WannaCry 2.0 | Malware Analysis

Talal Ahmed | Team Lambda

Sample Hash (SHA-256): ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

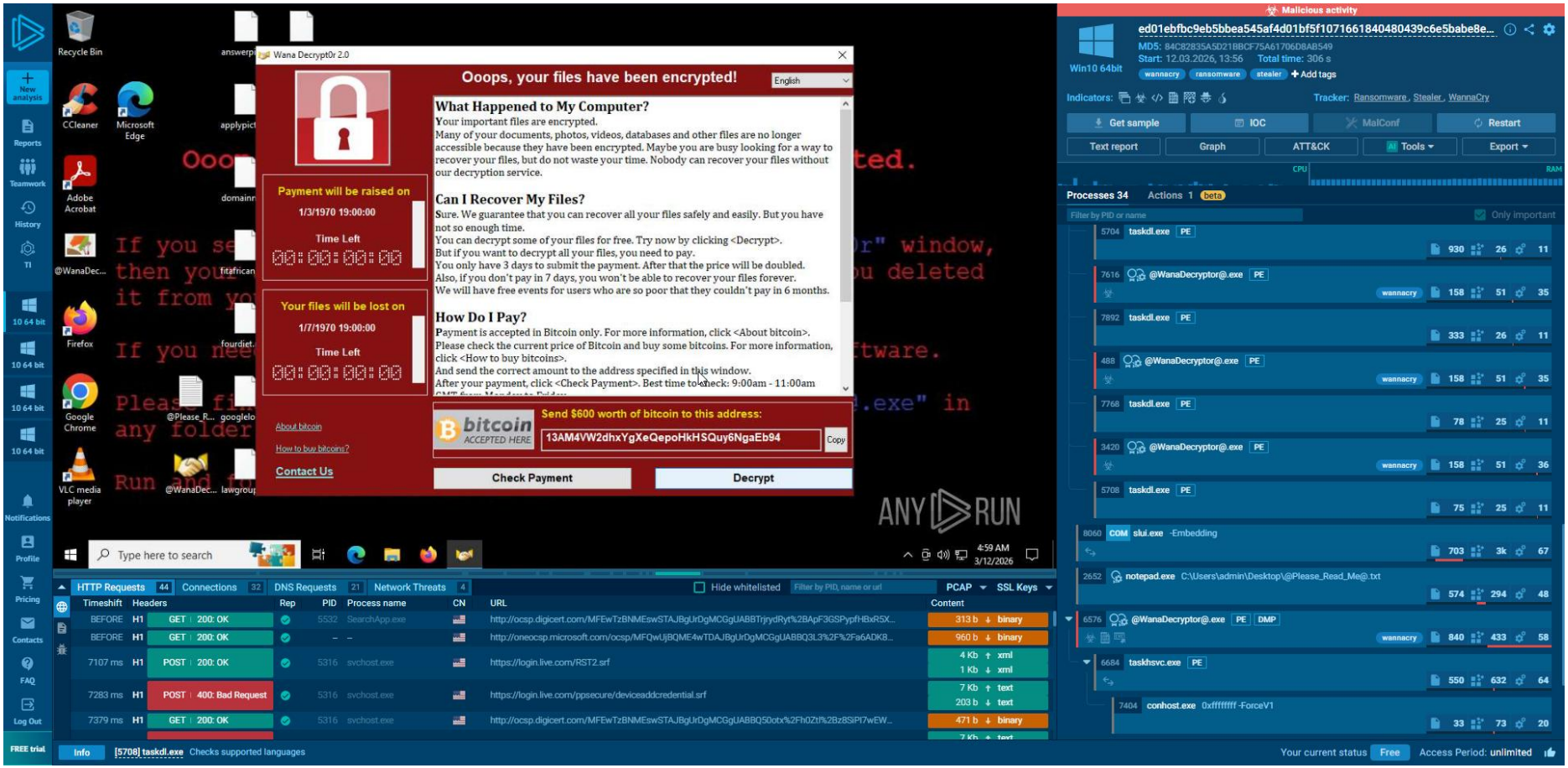
Malware Downloaded from: GitHub | **Password:** infected

Target OS: Windows 10 Professional (build: 19044, 64-bit)

1. Environment Setup & Methodology

To satisfy the safety requirements of the "Digital Bunker", the following isolated environment was established:

- **Virtualization:** A guest Windows 10 VM was deployed within an isolated VirtualBox environment, configured with a **Host-Only adapter** to prevent lateral movement to the physical host or external network.
- **Analysis Style:** An interactive "Live" approach was used via **ANY.RUN**, allowing for manual triggering of ransomware components (e.g., clicking the decryptor GUI) to observe secondary payloads.
- **Baseline Management:** A clean snapshot was taken prior to execution. **Regshot** was utilized to capture the initial system state for post-infection comparison.



2. Tools Employed

The analysis utilized a tiered toolkit to capture data at different layers of the OS:

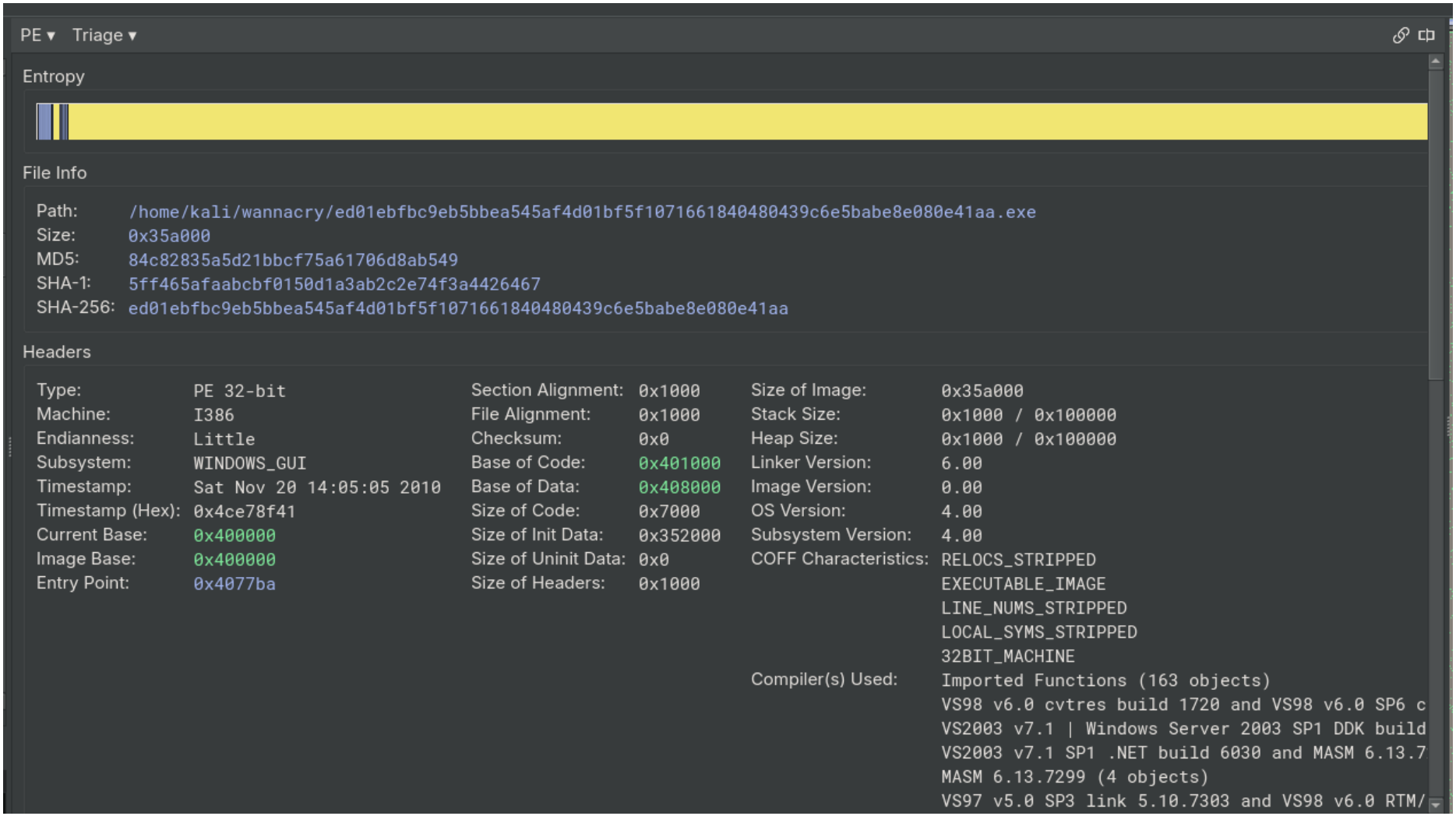
- **Binary Ninja:** Used for static disassembly to identify hardcoded strings, cryptographic constants, and the Import Address Table (IAT).

- **Process Monitor (ProcMon) via AnyRun:** Captured high-frequency system calls, identifying the exact millisecond the malware modified file permissions.
- **Process Explorer via AnyRun:** Monitored the process tree in real-time to identify "Orphan" processes spawned by the ransomware.
- **FakeNet-NG via AnyRun:** Intercepted DNS and HTTP requests, simulating a live internet connection to trick the malware into revealing its C2 architecture.

3. Detailed Static Analysis

Static analysis focused on the binary's potential capabilities without risking system infection.

- **File Metadata:**
  - **Timestamp:** 2010-11-20 09:05:05 (Indicating a forged or legacy timestamp commonly used in the 2017 WannaCry variant).
  - **Entropy:** High entropy sections were identified, suggesting a packed payload designed to evade signature-based AV.



- **Cryptographic Indicators:** The binary imports CryptGenKey, CryptDecrypt, and CryptEncrypt from the **Microsoft Enhanced RSA and AES Cryptographic Provider**, confirming its role as a high-grade encryption tool.

- **Embedded Command Strings:** Hardcoded strings reveal a "preparation phase" where the malware seizes control of the system:
  - icacls . /grant Everyone:F /T /C /Q: Recursively grants full permissions to all files in the current directory.
  - attrib +h .: Sets the "Hidden" attribute to conceal malicious components from the user.
- **Mutex Discovery:** The string Global\\MsWinZonesCacheCounterMutexA was found, which the malware uses as an infection marker to prevent re-infecting the same host.

PE ▾ Strings ▾

Search strings

```
0040eef5 ASCII )a95
0040ef08 ASCII yeFz
0040ef39 ASCII 2/O-_.X8w.+
0040ef87 ASCII |~}%.15
0040efac ASCII \trY[
0040efbe ASCII nb53
0040f005 ASCII ]4lL
0040f048 ASCII s0|8
0040f08c ASCII Microsoft Enhanced RSA and AES Cryptographic Provider
0040f0c4 ASCII CryptGenKey
0040f0d0 ASCII CryptDecrypt
0040f0e0 ASCII CryptEncrypt
0040f0f0 ASCII CryptDestroyKey
0040f100 ASCII CryptImportKey
0040f110 ASCII CryptAcquireContextA
0040f3f8 UTF-16 %s\\Intel
0040f40c UTF-16 %s\\ProgramData
0040f42c ASCII cmd.exe /c \"%s\"
0040f440 ASCII 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
0040f464 ASCII 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
0040f488 ASCII 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
0040f4ac ASCII %s%d
0040f4b4 ASCII Global\\MsWinZonesCacheCounterMutexA
0040f4d8 ASCII tasksche.exe
0040f4e8 ASCII TaskStart
0040f4f4 ASCII t.wnry
0040f4fc ASCII icacls . /grant Everyone:F /T /C /Q
0040f520 ASCII attrib +h .
0040f52c ASCII WNcry@2ol7
```

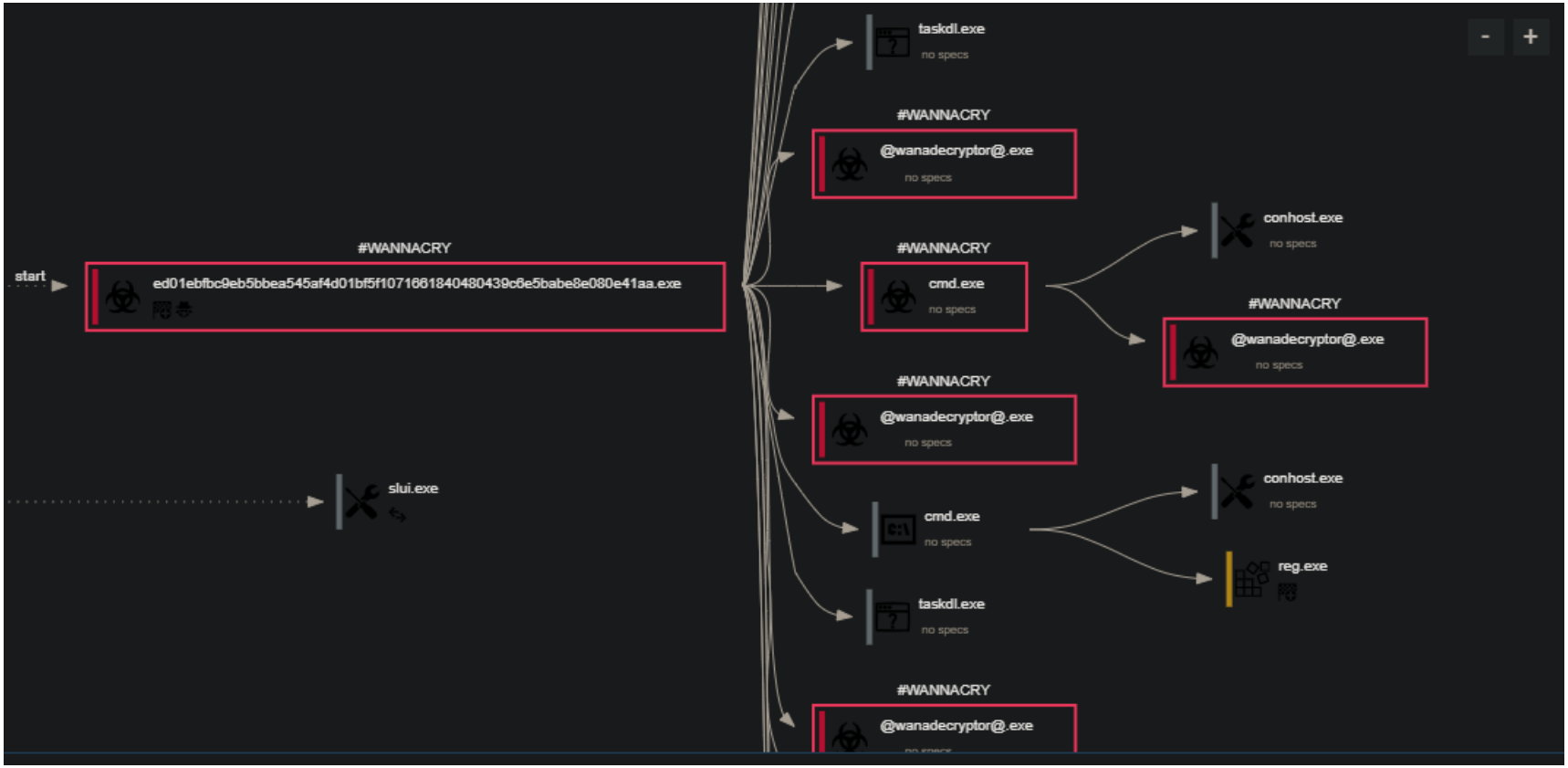
PE ▾ Strings ▾

Search strings

```
007595d5 ASCII t.wnry\n
007595e7 ASCII *($:{
0075962d ASCII taskdl.exe\n
00759689 ASCII taskse.exe\n
007596c9 ASCII lN$D
007596e5 ASCII u.wnry\n
0075972e UTF-16 VS_VERSION_INFO
0075978a UTF-16 StringFileInfo
007597ae UTF-16 040904B0
007597c6 UTF-16 CompanyName
007597e0 UTF-16 Microsoft Corporation
00759812 UTF-16 FileDescription
00759834 UTF-16 DiskPart
0075984e UTF-16 FileVersion
00759868 UTF-16 6.1.7601.17514 (win7sp1_rtm.101119-1850)
007598c2 UTF-16 InternalName
007598dc UTF-16 diskpart.exe
007598fe UTF-16 LegalCopyright
0075991e UTF-16  Microsoft Corporation. All rights reserved.
0075997e UTF-16 OriginalFilename
007599a0 UTF-16 diskpart.exe
007599c2 UTF-16 ProductName
007599dc UTF-16 Microsoft
007599f0 UTF-16  Windows
00759a02 UTF-16  Operating System
00759a2e UTF-16 ProductVersion
00759a4c UTF-16 6.1.7601.17514
00759a72 UTF-16 VarFileInfo
00759a92 UTF-16 Translation
```

4. Detailed Dynamic Analysis

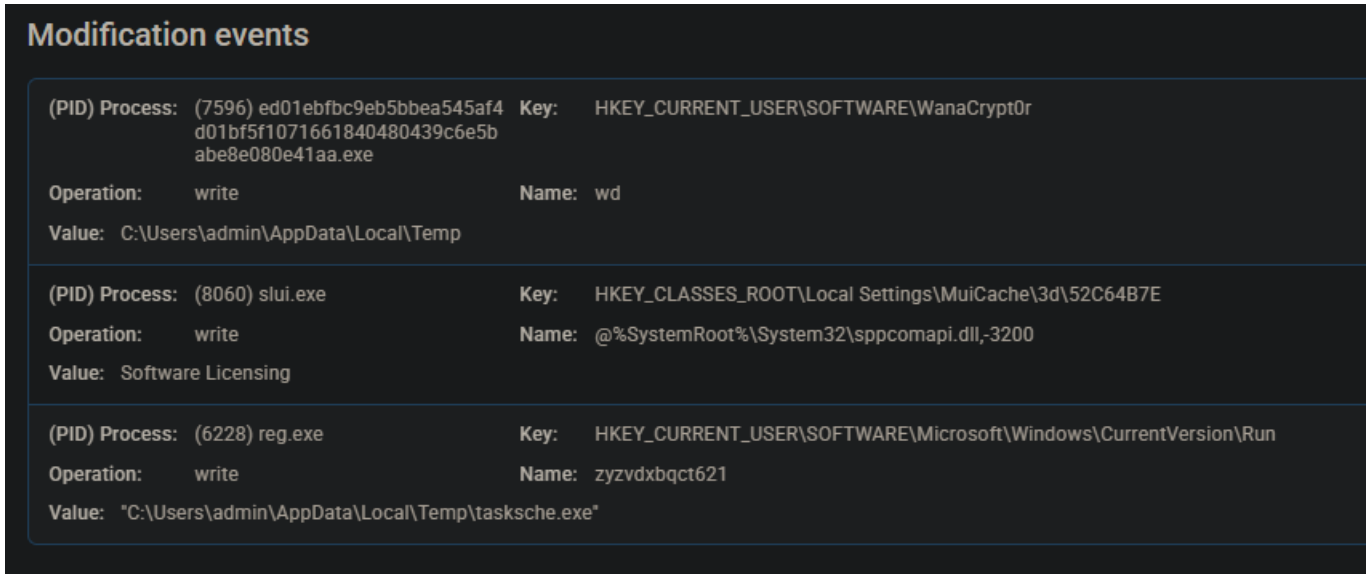
The dynamic phase observed the malware "in action" within the ANY.RUN sandbox.



- **Process Chain (Execution Flow):**
    1. **Main Payload:** ed01eb...exe (PID: 7596) initiates the infection.
    2. **Command Execution:** It spawns cmd.exe (PID: 4564) to run hidden batch scripts.

3. **Payload Extraction:** Multiple instances of @WanaDecryptor@.exe (PIDs: 6576, 2692, 6064) are launched to perform the actual file encryption.
4. **Self-Cleanup:** taskdl.exe (PID: 3340) is used to delete temporary files and "cleanup" the infection footprints.

- **Registry and Persistence:**
  - The malware utilized reg.exe (PID: 6228) to modify the **Autorun** values, ensuring the ransom note and encryption engine launch on every system reboot.

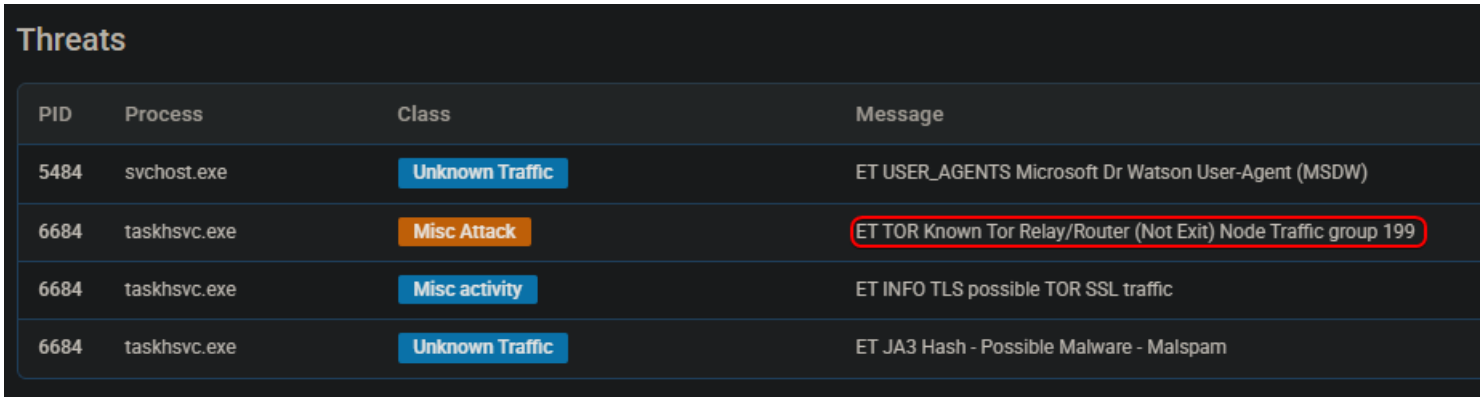


- **File System Impact:**
  - **Targeted Directories:** Malicious files were written to the **Word startup folder** and **Chrome extension folder** to maintain persistence and potentially intercept browser data.
  - **Encryption Activity:** The system's **temporary directory** was used as a staging area for .wnry components.

Dropped files

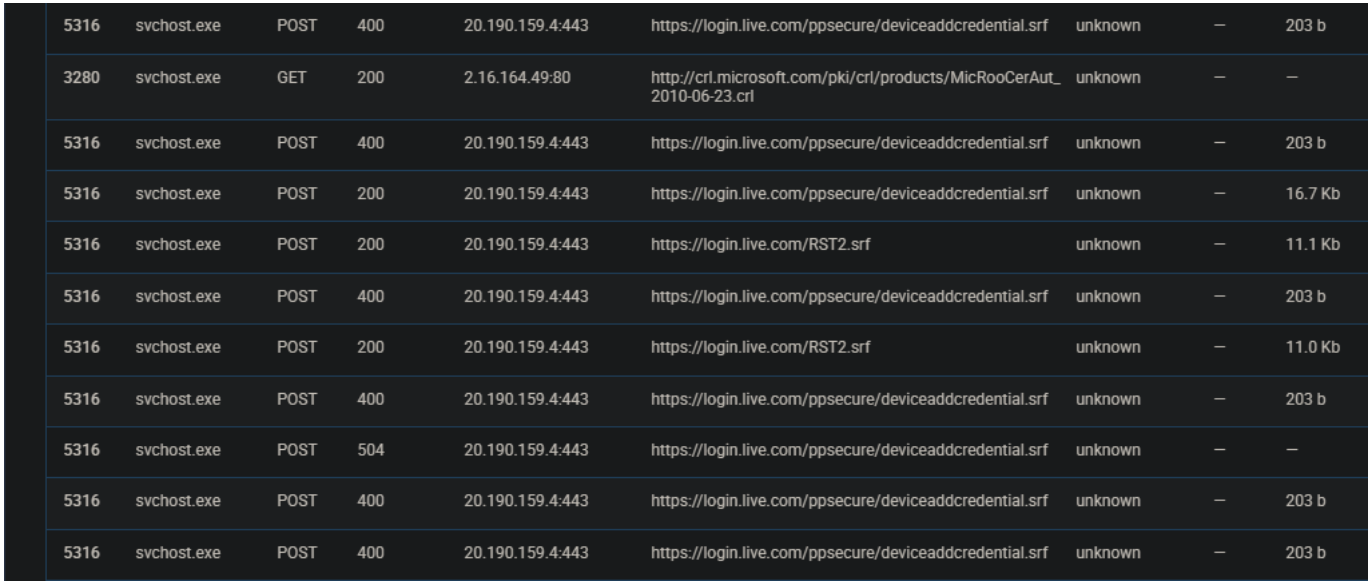
PID	Process	Filename	Type
7596	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	C:\Users\admin\AppData\Local\Temp\b.wnry	–
		MD5: C17170262312F3BE7027BC2CA825BF0C SHA256: D5E0E8694DDC0548D8E6B87C83D50F4AB85C1DEBADB106D6A6A794C3E746F4FA	
7596	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	C:\Users\admin\AppData\Local\Temp\c.wnry	–
		MD5: AE08F79A0D800B82FCBE1B43CDBDBEFC SHA256: 055C7760512C98C8D51E4427227FE2A7EA3B34EE63178FE78631FA8AA6D15622	
7596	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	C:\Users\admin\AppData\Local\Temp\msg\m_dutch.wnry	–
		MD5: 7A8D499407C6A647C03C4471A67EAAD7 SHA256: 2C95BEF914DA6C50D7BDEDEC601E589FBB4FDA24C4863A7260F4F72BD025799C	
7596	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	C:\Users\admin\AppData\Local\Temp\msg\m_bulgarian.wnry	–
		MD5: 95673B0F968C0F55B32204361940D184 SHA256: 40B37E7B80CF678D7DD302AAF41B88135ADE6DDF44D89BDBA19CF171564444BD	
7596	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	C:\Users\admin\AppData\Local\Temp\msg\m_croatian.wnry	–
		MD5: 17194003FA70CE477326CE2F6DEEB270 SHA256: 3F33734B2D34CCE83936CE99C3494CD845F1D2C02D7F6DA31D42DFC1CA15A171	
7596	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	C:\Users\admin\AppData\Local\Temp\msg\m_french.wnry	–
		MD5: 4E57113A6BF6B88FDD32782A4A381274 SHA256: 9BD38110E6523547AED50617DDC77D0920D408FAEED2B7A21AB163FDA22177BC	
7596	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	C:\Users\admin\AppData\Local\Temp\msg\m_chinese (simplified).wnry	–
		MD5: 0252D45CA21C8E43C9742285C48E91AD SHA256: 845D0E178AEEBD6C7E2A2E9697B2BF6CF02028C50C288B3BA88FE2918EA2834A	
7596	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	C:\Users\admin\AppData\Local\Temp\msg\m_danish.wnry	–
		MD5: 2C5A3B81D5C4715B7BEA01033367FCB5 SHA256: A75BB44284B9DB8D702692F84909A7E23F21141866ADF3DB888042E9109A1CB6	
7596	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	C:\Users\admin\AppData\Local\Temp\msg\m_chinese (traditional).wnry	–

- **Network Forensics:**
    - The analysis detected significant indicators of **Tor** usage, intended to anonymize the location of the Command & Control (C2) servers.



Threats

PID	Process	Class	Message
5484	svchost.exe	Unknown Traffic	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)
6684	taskhsvc.exe	Misc Attack	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 199
6684	taskhsvc.exe	Misc activity	ET INFO TLS possible TOR SSL traffic
6684	taskhsvc.exe	Unknown Traffic	ET JA3 Hash - Possible Malware - Malspam



5316	svchost.exe	POST	400	20.190.159.4:443	https://login.live.com/ppsecure/deviceaddcredential.srf	unknown	–	203 b
3280	svchost.exe	GET	200	2.16.164.49:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	–	–
5316	svchost.exe	POST	400	20.190.159.4:443	https://login.live.com/ppsecure/deviceaddcredential.srf	unknown	–	203 b
5316	svchost.exe	POST	200	20.190.159.4:443	https://login.live.com/ppsecure/deviceaddcredential.srf	unknown	–	16.7 Kb
5316	svchost.exe	POST	200	20.190.159.4:443	https://login.live.com/RST2.srf	unknown	–	11.1 Kb
5316	svchost.exe	POST	400	20.190.159.4:443	https://login.live.com/ppsecure/deviceaddcredential.srf	unknown	–	203 b
5316	svchost.exe	POST	200	20.190.159.4:443	https://login.live.com/RST2.srf	unknown	–	11.0 Kb
5316	svchost.exe	POST	400	20.190.159.4:443	https://login.live.com/ppsecure/deviceaddcredential.srf	unknown	–	203 b
5316	svchost.exe	POST	504	20.190.159.4:443	https://login.live.com/ppsecure/deviceaddcredential.srf	unknown	–	–
5316	svchost.exe	POST	400	20.190.159.4:443	https://login.live.com/ppsecure/deviceaddcredential.srf	unknown	–	203 b
5316	svchost.exe	POST	400	20.190.159.4:443	https://login.live.com/ppsecure/deviceaddcredential.srf	unknown	–	203 b

1456	icacls . /grant Everyone:F /T /C /Q	C:\Windows\SysWOW64\icacls.exe	–	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

Information

User: admin
Company: Microsoft Corporation
Integrity Level: MEDIUM
Exit code: 0
Version: 10.0.19041.1 (WinBuild.160101.0800)

Modules

Images

c:\windows\syswow64\icacls.exe
c:\windows\system32\ntdll.dll
c:\windows\syswow64\ntdll.dll
c:\windows\system32\wow64.dll
c:\windows\system32\wow64win.dll
c:\windows\system32\wow64cpu.dll
c:\windows\syswow64\kernel32.dll
c:\windows\syswow64\kernelbase.dll
c:\windows\syswow64\apphelp.dll
c:\windows\syswow64\msvcrt.dll

Previous 1 2 Next

5. Hybrid Analysis Correlation

The hybrid approach validates static theories with dynamic evidence:

Static Finding (Code)	Dynamic Observation (Behavior)	Conclusion
icacls string in binary	Process 7596 calls icacls.exe	Malware grants itself full system rights.
CryptEncrypt API imports	Mass creation of .wnry files	Confirmed automated ransomware engine.
tasksche.exe string	Persistence keys added to Registry	High-level persistence mechanism confirmed.

---

6. Incident Response (IR) Plan

Phase 1: Detection

- **SIEM Alert:** Configure alerts for any process spawning icacls with the /grant Everyone:F flag.
- **Endpoint Detection:** Monitor for the creation of files with the .wnry extension.

Phase 2: Containment

- **Network Isolation:** Immediately disconnect the infected host from the VLAN to prevent the "EternalBlue" exploit from spreading laterally.
- **Protocol Block:** Disable **SMBv1** network-wide, as this is the primary propagation vector for this malware family.

Phase 3: Eradication

- **Process Termination:** Kill all active PIDs associated with @WanaDecryptor@.exe and tasksche.exe.

- **Registry Cleanup:** Delete keys from ...\CurrentVersion\Run that point to the ransomware directory.
- **File Wipe:** Securely delete all files in the C:\Users\[User]\AppData\Local\Temp directory used for staging.

Phase 4: Recovery

- **Restoration:** Re-image the infected machine from a clean Windows 10 build.
- **Data Retrieval:** Restore user data from **offline, air-gapped backups**. Do not attempt to use the built-in decryptor, as paying the ransom does not guarantee the recovery key.


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
1/3/1970 19:00:00
Time Left
00:00:00:00
Your files will be lost on
1/7/1970 19:00:00
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
Send $600 worth of bitcoin to this address:
bitcoin ACCEPTED HERE
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Copy
Check Payment
Decrypt
Recycle Bin
CCleaner
Microsoft Edge
Adobe Acrobat
@WanaDec...
Firefox
Google Chrome
VLC media player
@Please_R...
@WanaDec...
ANY RUN
Type here to search
5:01 AM
3/12/2026