

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

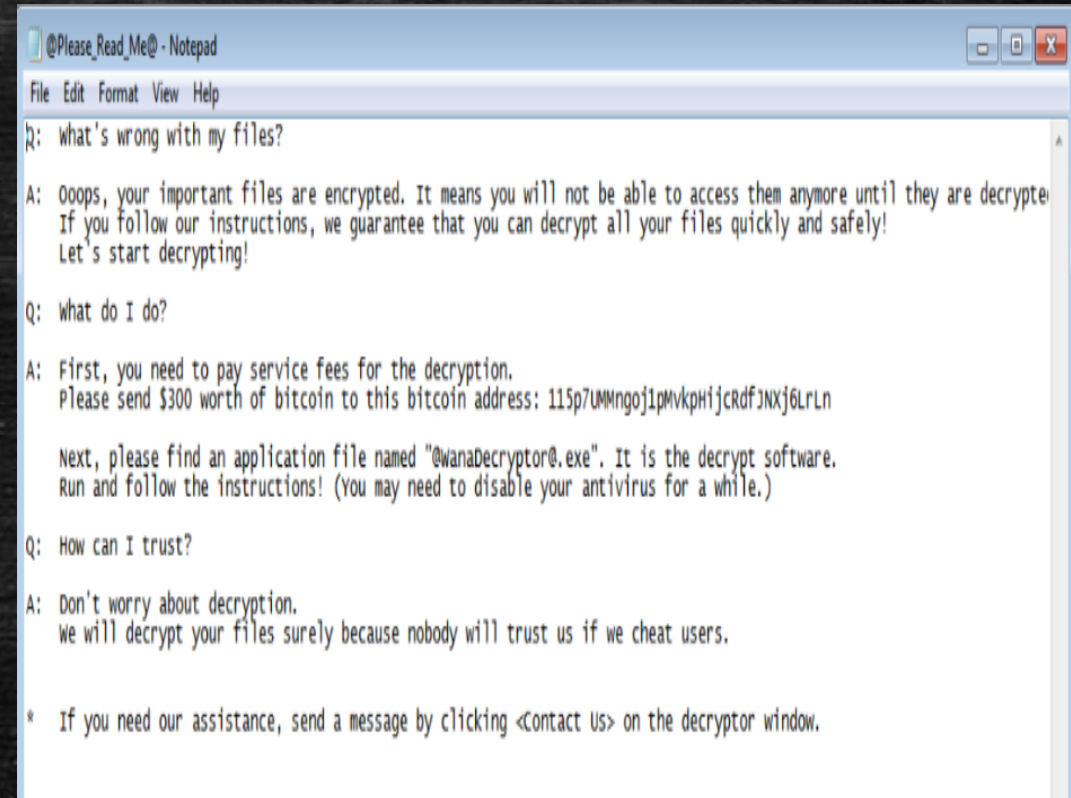
- VMware workstation
 - Win7 64 bits
 - Regshot
 - Wireshark
 - Process Monitor
 - procDot
- ANY.RUN
 - Win7 64 bit/win10

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



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\MSS000006.log
C:\Users\All Users\Microsoft\Search\Data\Applications\windows\MSS000006.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)

Apply a display filter ... <Ctrl-/>					
No.	Source	Destination	Protocol	Host	Info
1	192.168.56.102	8.8.8.8	DNS		Standard query 0xe9f4 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com
2	8.8.8.8	192.168.56.102	DNS		Standard query response 0xe9f4 Server failure A www.iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com
3	192.168.56.102	8.8.8.8	DNS		Standard query 0xf6a2 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com
4	8.8.8.8	192.168.56.102	DNS		Standard query response 0xf6a2 Server failure A www.iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com
5	192.168.56.102	105.162.147.224	TCP		49243 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
6	192.168.56.102	192.168.56.1	TCP		49244 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	192.168.56.102	192.168.56.1	TCP		[TCP Retransmission] 49244 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	192.168.56.102	192.168.56.1	TCP		[TCP Retransmission] 49244 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 2: 109 bytes on wire (872 bits), 109 bytes captured (872 bits)
> Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PcsCompu, fe:3f:b9 (08:00:27:fe:3f:b9)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.56.102
> User Datagram Protocol, Src Port: 53, Dst Port: 49276
> Domain Name System (response)

<http://www.ayylmaoTJHSSTasdfasdfasdfasdfasdfasdf.com>

arp					
No.	Source	Destination	Protocol	Host	Info
3	d4:da:6d:d6:67:03	Broadcast	ARP		Who has 192.168.100.9? Tell 192.168.100.2
11	d4:da:6d:d6:67:03	Broadcast	ARP		Who has 192.168.100.9? Tell 192.168.100.2
24	d4:da:6d:d6:67:03	Broadcast	ARP		Who has 192.168.100.9? Tell 192.168.100.2
30	d4:da:6d:d6:67:03	Broadcast	ARP		Who has 192.168.100.9? Tell 192.168.100.2
35	24:1d:78:22:91:78	Broadcast	ARP		Who has 192.168.100.2? Tell 192.168.100.14
36	d4:da:6d:d6:67:03	24:1d:78:22:91:78	ARP		192.168.100.2 is at d4:da:6d:d6:67:03
39	24:1d:78:22:91:78	Broadcast	ARP		Who has 192.168.100.2? Tell 192.168.100.14
40	d4:da:6d:d6:67:03	24:1d:78:22:91:78	ARP		192.168.100.2 is at d4:da:6d:d6:67:03
45	d4:da:6d:d6:67:03	Broadcast	ARP		Who has 192.168.100.9? Tell 192.168.100.2
52	d4:da:6d:d6:67:03	Broadcast	ARP		Who has 192.168.100.9? Tell 192.168.100.2
53	d4:da:6d:d6:67:03	24:1d:78:22:91:78	ARP		Who has 192.168.100.14? Tell 192.168.100.2

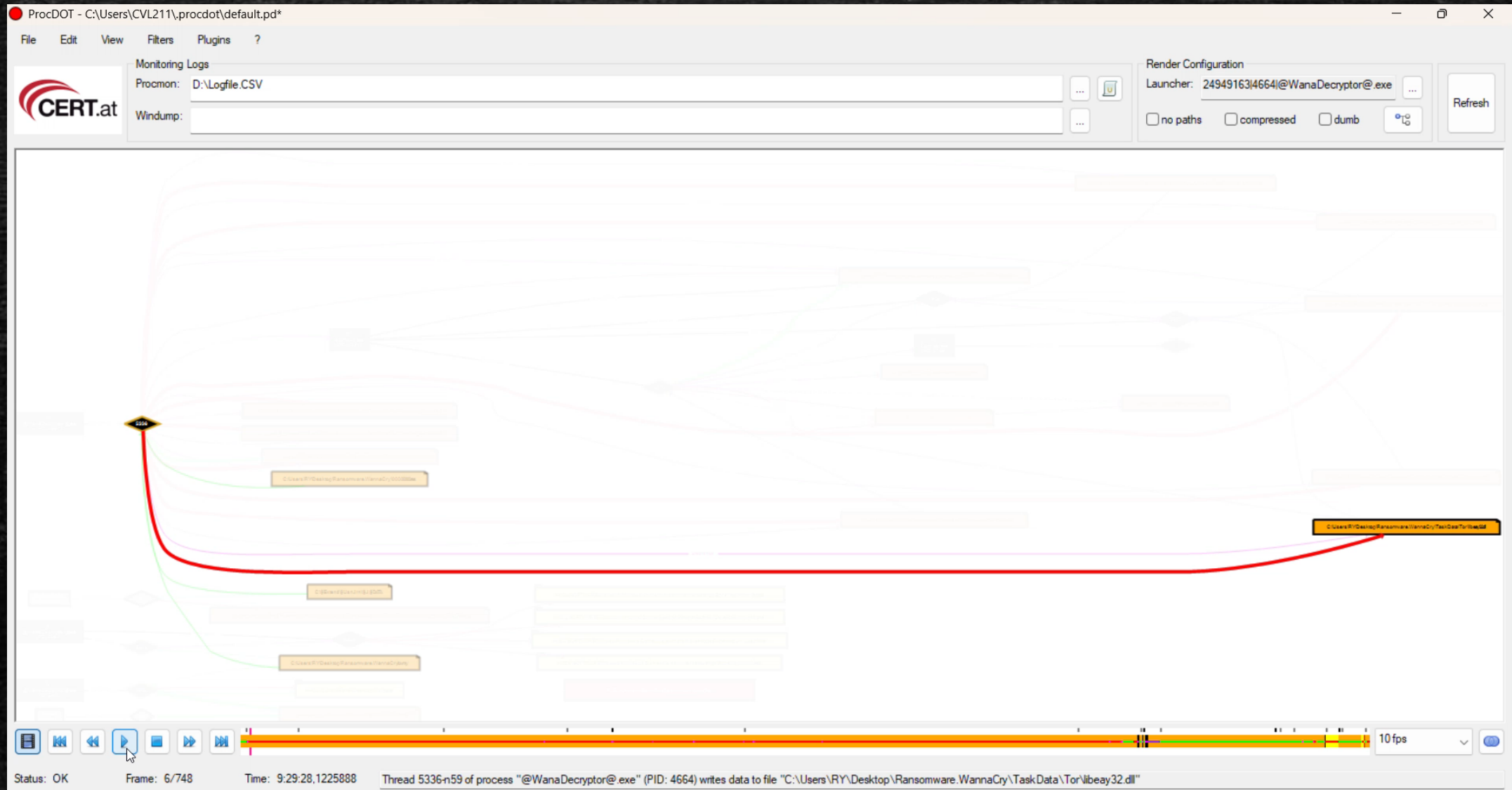
> Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: d4:da:6d:d6:67:03 (d4:da:6d:d6:67:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

Network Behavior (Wireshark)

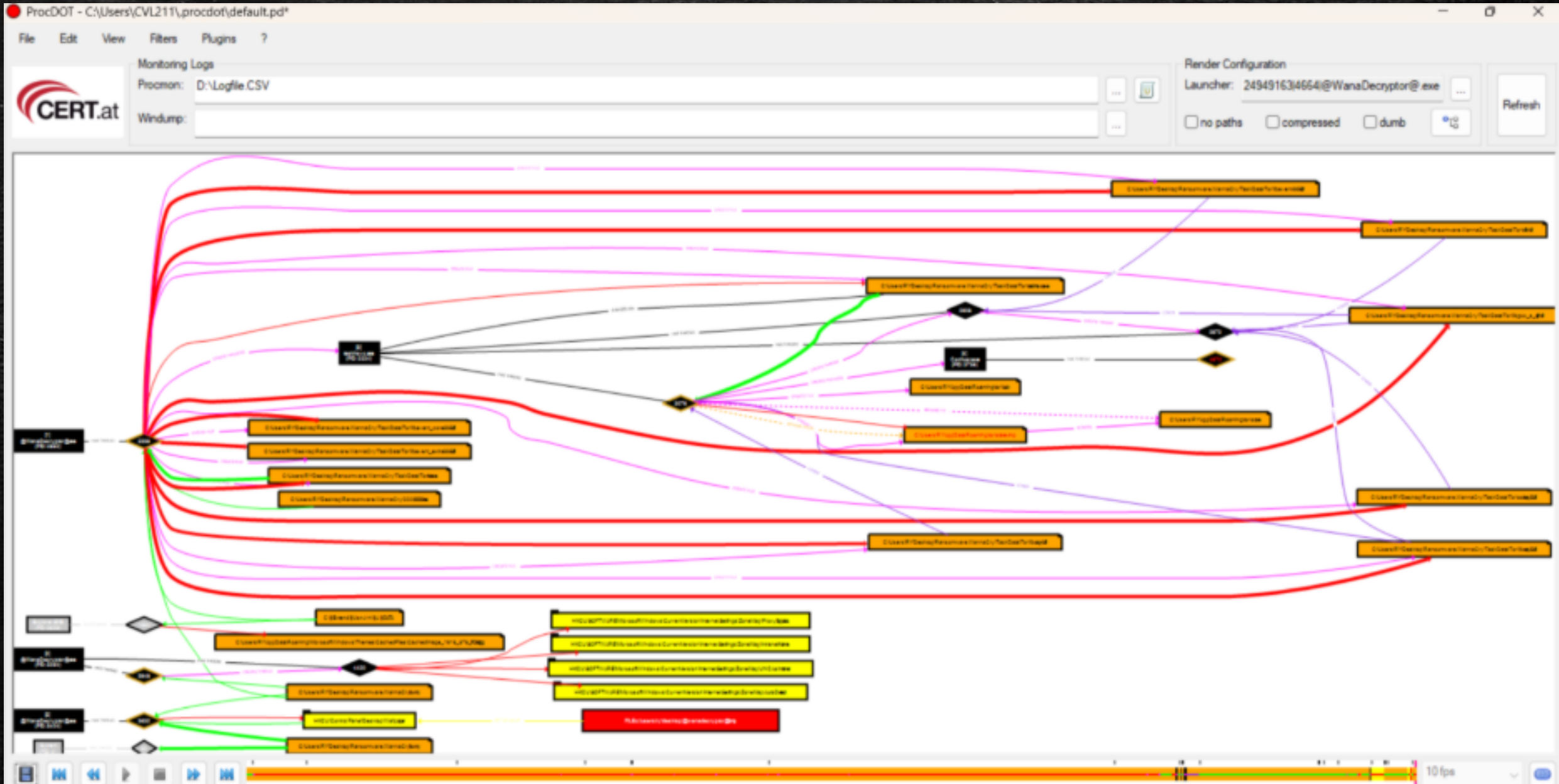
Apply a display filter ... <Ctrl-/>					
No.	Source	Destination	Protocol	Host	Info
9	192.168.56.102	107.206.174.46	TCP		49258 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	192.168.56.102	35.196.67.245	TCP		49268 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	192.168.56.102	147.24.136.160	TCP		49272 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
12	192.168.56.102	108.146.43.23	TCP		49283 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	192.168.56.102	185.134.87.160	TCP		49285 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	192.168.56.102	80.21.223.117	TCP		49294 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	192.168.56.102	98.231.218.217	TCP		49296 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	192.168.56.102	152.168.177.160	TCP		49300 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	192.168.56.102	216.2.44.92	TCP		49308 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
18	192.168.56.102	202.203.214.57	TCP		49311 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
19	192.168.56.102	156.70.196.181	TCP		49316 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
20	192.168.56.102	14.112.44.180	TCP		49322 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

Apply a display filter ... <Ctrl-/>					
> Frame 2: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0					
> Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: 02:00:00:00:00:00					
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.100.14					
> User Datagram Protocol, Src Port: 53, Dst Port: 49174					
> Domain Name System (response)					
No.	Source	Destination	Protocol	Host	Info
2434	192.168.100.14	2.16.106.21	TCP		49174 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2435	192.168.100.14	23.53.113.159	TCP		49173 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2436	192.168.100.14	2.16.106.21	TCP		49175 → 80 [RST, ACK] Seq=316 Ack=205 Win=0 Len=0
2437	192.168.100.14	104.97.14.192	TCP		49176 → 443 [RST, ACK] Seq=29897 Ack=37637 Win=0 Len=0
2438	192.168.100.14	104.97.14.192	TCP		49177 → 443 [RST, ACK] Seq=31560 Ack=139565 Win=0 Len=0
2439	192.168.100.14	2.23.77.188	TCP		49178 → 80 [RST, ACK] Seq=145 Ack=976 Win=0 Len=0
2440	192.168.100.14	151.101.38.172	TCP		49181 → 80 [RST, ACK] Seq=246 Ack=73649 Win=0 Len=0
2441	192.168.100.14	151.101.38.172	TCP		49180 → 80 [RST, ACK] Seq=246 Ack=73649 Win=0 Len=0
2442	192.168.100.14	2.23.77.188	TCP		49179 → 80 [RST, ACK] Seq=145 Ack=976 Win=0 Len=0
2443	192.168.100.14	104.97.14.192	TCP		49182 → 443 [RST, ACK] Seq=45894 Ack=48646 Win=0 Len=0
2444	192.168.100.14	20.190.160.132	TCP		49201 → 443 [RST, ACK] Seq=3322 Ack=11913 Win=0 Len=0
2445	192.168.100.14	104.97.14.192	TCP		49185 → 443 [RST, ACK] Seq=52410 Ack=304558 Win=0 Len=0
2446	192.168.100.14	2.16.106.200	TCP		49186 → 443 [RST, ACK] Seq=9626 Ack=36701 Win=0 Len=0
2447	192.168.100.14	2.16.106.200	TCP		49194 → 443 [RST, ACK] Seq=3170 Ack=5761 Win=0 Len=0
2448	192.168.100.14	2.16.106.200	TCP		49187 → 443 [RST, ACK] Seq=5734 Ack=11796 Win=0 Len=0
2449	192.168.100.14	2.16.106.200	TCP		49188 → 443 [RST, ACK] Seq=7067 Ack=13504 Win=0 Len=0
> Frame 563: 620 bytes on wire (4960 bits), 620 bytes captured (4960 bits) on interface 0					
> Ethernet II, Src: d4:da:6d:d6:67:03 (d4:da:6d:d6:67:03), Dst: 24:1d:78:22:91:78 (24:1d:78:22:91:78)					
> Internet Protocol Version 4, Src: 151.101.38.172, Dst: 192.168.100.14					
> Transmission Control Protocol, Src Port: 80, Dst Port: 49181, Seq: 64175, Ack: 246, Len: 566					
> Hypertext Transfer Protocol					

Procdot Diagram Video



ProcDot Diagram



Any.Run

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?
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. 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 Bitcoin. For more information, click <How to buy Bitcoin>. And send the correct amount to the address specified in this window. After your payment, click <Send Payment>. Best time to send: 9:00am - 11:00pm UTC.

Payment will be raised on
9/30/2025 20:51:40
Time Left
02:23:57:25

Your files will be lost on
10/3/2025 20:51:40
Time Left
06:23:57:25

Send \$300 worth of bitcoin to this address:
128YDFgus2BHyMgnd1Hy7AMh45SMw

Bitcoin
ACCEPTED HERE

Check Payment **Decrypt**

Warning [2780] taskl.exe Starts a Microsoft application from unusual location

Ransomware.WannaCry.zip
MD5: EF75BF09D8A2C584D2BC17309B5CF0
Start: 27/09/2023, 16:43
[win7.exe] [wannacry] [ransomware] [kinder] [update]

09:42 **Add time** **Stop**

Tracker: Ransomware, Stealer, WannaCry
CPU 1% **RAM 24%**

Processes 53 **Actions 7** **beta**

Filter by PID or name **Only important**

PID	Process name	Size	Private	Working Set	Page Faults	Page Faults/sec	Page Faults/min	Page Faults/hour	Page Faults/day	Page Faults/week	Page Faults/month	Page Faults/year
2720	WinRAR.exe	C:\Users\admin\Desktop\Ransomware.WannaCry.zip	1k	2k	0	0	0	0	0	0	0	0
3048	ed01ebfbc9eb3bba545af4d01b5f071661840480439c65babe060e41aa.exe	PE	DMP	86k	180	0	0	0	0	0	0	0
3548	attrib.exe	-rb	72	12	0	0	0	0	0	0	0	0

Process details ID 716 No verdict

taskl.exe
6.1.7600.16385 (win7_rtm.090713-1355)
SQL Client Configuration Utility EXE
Username: admin
Start: +431800ms
Command line
taskl.exe
More Info
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	ieexplore.exe	US	http://go.microsoft.com/fwlink/?LinkId...	-					
226.22 s	GET 301: Moved Per...	✓	2300	ieexplore.exe	DE	http://shell.windows.com/fileassoc/file...	-					
227.15 s	GET 200: OK	✓	2300	ieexplore.exe	DE	http://cacerts.digicert.com/DigiCertGlo...	579 b ↓ binary					
227.19 s	GET 200: OK	✓	2300	ieexplore.exe	DE	http://cacerts.digicert.com/DigiCertGlo...	579 b ↓ binary					
227.19 s	GET 200: OK	✓	2300	ieexplore.exe	DE	http://ctdl.windowsupdate.com/msdo...	71 Kb ↓ compres					
227.20 s	GET 200: OK	✓	2300	ieexplore.exe	DE	http://ctdl.windowsupdate.com/msdo...	71 Kb ↓ compres					
319.79 s	GET 302: Found	✓	688	ieexplore.exe	US	http://go.microsoft.com/fwlink/?LinkId...	-					

Network connections

HTTP Requests 6		Connections 39		DNS Requests 16		Threats 1		Filter by PID, domain, name or ip			
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic	
27991 ms	TCP	✓	1200	SIHClient.exe	🇺🇸	74.178.76.128	443	slscr.update...	MICROSOFT-CO...	↑ 751 b	↓
28989 ms	TCP	✓	1260	SIHClient.exe	🇺🇸	20.242.39.171	443	fe3cr.delivery...	MICROSOFT-CO...	↑ 602 b	↓
29993 ms	TCP	✓	1260	SIHClient.exe	🇺🇸	74.178.76.128	443	slscr.update...	MICROSOFT-CO...	↑ 584 b	↓
30992 ms	TCP	✓	1260	SIHClient.exe	🇺🇸	74.178.76.128	443	slscr.update...	MICROSOFT-CO...	↑ 751 b	↓
41295 ms	TCP	✓	5224	SearchApp.exe	🇺🇸	23.43.168.221	443	www.bing.com	AKAMAI-AS	↑ 197 b	↓
53501 ms	TCP	✓	7920	slui.exe	🇺🇸	4.154.185.43	443	activation-v2...	MICROSOFT-CO...	↑ 309 b	↓
112.95 s	TCP	✓	7716	slui.exe	🇺🇸	4.154.185.43	443	activation-v2...	MICROSOFT-CO...	↑ 291 b	↓
120.06 s	TCP	✓	3464	svchost.exe	🇺🇸	4.207.247.139	443	client.wns.wi...	MICROSOFT-CO...	↑ 2 Kb	↓

HTTP Requests 6		Connections 39		DNS Requests 16		Threats 1		Filter by PID, domain, name or ip			
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic	
BEFORE	UDP	✓	4	System	?	192.168.100.255	137	-	-	↑ 2 Kb	↓
BEFORE	TCP	✓	6016	MoUsocoreWorker.exe	🇮🇹	51.104.136.2	443	settings-win....	MICROSOFT-CO...	Waiting for the Dat	
BEFORE	TCP	✓	7160	RUXIMICS.exe	🇮🇹	51.104.136.2	443	settings-win....	MICROSOFT-CO...	Waiting for the Dat	
2390 ms	UDP	✓	4	System	?	192.168.100.255	138	-	-	↑ 3 Kb	↓
10519 ms	TCP	✓	5224	SearchApp.exe	🇺🇸	23.43.168.221	443	www.bing.com	AKAMAI-AS	↑ 3 Kb	↓ 11
10539 ms	TCP	✓	5224	SearchApp.exe	🇺🇸	23.43.168.221	443	www.bing.com	AKAMAI-AS	↑ 6 Kb	↓
11616 ms	TCP	✓	6940	svchost.exe	🇺🇸	40.126.24.82	443	login.live.com	MICROSOFT-CO...	↑ 11 Kb	↓ 2
11623 ms	TCP	✓	6040	svchost.exe	🇺🇸	40.126.24.82	443	login.live.com	MICROSOFT-CO...	↑ 11 Kb	↓ 2

DNS Request and Threats

HTTP Requests	6	Connections	39	DNS Requests	16	Threats	1	Filter by IP or domain
Timeshift	Status	Rep	Domain	IP				
BEFORE	Responded	✓	settings-win.data.microsoft.com	51.104.136.2				
BEFORE	Responded	✓	google.com	142.250.74.46				
10507 ms	Responded	✓	www.bing.com	23.43.168.221				
10508 ms	Responded	✓	login.live.com	40.126.24.82				
11610 ms	Responded	✓	ocsp.digicert.com	184.28.9.100				
12620 ms	Responded	✓	th.bing.com	23.43.168.198				
12621 ms	Responded	✓	client.wns.windows.com	4.207.247.139				
13653 ms	Responded	✓	are men com	20.100.58.43				

HTTP Requests	6	Connections	39	DNS Requests	17	Threats	1	Filter by message
Timeshift	Class	PID	Process name	Message				
19483 ms	Unknown Traffic	-	-	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)				

[2240] @WanaDecryptor@.exe C:\Users\admin\Desktop\@WanaDecryptor@.exe

Main Information

- Code signing: 1
- Process dump: 1
- Events: 1
- Modified files: 10
- Registry changes: 0
- Synchronization: 0
- HTTP requests: 0
- Connections: 0
- Network flows: 0
- Modules: 36
- Setting: 0

Threat Verdict

100
OUT OF 100

Malicious

The score is an approximate value calculated by AI/ML algorithm based on process and user actions

Subscore: 100%

Process Information

Company: admin
MD: 6151521-08677624-42884629-82287-882-1080
SL: MEDIUM
Start: 466.24 s

File Information

Company: Microsoft Corporation
Description: Load-Package-Quarantine
Version: 5.1.7628.12185 (win7_x64-086713-12185)

Command line

WanaDecryptor@.exe

Timeline of the process

0 s: 466.24 s

Danger 4

- WanaDecryptor has been detected (VMB)
- 1368A381 Registry Run Keys / Startup Folder (C)
- WanaDecryptor has been detected
- 1368A381 Local Data Storage (C)
- WanaDecryptor has been detected

Warning and Stop

Warning 2

- Executable content was dropped or overwritten
- Starts a Microsoft application from unusual location

Other 3

- The sample compiled with english language support
- 13682 Query Registry (C)
- Checks supported languages

[3048] ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6

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\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe0e08de41aa.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 data

T1518 Software Discovery (1)
Actions looks like stealing of personal data

WANNACRY has been detected (YARA)

T1176 Software Extensions (1)
Modifies files in the Chrome extension folder

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

Processes 69	Actions 12	beta
Search		Hide all
C:\Users\admin\Desktop\s.wnry		
✔ Launching a file from an archive		
File: zlib1.dll		
Tor/zlib1.dll		
✔ Launching a file from an archive		
File: libevent-2-0-5.dll		
Tor/libevent-2-0-5.dll		
✔ Launching a file from an archive		
File: ssleay32.dll		
Tor/ssleay32.dll		
✔ Launching a file from an archive		
File: libevent_core-2-0-5.dll		
Tor/libevent_core-2-0-5.dll		
✔ Launching a file from an archive		
File: libssp-0.dll		
Tor/libssp-0.dll		

▼ Approved

✔ Extracting a file from an archive

File: Ransomware.WannaCry.zip to C:\Users\admin\Desktop\

Ransomware.WannaCry.zip

✔ Launching a file from an archive

File: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

✔ Launching a file from the Downloads directory

File: C:\Users\admin\Downloads\@Please_Read_Me@.txt

✔ Launching a file from the Downloads directory

File: C:\Users\admin\Downloads\@WanaDecryptor@.exe

✔ Extracting a file from an archive

File: C:\Users\admin\Desktop\s.wnry to C:\Users\admin\Desktop\

C:\Users\admin\Desktop\s.wnry

MITRE ATT&CK Matrix: WannaCryBehavior Overview

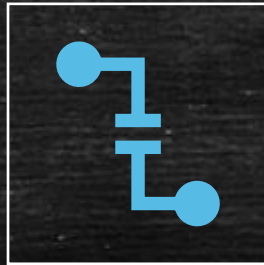
MITRE ATT&CK Matrix											
Tactics 9 Techniques 18 Events 160			Enterprise & Mobile tactics ▾ • Danger (40) • Warning (17) • Other (103)								
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	C & C	Exfiltration	Impact
Phishing (1/4) Spearphishing Attachment 1	Command and Scripting Interpreter (2/12) 4 Visual Basic 1 User Execution (1/4) Malicious File 5	Modify Registry 1 Office Application Startup (0/6) 1 Software Extensions (0/2) 10 Boot or Logon Autostart Execution (1/14) Registry Run Keys / Startup Folder 3	Boot or Logon Autostart Execution (1/14) Registry Run Keys / Startup Folder 3	Masquerading (1/11) Rename Legitimate Utilities 8 Modify Registry 1 File and Directory Permissions Modification (1/2) Windows File and Directory Permissions Modification 2 Hide Artifacts (1/14) Hidden Files and Directories 1	Unsecured Credentials (1/8) Credentials In Files 10	Query Registry 68 System Information Discovery 30 Software Discovery (0/1) 10		Data Staged (1/2) Local Data Staging 2			Data Encrypted for Impact 3

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
