Malware Analysis

WannaCry ransomware

Yasmin Hassen

Project objective and scope

- Main objective
  - Analyze how WannaCry behaves and acts within a Windows 7 64 bits environment.
- Scope
  - Includes
    - Dynamic runtime analysis
    - IOCs
    - Tool-based observations
  - Excludes
    - Source code analysis and reverse engineering

Tools used

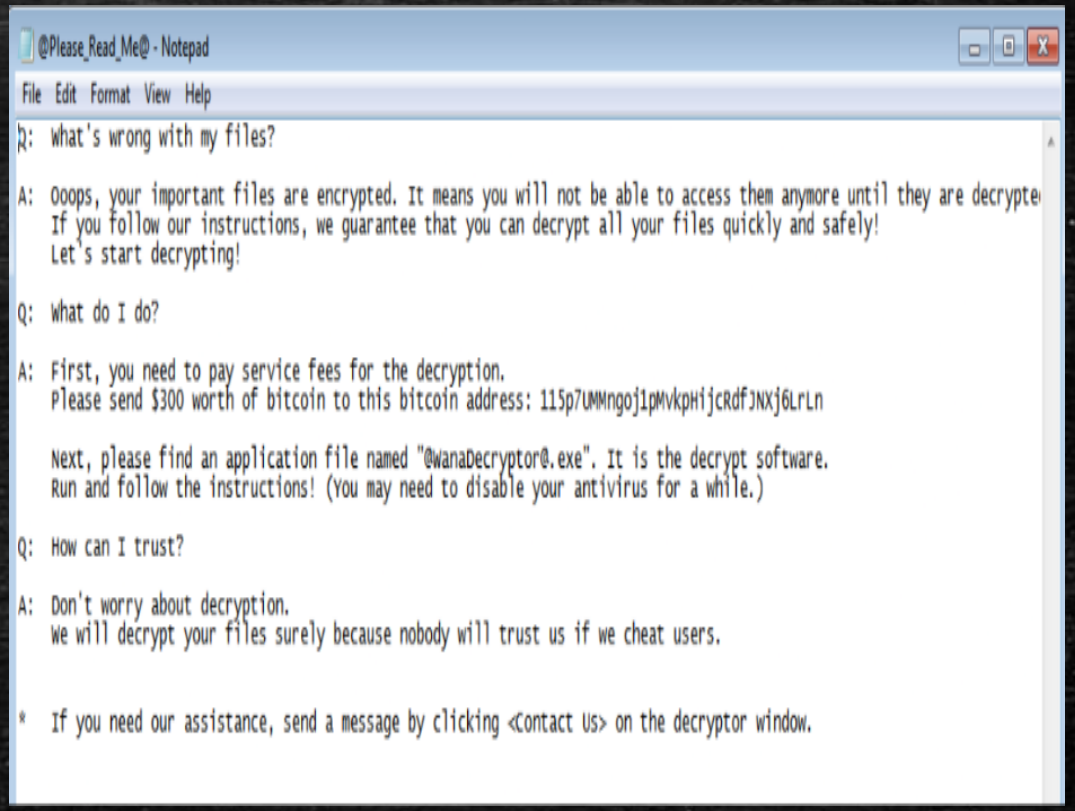
- VMware workstation
  - Win7 64 bits
  - Regshot
  - Wireshark
  - Process Monitor
  - procDot
- ANY.RUN
  - Win7 64 bit/win10

What is WannaCry Malware?

- Ransomware first released in **May 2017**
- Targets **Windows systems** (especially Windows 7)
- Encrypts user files and demands Bitcoin payment
- Variants & versions have emerged with slight modifications
- Major global outbreak — infected~200,000+ systems in 150+ countries
- Significant damage to organizations like UK’s NHS, Telefónica, FedEx

First Run


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
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
9/24/2025 11:48:24
Time Left
02:23:58:01
Your files will be lost on
9/28/2025 11:48:24
Time Left
06:23:58:01
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt


@Please_Read_Me@ - Notepad
File Edit Format View Help
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.

Registry & File Changes (Regshot)

~res-x64 - Notepad

File Edit Format View Help

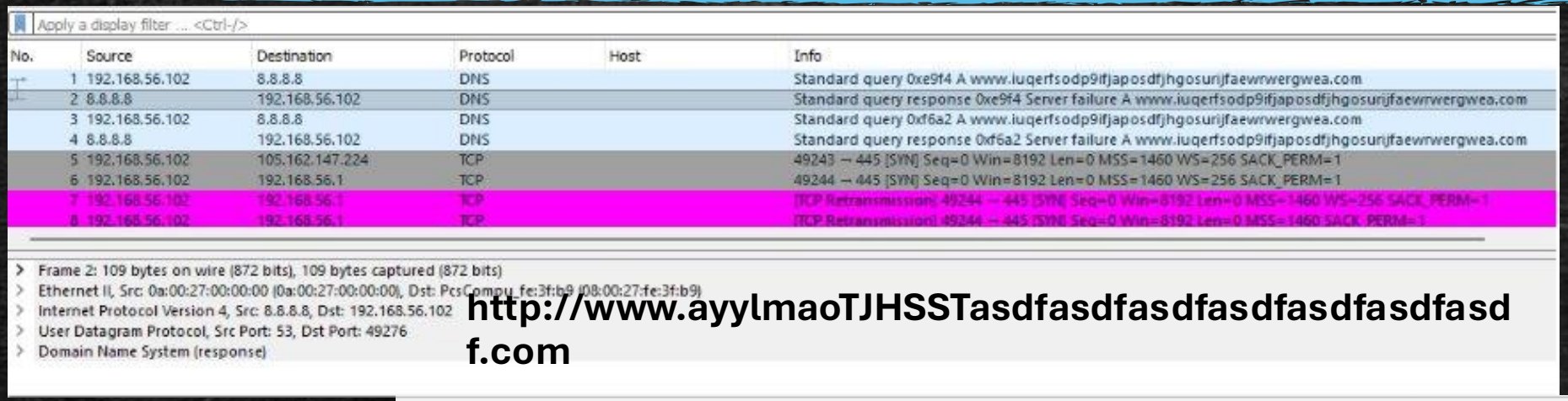
```
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2025/9/21 17:43:56   ,   2025/9/21 17:46:48
Computer: RY-PC , RY-PC
Username: RY , RY

----------------------------------
Keys added: 32
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Monitored
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Quarantined
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.exe\OpenWithList
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Microsoft\Windows Script Host
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Microsoft\Windows Script Host\Settings
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\0
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\24
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\24\Shell
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\24\Shell\{5C4F28B5-F869-4E84-8E60-F11DB
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\25
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\25\Shell
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\25\Shell\{5C4F28B5-F869-4E84-8E60-F11DB
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Classes\VirtualStore
HKU\S-1-5-21-2941047207-3759080301-1366204363-1000\Software\Classes\VirtualStore\MACHINE
```

~res-x64 - Notepad

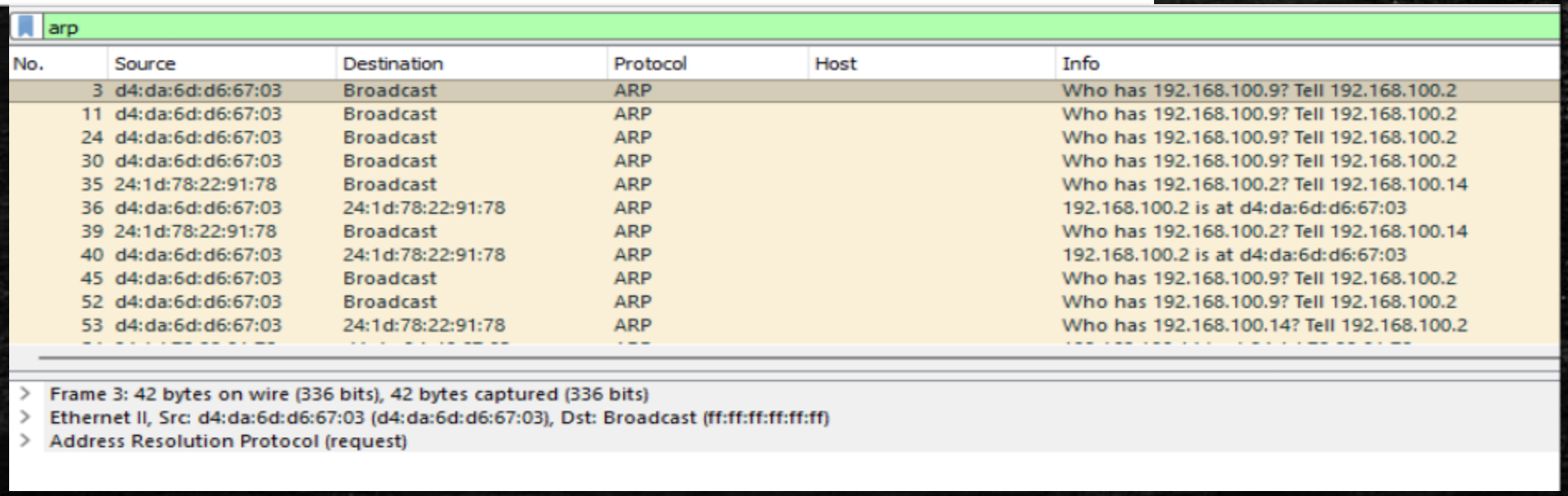
File Edit Format View Help

```
C:\wireshark\NEWS.txt.WNCRY
C:\wireshark\README.txt.WNCRY
C:\wireshark\README.windows.txt.WNCRY

----------------------------------
Files deleted: 6
----------------------------------
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS00006.log
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\MSS00006.log
C:\wireshark\COPYING.txt
C:\wireshark\NEWS.txt
C:\wireshark\README.txt
C:\wireshark\README.windows.txt

----------------------------------
Files [attributes?] modified: 43
----------------------------------
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.chk
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.log
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSStmp.log
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\MSS.chk
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\MSS.log
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\MSStmp.log
```

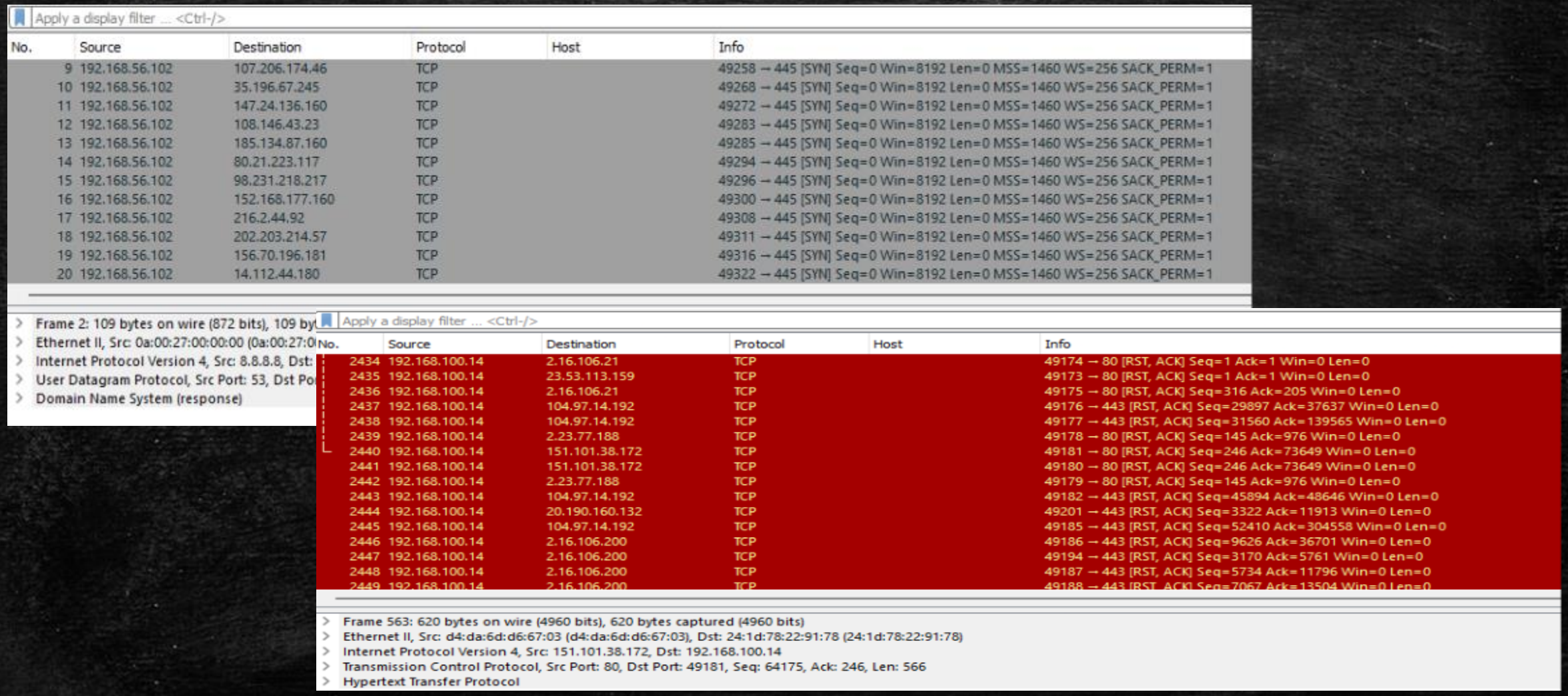
Network Behavior (Wireshark)



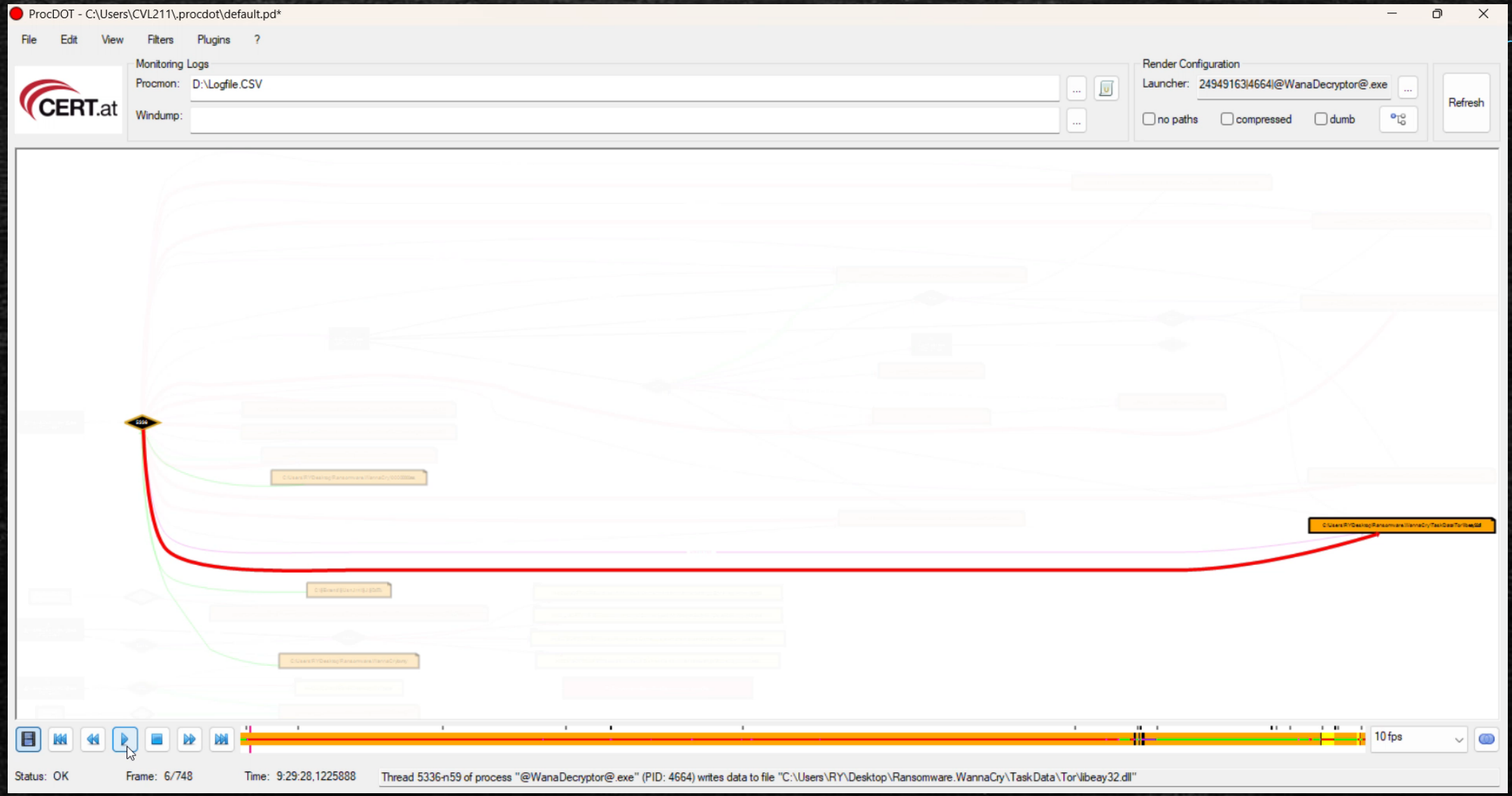
http://www.ayylmaoTJHSSTasdfasdfasdfasdfasdfasdfasdf.com



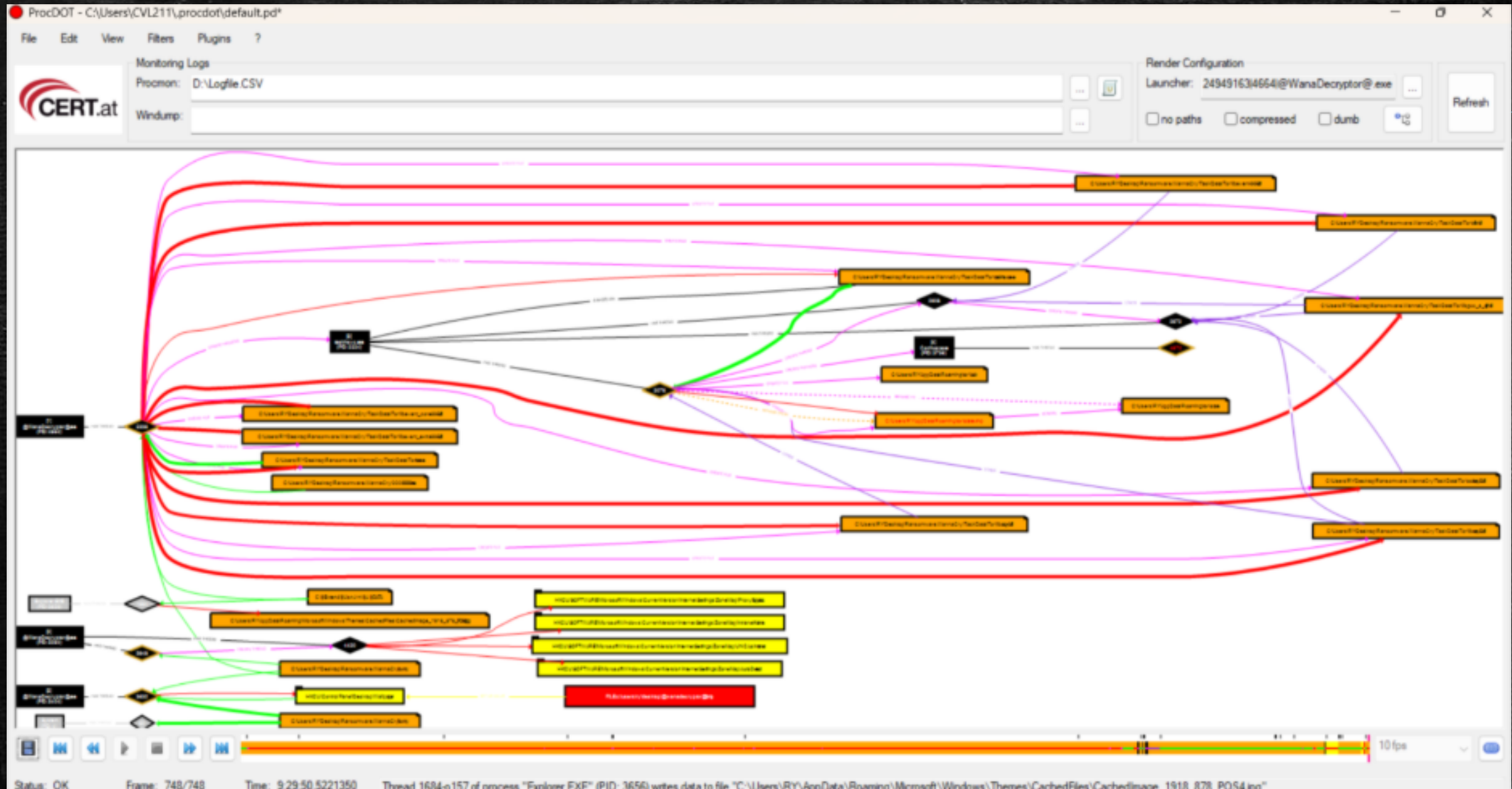
Network Behavior (Wireshark)



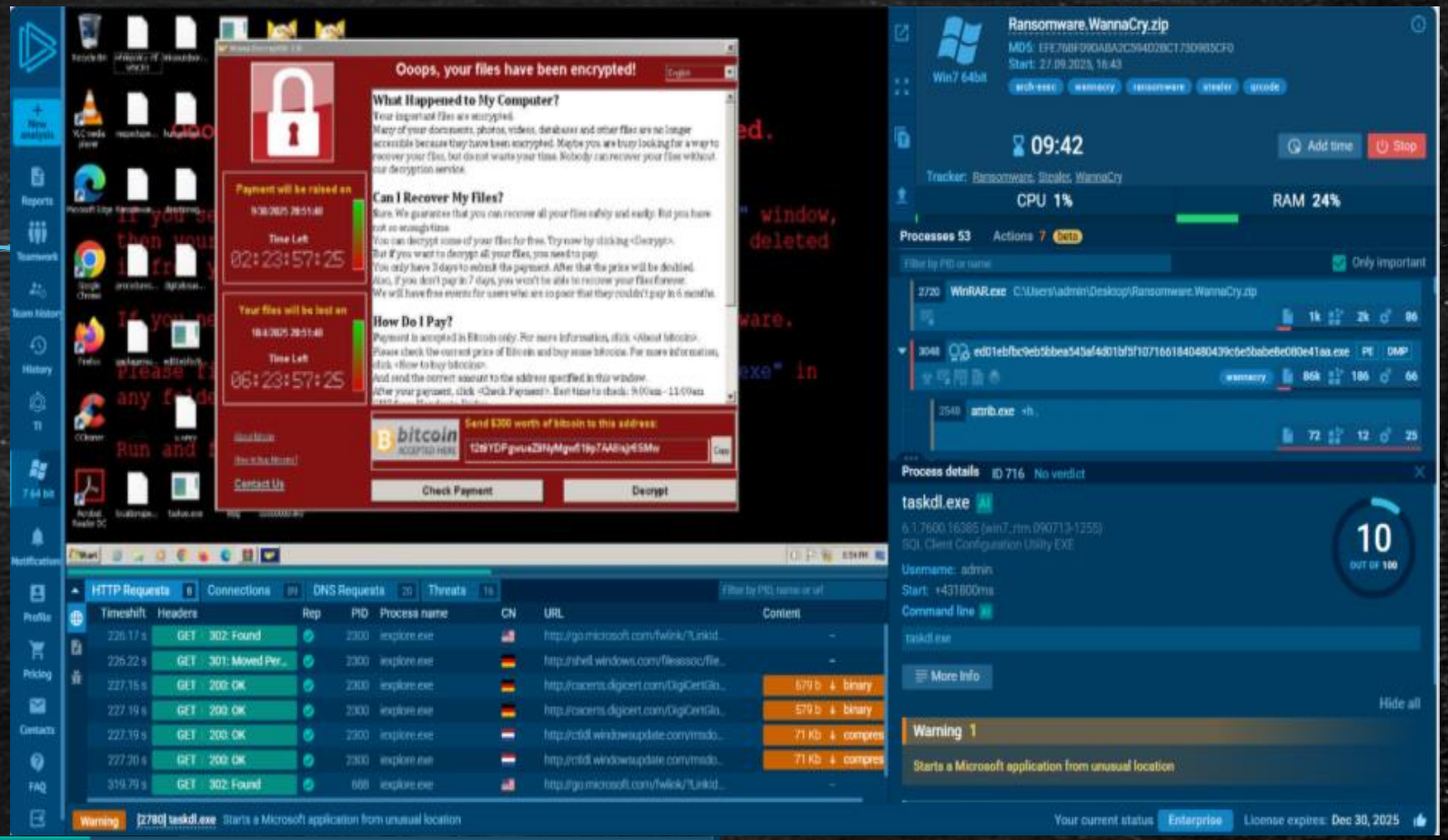
Procdot Diagram Video



ProcDot Diagram

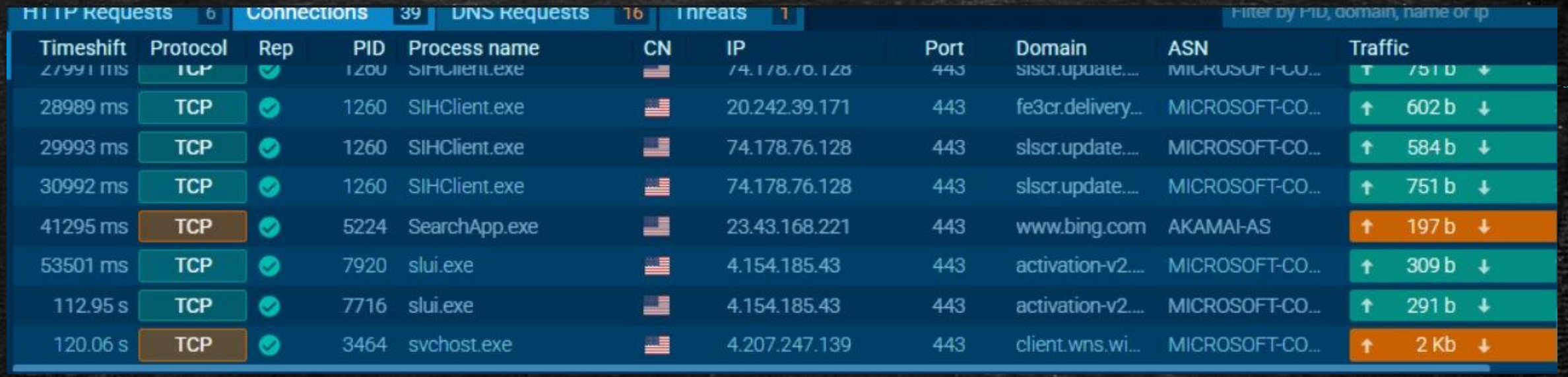


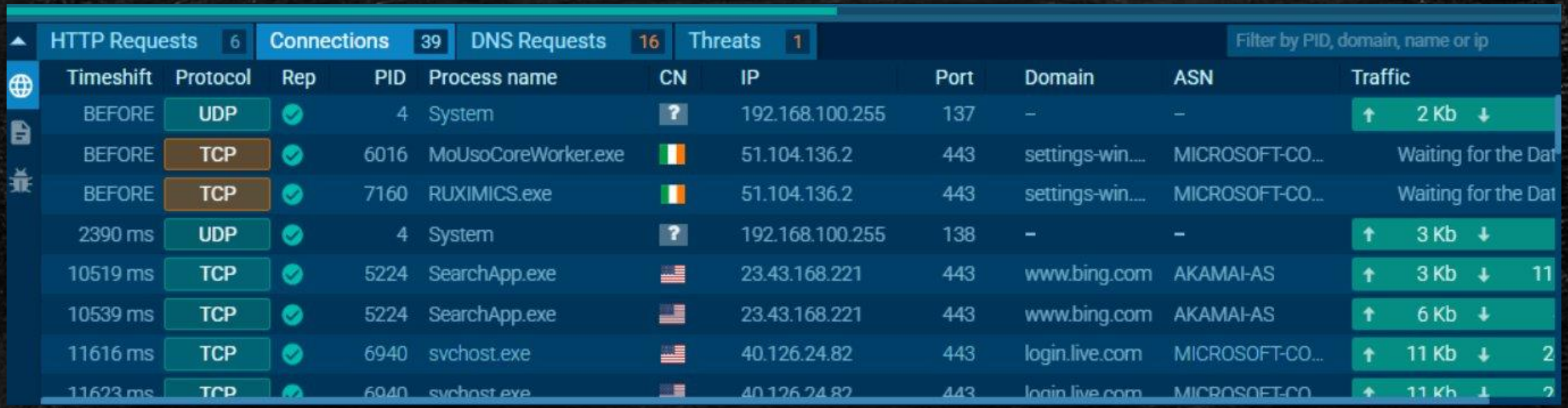
Any.Run


Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
Payment will be raised on
Time Left
02:23:57:25
Your files will be lost on
06:23:57:25
bitcoin
Send $300 worth of bitcoin to this address:
Contact Us
Check Payment
Decrypt
HTTP Requests 8
Connections 89
DNS Requests 20
Threats 15
Timeshift
Headers
Rep
PID
Process name
CN
URL
Content
GET 302: Found
GET 301: Moved Per...
GET 200: OK
Warning
[2780] taskdl.exe Starts a Microsoft application from unusual location
Ransomware.WannaCry.zip
Win7 64bit
09:42
Add time
Stop
Tracker: Ransomware, Stealer, WannaCry
CPU 1%
RAM 24%
Processes 53
Actions 7
Only important
WinRAR.exe
taskdl.exe
Process details
ID 716
No verdict
10
OUT OF 100
Username: admin
Start: +431600ms
Command line
More Info
Hide all
Warning 1
Starts a Microsoft application from unusual location
Your current status
Enterprise
License expires: Dec 30, 2025


HTTP Requests 8
Connections 90
DNS Requests 20
Threats 17
Filter by PID, name or url
Timeshift
Headers
Rep
PID
Process name
CN
URL
Content
226.17 s GET 302: Found 2300 iexplore.exe http://go.microsoft.com/fwlink/?LinkId... –
226.22 s GET 301: Moved Per... 2300 iexplore.exe http://shell.windows.com/fileassoc/file... –
227.15 s GET 200: OK 2300 iexplore.exe http://cacerts.digicert.com/DigiCertGlo... 579 b binary
227.19 s GET 200: OK 2300 iexplore.exe http://cacerts.digicert.com/DigiCertGlo... 579 b binary
227.19 s GET 200: OK 2300 iexplore.exe http://ctldl.windowsupdate.com/msdo... 71 Kb compres
227.20 s GET 200: OK 2300 iexplore.exe http://ctldl.windowsupdate.com/msdo... 71 Kb compres
319.79 s GET 302: Found 688 iexplore.exe http://go.microsoft.com/fwlink/?LinkId... –

Network connections

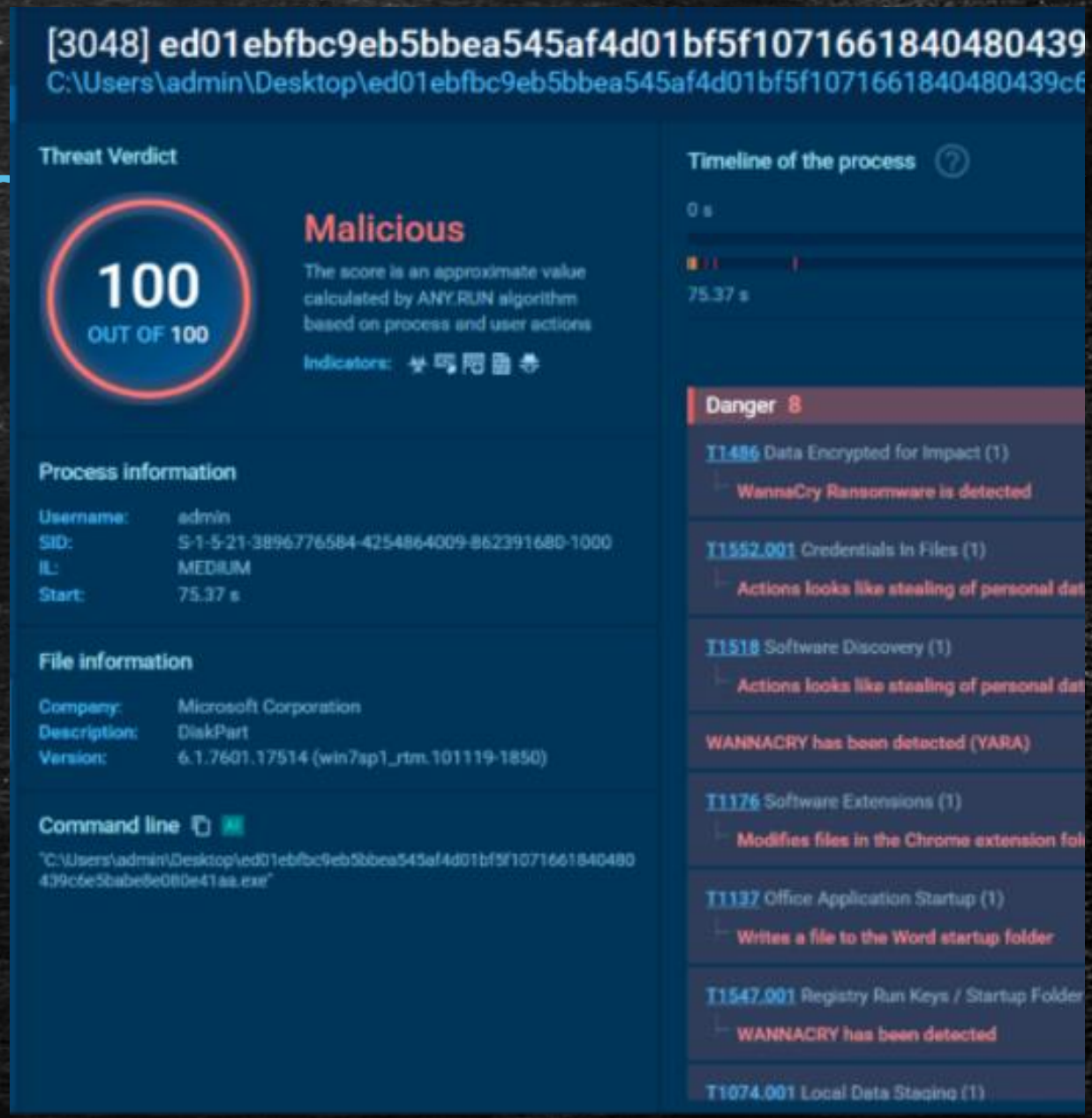




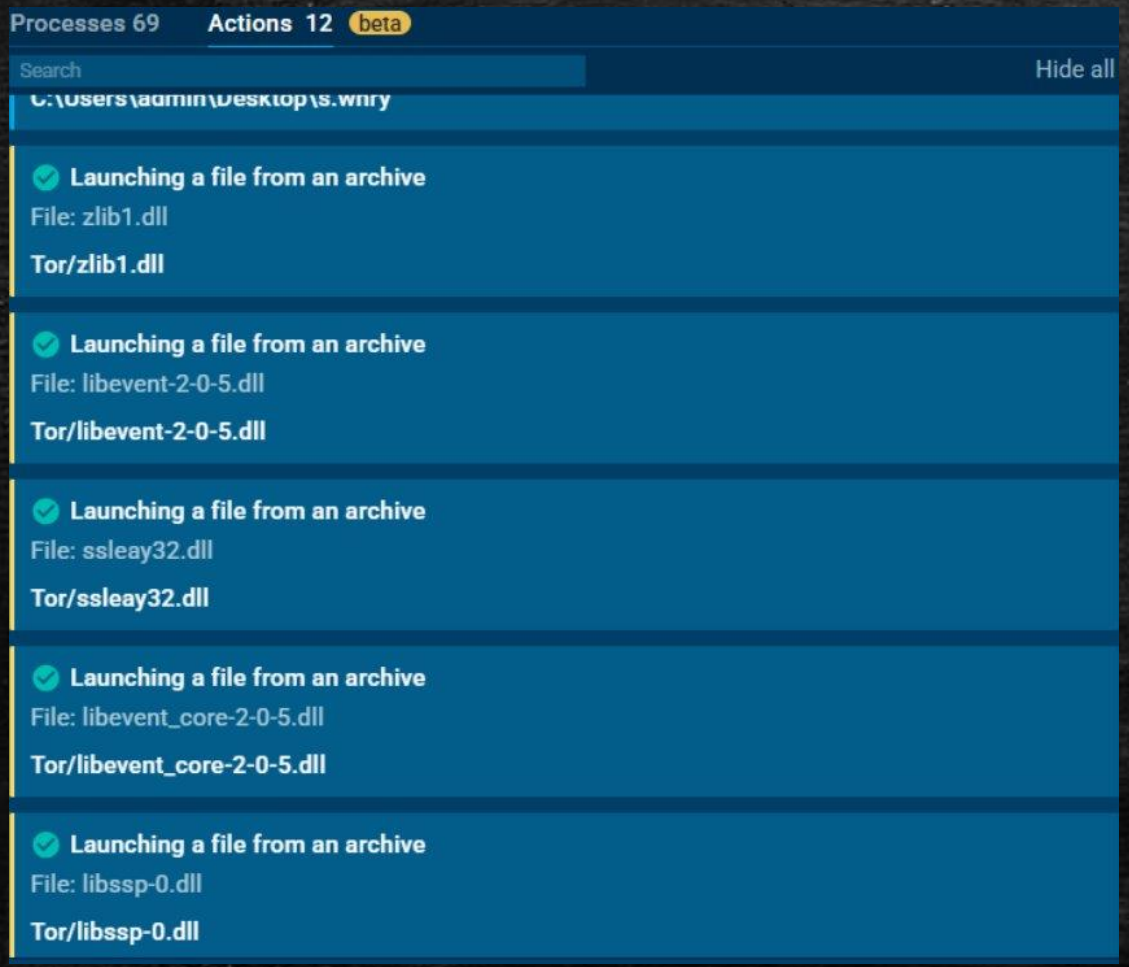
DNS Request and Threats

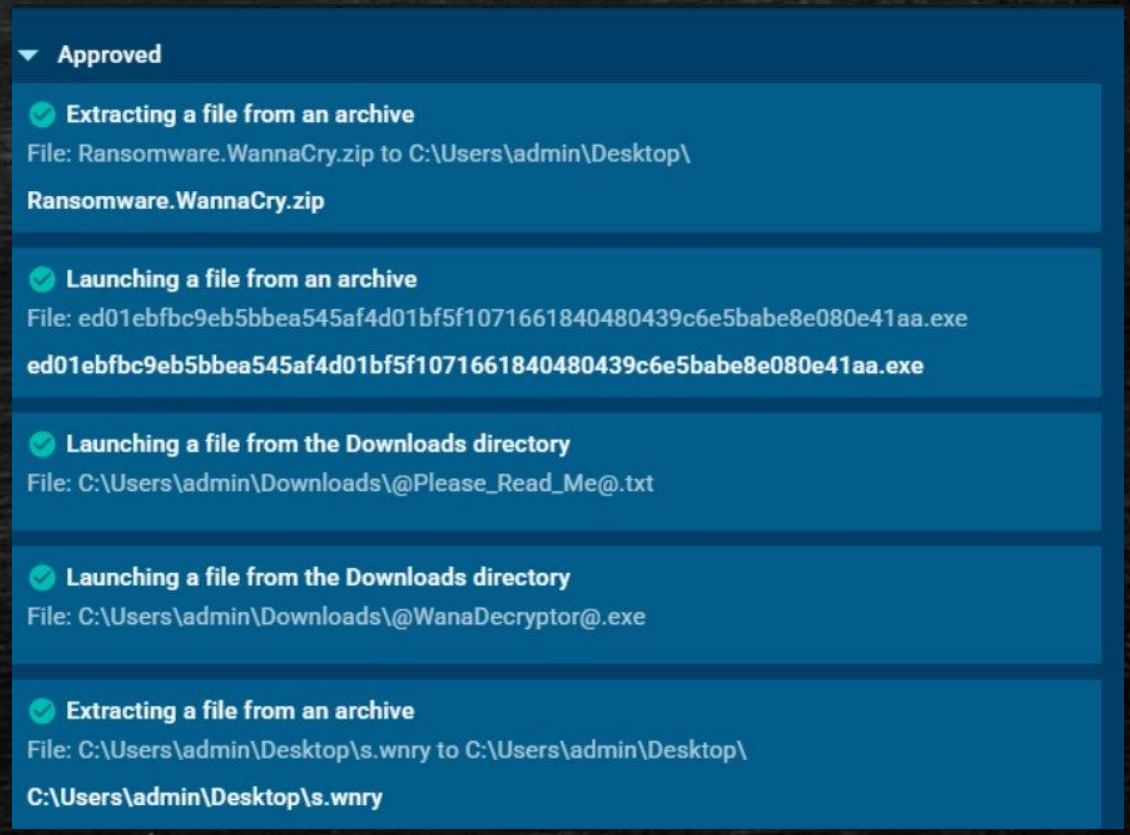

[2240] @WanaDecryptor@.exe C:\Users\admin\Desktop\@WanaDecryptor@.exe
Threat Verdict
100
OUT OF 100
Malicious
Timeline of the process
Process information
File information
Command line
Danger 4
Warning 2
Other 3


T1562.003 Impair Command History Logging (1)
Process checks Powershell history file
T1059.003 Windows Command Shell (2)
Executing commands from a *.bat* file
Starts CMD.EXE for commands execution
T1222.001 Windows File and Directory Permissions Modification (2)
Uses ATTRIB.EXE to modify file attributes
Uses ICACLS.EXE to modify access control lists
T1564.001 Hidden Files and Directories (1)
Uses ATTRIB.EXE to modify file attributes
Executable content was dropped or overwritten
T1036.003 Rename Legitimate Utilities (1)
Process drops legitimate windows executable

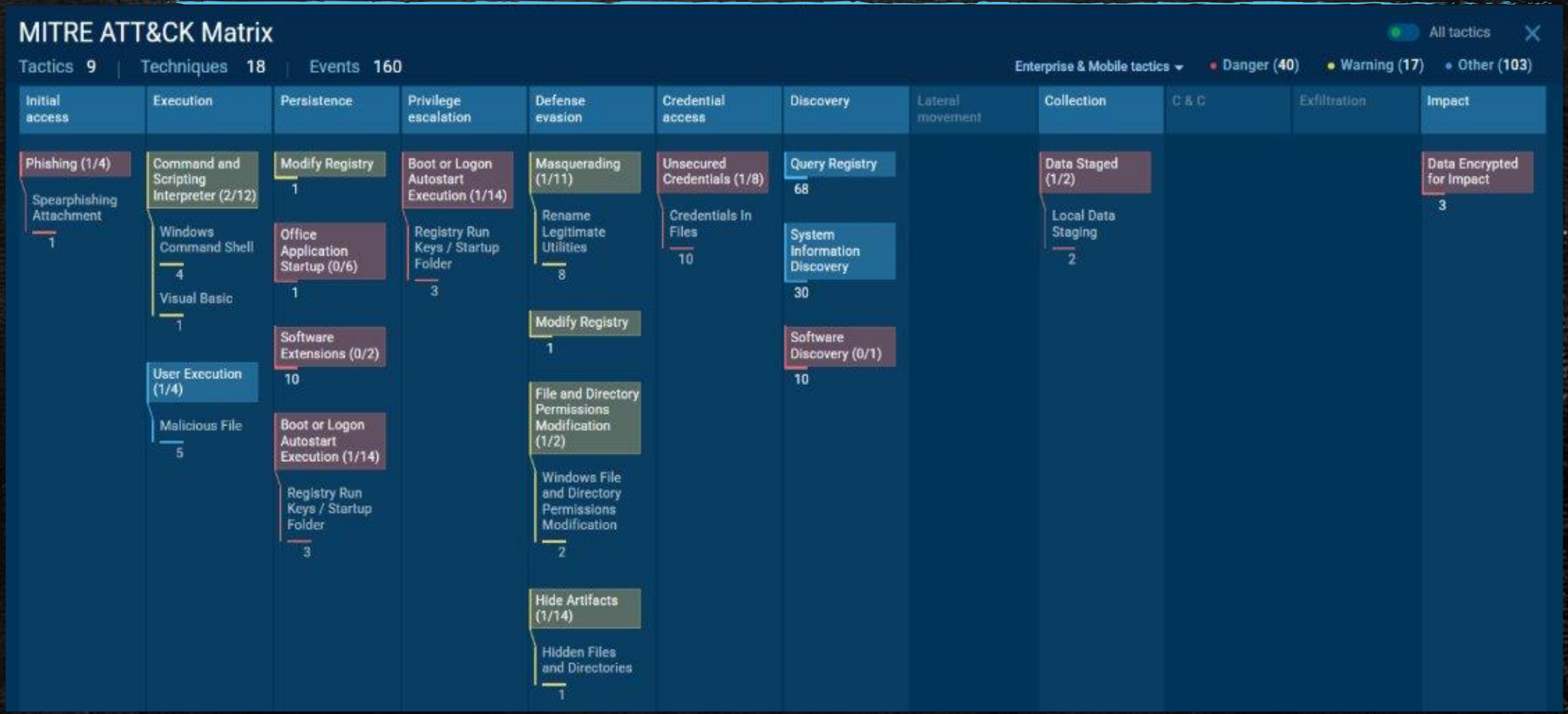

[3048] ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439
C:\Users\admin\Desktop\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6
Threat Verdict
100
OUT OF 100
Malicious
The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions
Indicators:
Process information
Username: admin
SID: S-1-5-21-3896776584-4254864009-862391680-1000
IL: MEDIUM
Start: 75.37 s
File information
Company: Microsoft Corporation
Description: DiskPart
Version: 6.1.7601.17514 (win7sp1_rtm.101119-1850)
Command line
"C:\Users\admin\Desktop\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe"
Timeline of the process
0 s
75.37 s
Danger 8
T1486 Data Encrypted for Impact (1)
WannaCry Ransomware is detected
T1552.001 Credentials In Files (1)
Actions looks like stealing of personal dat
T1518 Software Discovery (1)
Actions looks like stealing of personal dat
WANNACRY has been detected (YARA)
T1176 Software Extensions (1)
Modifies files in the Chrome extension fol
T1137 Office Application Startup (1)
Writes a file to the Word startup folder
T1547.001 Registry Run Keys / Startup Folder
WANNACRY has been detected
T1074.001 Local Data Staging (1)

File activity and Execution Flow





MITRE ATT&CK Matrix: WannaCryBehavior Overview



How to prevent it

System hardening

- Keep OS updated (MS17-010 patch blocks WannaCry exploit)
- Disable SMBv1 protocol
- Enable Windows Defender / EDR solutions

Network defense

- Use firewalls to limit outbound SMB/HTTP connections
- Segment internal networks to contain lateral spread

User behavior

- Avoid opening unknown attachments
- Regularly back up data offline
- Train users on phishing awareness

References

Bezerra, M. (2025, May 21). *WannaCry ransomware analysis: Lateral Movement propagation*. Acalvio. https://www.acalvio.com/ransomware/wannacry-ransomware-analysis-lateral-movement-propagation/

ManojPatil99. (n.d.). *Manojpatil99/WannaCry-ransomware-malware-analysis*. GitHub https://github.com/ManojPatil99/WannaCry-Ransomware-Malware-Analysis

Github https://github.com/ytisf/theZoo

Jake Walker. (2025, March 25). *Running WannaCry in a virtual machine* https://jakew.me/wannacry-vm/

Markruss. (n.d.). *Process Monitor - Sysinternals*. Process Monitor - Sysinternals | Microsoft Learn. https://learn.microsoft.com/en-us/sysinternals/downloads/procmon

Thank you