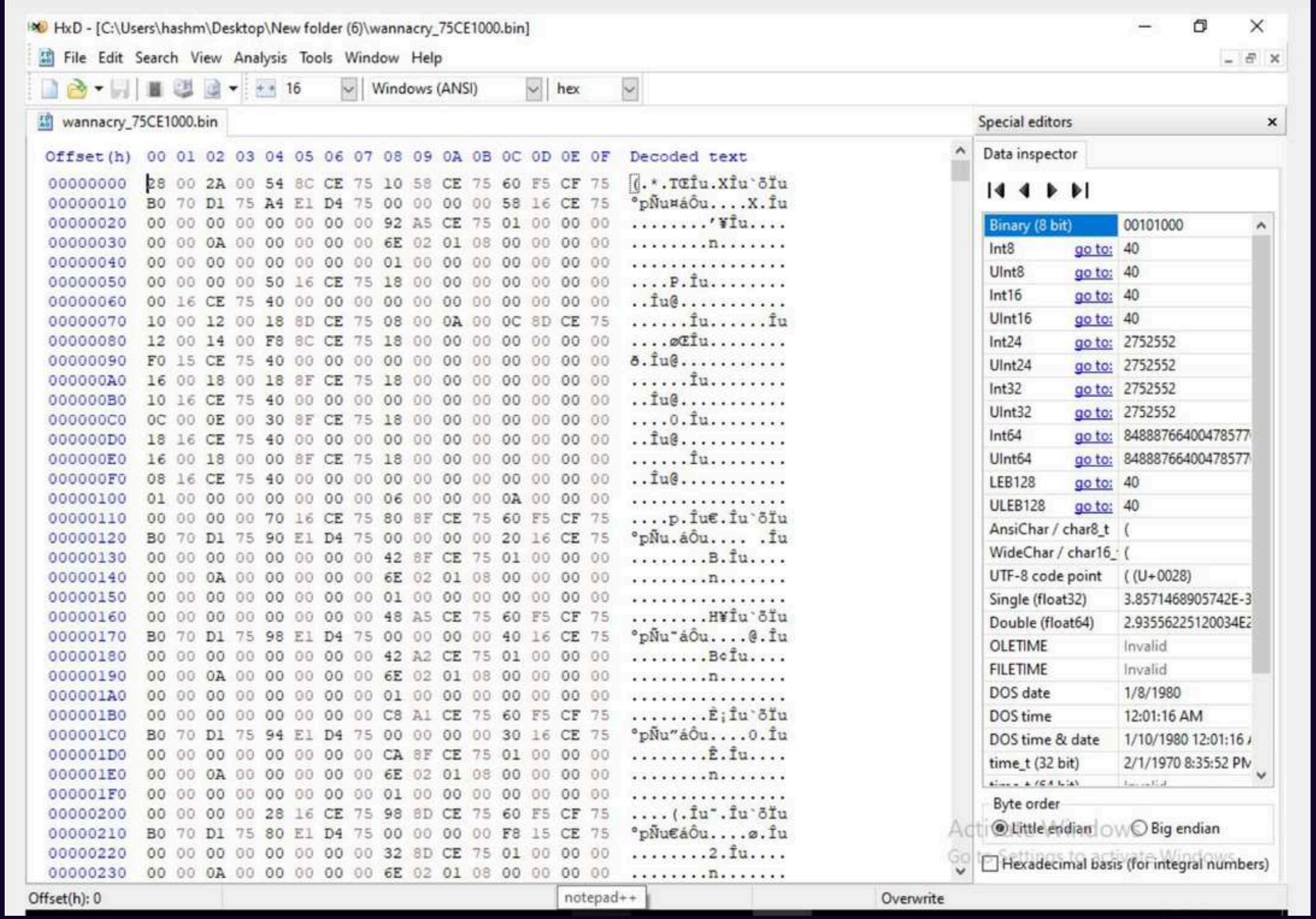
No items match your search.

File name: wannacry_75CE1000.bin

Save as type: Binary files (*.bin)

# Examining the Dump in HxD

The saved dump was opened in HxD, a hex editor, to inspect and correct the binary data. HxD is useful for low-level file corrections


HxD - [C:\Users\hashm\Desktop\New folder (6)\wannacry_75CE1000.bin]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
wannacry_75CE1000.bin
Special editors
Data inspector
notepad++
Overwrite

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  28 00 2A 00 54 8C CE 75 10 58 CE 75 60 F5 CF 75  (.*.TŒÎu.XÎu`õÏu
00000010  B0 70 D1 75 A4 E1 D4 75 00 00 00 00 58 16 CE 75  °pÑu¤áÔu....X.Îu
00000020  00 00 00 00 00 00 00 00 92 A5 CE 75 01 00 00 00  ........’¥Îu....
00000030  00 00 0A 00 00 00 00 00 6E 02 01 08 00 00 00 00  ........n.......
00000040  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 50 16 CE 75 18 00 00 00 00 00 00 00  ....P.Îu........
00000060  00 16 CE 75 40 00 00 00 00 00 00 00 00 00 00 00  ..Îu@...........
00000070  10 00 12 00 18 8D CE 75 08 00 0A 00 0C 8D CE 75  ......Îu......Îu
00000080  12 00 14 00 F8 8C CE 75 18 00 00 00 00 00 00 00  ....øŒÎu........
00000090  F0 15 CE 75 40 00 00 00 00 00 00 00 00 00 00 00  ð.Îu@...........
000000A0  16 00 18 00 18 8F CE 75 18 00 00 00 00 00 00 00  ......Îu........
000000B0  10 16 CE 75 40 00 00 00 00 00 00 00 00 00 00 00  ..Îu@...........
000000C0  0C 00 0E 00 30 8F CE 75 18 00 00 00 00 00 00 00  ....0.Îu........
000000D0  18 16 CE 75 40 00 00 00 00 00 00 00 00 00 00 00  ..Îu@...........
000000E0  16 00 18 00 00 8F CE 75 18 00 00 00 00 00 00 00  ......Îu........
000000F0  08 16 CE 75 40 00 00 00 00 00 00 00 00 00 00 00  ..Îu@...........
00000100  01 00 00 00 00 00 00 00 06 00 00 00 0A 00 00 00  ................
00000110  00 00 00 00 70 16 CE 75 80 8F CE 75 60 F5 CF 75  ....p.Îu€.Îu`õÏu
00000120  B0 70 D1 75 90 E1 D4 75 00 00 00 00 20 16 CE 75  °pÑu.áÔu.... .Îu
00000130  00 00 00 00 00 00 00 00 42 8F CE 75 01 00 00 00  ........B.Îu....
00000140  00 00 0A 00 00 00 00 00 6E 02 01 08 00 00 00 00  ........n.......
00000150  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
00000160  00 00 00 00 00 00 00 00 48 A5 CE 75 60 F5 CF 75  ........H¥Îu`õÏu
00000170  B0 70 D1 75 98 E1 D4 75 00 00 00 00 40 16 CE 75  °pÑu˜áÔu....@.Îu
00000180  00 00 00 00 00 00 00 00 42 A2 CE 75 01 00 00 00  ........B¢Îu....
00000190  00 00 0A 00 00 00 00 00 6E 02 01 08 00 00 00 00  ........n.......
000001A0  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
000001B0  00 00 00 00 00 00 00 00 C8 A1 CE 75 60 F5 CF 75  ........È¡Îu`õÏu
000001C0  B0 70 D1 75 94 E1 D4 75 00 00 00 00 30 16 CE 75  °pÑu”áÔu....0.Îu
000001D0  00 00 00 00 00 00 00 00 CA 8F CE 75 01 00 00 00  ........Ê.Îu....
000001E0  00 00 0A 00 00 00 00 00 6E 02 01 08 00 00 00 00  ........n.......
000001F0  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
00000200  00 00 00 00 28 16 CE 75 98 8D CE 75 60 F5 CF 75  ....(.Îu˜.Îu`õÏu
00000210  B0 70 D1 75 80 E1 D4 75 00 00 00 00 F8 15 CE 75  °pÑu€áÔu....ø.Îu
00000220  00 00 00 00 00 00 00 00 32 8D CE 75 01 00 00 00  ........2.Îu....
00000230  00 00 0A 00 00 00 00 00 6E 02 01 08 00 00 00 00  ........n.......
```

Offset(h): 0

| | | |
|---|---|---|
| Binary (8 bit) | | 00101000 |
| Int8 | go to: | 40 |
| UInt8 | go to: | 40 |
| Int16 | go to: | 40 |
| UInt16 | go to: | 40 |
| Int24 | go to: | 2752552 |
| UInt24 | go to: | 2752552 |
| Int32 | go to: | 2752552 |
| UInt32 | go to: | 2752552 |
| Int64 | go to: | 848887664004785777 |
| UInt64 | go to: | 848887664004785777 |
| LEB128 | go to: | 40 |
| ULEB128 | go to: | 40 |
| AnsiChar / char8_t | | ( |
| WideChar / char16_ | | ( |
| UTF-8 code point | | ( (U+0028) |
| Single (float32) | | 3.8571468905742E-3 |
| Double (float64) | | 2.93556225120034E2 |
| OLETIME | | Invalid |
| FILETIME | | Invalid |
| DOS date | | 1/8/1980 |
| DOS time | | 12:01:16 AM |
| DOS time & date | | 1/10/1980 12:01:16 A |
| time_t (32 bit) | | 2/1/1970 8:35:52 PM |

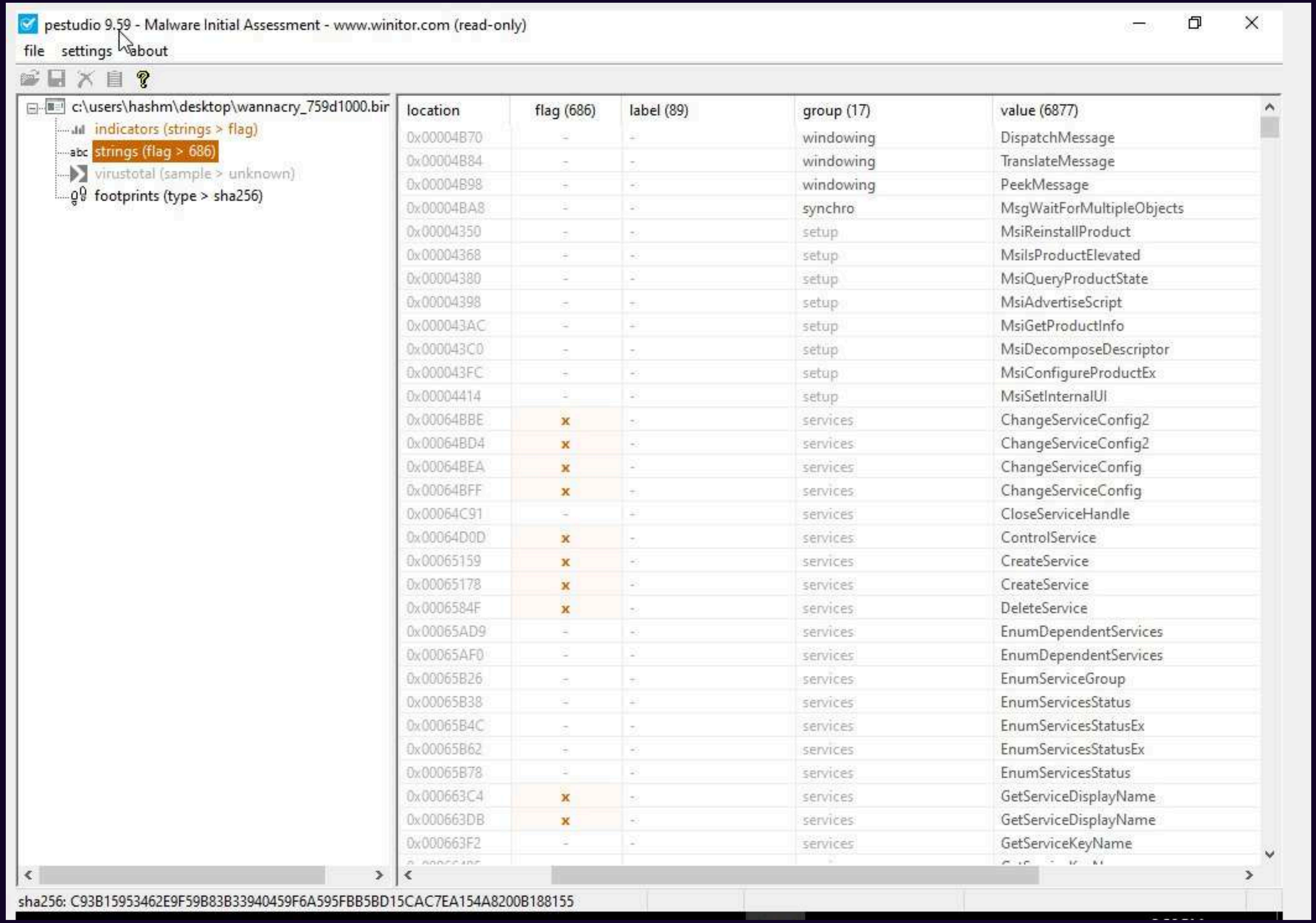
Byte order

● Little endian ○ Big endian

□ Hexadecimal basis (for integral numbers)

# PeStudio String Analysis for Hidden Clues

Using PeStudio, we analyzed strings within the dumped file to identify interesting text and clues about the ransomware's behavior.


pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)
file
settings
about

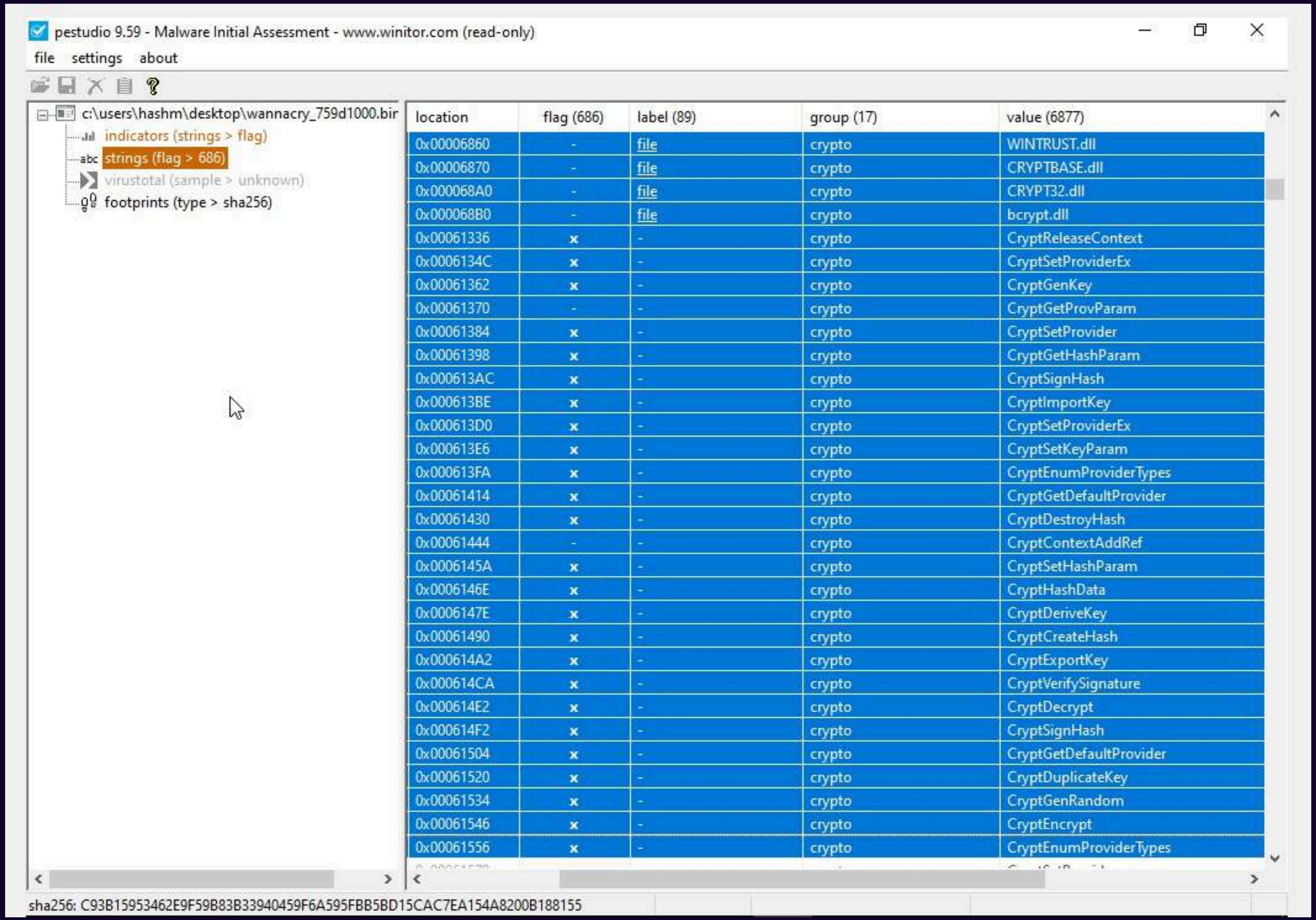
c:\users\hashm\desktop\wannacry_759d1000.bir
- indicators (strings > flag)
- strings (flag > 686)
- virustotal (sample > unknown)
- footprints (type > sha256)

| location | flag (686) | label (89) | group (17) | value (6877) |
|---|---|---|---|---|
| 0x00004B70 | - | - | windowing | DispatchMessage |
| 0x00004B84 | - | - | windowing | TranslateMessage |
| 0x00004B98 | - | - | windowing | PeekMessage |
| 0x00004BA8 | - | - | synchro | MsgWaitForMultipleObjects |
| 0x00004350 | - | - | setup | MsiReinstallProduct |
| 0x00004368 | - | - | setup | MsiIsProductElevated |
| 0x00004380 | - | - | setup | MsiQueryProductState |
| 0x00004398 | - | - | setup | MsiAdvertiseScript |
| 0x000043AC | - | - | setup | MsiGetProductInfo |
| 0x000043C0 | - | - | setup | MsiDecomposeDescriptor |
| 0x000043FC | - | - | setup | MsiConfigureProductEx |
| 0x00004414 | - | - | setup | MsiSetInternalUI |
| 0x00064BBE | x | - | services | ChangeServiceConfig2 |
| 0x00064BD4 | x | - | services | ChangeServiceConfig2 |
| 0x00064BEA | x | - | services | ChangeServiceConfig |
| 0x00064BFF | x | - | services | ChangeServiceConfig |
| 0x00064C91 | - | - | services | CloseServiceHandle |
| 0x00064D0D | x | - | services | ControlService |
| 0x00065159 | x | - | services | CreateService |
| 0x00065178 | x | - | services | CreateService |
| 0x0006584F | x | - | services | DeleteService |
| 0x00065AD9 | - | - | services | EnumDependentServices |
| 0x00065AF0 | - | - | services | EnumDependentServices |
| 0x00065B26 | - | - | services | EnumServiceGroup |
| 0x00065B38 | - | - | services | EnumServicesStatus |
| 0x00065B4C | - | - | services | EnumServicesStatusEx |
| 0x00065B62 | - | - | services | EnumServicesStatusEx |
| 0x00065B78 | - | - | services | EnumServicesStatus |
| 0x000663C4 | x | - | services | GetServiceDisplayName |
| 0x000663DB | x | - | services | GetServiceDisplayName |
| 0x000663F2 | - | - | services | GetServiceKeyName |

sha256: C93B15953462E9F59B83B33940459F6A595FBB5BD15CAC7EA154A8200B188155

# PeStudio String Analysis for Hidden Clues

Using PeStudio, we analyzed strings within the dumped file to identify interesting text and clues about the ransomware’s behavior.



pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)
file settings about
c:\users\hashm\desktop\wannacry_759d1000.bir
indicators (strings > flag)
strings (flag > 686)
virustotal (sample > unknown)
footprints (type > sha256)

| location | flag (686) | label (89) | group (17) | value (6877) |
|---|---|---|---|---|
| 0x00006860 | - | file | crypto | WINTRUST.dll |
| 0x00006870 | - | file | crypto | CRYPTBASE.dll |
| 0x000068A0 | - | file | crypto | CRYPT32.dll |
| 0x000068B0 | - | file | crypto | bcrypt.dll |
| 0x00061336 | x | - | crypto | CryptReleaseContext |
| 0x0006134C | x | - | crypto | CryptSetProviderEx |
| 0x00061362 | x | - | crypto | CryptGenKey |
| 0x00061370 | - | - | crypto | CryptGetProvParam |
| 0x00061384 | x | - | crypto | CryptSetProvider |
| 0x00061398 | x | - | crypto | CryptGetHashParam |
| 0x000613AC | x | - | crypto | CryptSignHash |
| 0x000613BE | x | - | crypto | CryptImportKey |
| 0x000613D0 | x | - | crypto | CryptSetProviderEx |
| 0x000613E6 | x | - | crypto | CryptSetKeyParam |
| 0x000613FA | x | - | crypto | CryptEnumProviderTypes |
| 0x00061414 | x | - | crypto | CryptGetDefaultProvider |
| 0x00061430 | x | - | crypto | CryptDestroyHash |
| 0x00061444 | - | - | crypto | CryptContextAddRef |
| 0x0006145A | x | - | crypto | CryptSetHashParam |
| 0x0006146E | x | - | crypto | CryptHashData |
| 0x0006147E | x | - | crypto | CryptDeriveKey |
| 0x00061490 | x | - | crypto | CryptCreateHash |
| 0x000614A2 | x | - | crypto | CryptExportKey |
| 0x000614CA | x | - | crypto | CryptVerifySignature |
| 0x000614E2 | x | - | crypto | CryptDecrypt |
| 0x000614F2 | x | - | crypto | CryptSignHash |
| 0x00061504 | x | - | crypto | CryptGetDefaultProvider |
| 0x00061520 | x | - | crypto | CryptDuplicateKey |
| 0x00061534 | x | - | crypto | CryptGenRandom |
| 0x00061546 | x | - | crypto | CryptEncrypt |
| 0x00061556 | x | - | crypto | CryptEnumProviderTypes |

sha256: C93B15953462E9F59B83B33940459F6A595FBB5BD15CAC7EA154A8200B188155

# THANK YOU!