McAfee Labs Threat Advisory

Ransom-WannaCry

June 22, 2018

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL**:** https://sns.secure.mcafee.com/signup_login.

Summary

Ransomware-WannaCry is a detection for a family of ransomware that on execution encrypts certain file types present in the user's system. The compromised user must pay the attacker with a ransom to get the files decrypted.

McAfee products detect this threat under the following detection name:

- Ransom-WannaCry, Ransom-WNCry, Real Protect-EC, Real Protect-SC, Real Protect.gh, Real Protect.bx

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

Infection and Propagation Vectors

Even though this has not been confirmed, the malware's initial vector is expected to be Spam email. The malware spreads by exploiting shares and uses the EternalBlue (MS17-010 Echo Response - SMB vulnerability) vulnerability. The authors have utilized publicly available exploit code and embedded it as a part of their dropper. The malware, on execution, connects to the IPC$ tree and attempts a transaction on FID 0, triggers the vulnerability, and then exploits it.

During replication, we observed that it generates a random set of IP addresses for the purposes of propagation. These IPs are not restricted to internal IPs.

Affected systems: Microsoft Windows XP, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7, Windows 8.1, Windows RT 8.1, Windows Server 2012 and R2, Windows 10, Windows Server 2016

Characteristics and Symptoms

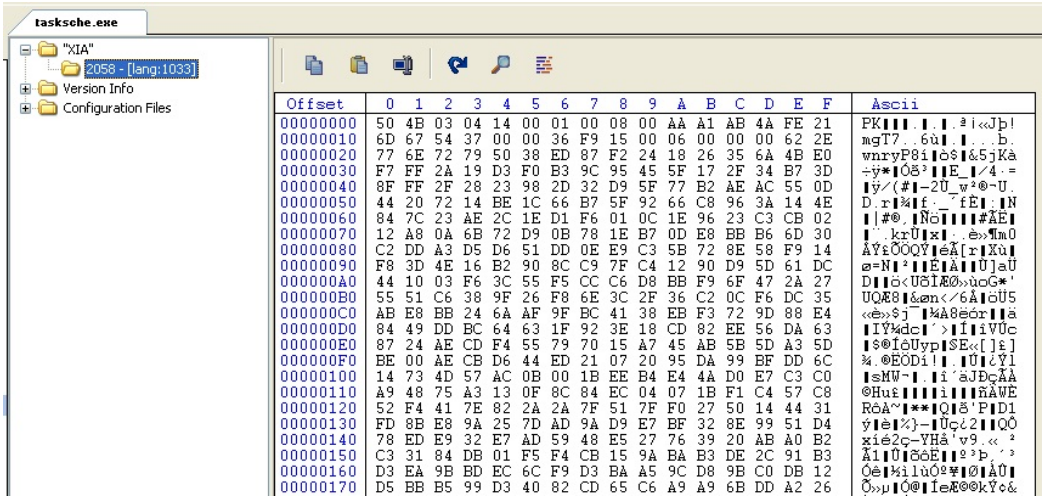
The following section describes various components of the malware. There is a main dropper and a sub dropper component. The main dropper contains the shell code needed for propagation and the sub dropper sets up the machine for encryption. The sub dropper is contained within the main dropper.

On execution, the main dropper checks for the following:

- http://www[dot]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[dot]com
- hxxp://www[dot]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[dot]com

If the domain is active, the malware simply quits without doing anything else. (For this purpose, the research community has sink holed this domain to prevent further malware infections.) It is thus recommended that your organization allow connectivity to this domain. In a few samples, we have observed that this domain connectivity check is absent; however in most samples that were seen on the May 12th 2017 attacks, samples attempted connecting to this domain.

The sub dropper contains multiple components in the form of a password-protected ZIP file in its Resource section. The password is hardcoded "WNcry@2ol7". The dropped components by this sub dropper are responsible for other activities on the system. The figure below shows an example ZIP.



The dropper installs itself as a service called MSSECSVC2.0 with description “Microsoft Security Service (2.0)” as a restart mechanism. Once the service is started, it generated its random list of IP addresses to target.

The dropper uses the command line below to remove any existing shadow volumes and backups:

Cmd /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet

The dropper component executes the following commands:

attrib +h .
icacls. /grant Everyone:F /T /C /Q
taskdl.exe
@WanaDecryptor@.exe fi
148131494626672.bat
@WanaDecryptor@.exe co
cmd.exe /c start /b @WanaDecryptor@.exe vs
taskse.exe C:\Users\[User]\AppData\Local\Temp\@WanaDecryptor@.exe
@WanaDecryptor@.exe
cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "vlyxsemjujkp530" /t REG_SZ /d "\"<Install Dir>\tasksche.exe\"" /f
cscript.exe //nologo m.vbs

The ransomware is granting full access to all files by using the command:

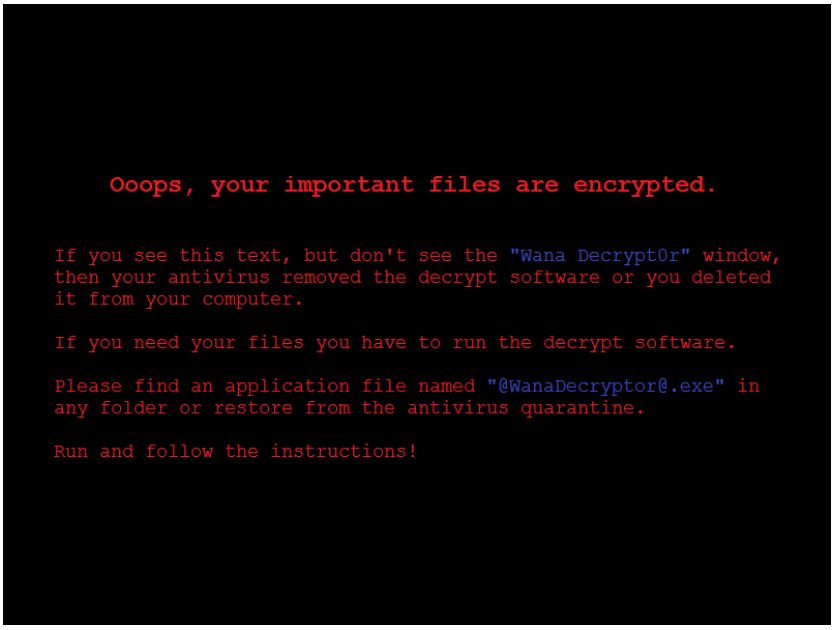
- icacls. /grant Everyone:F /T /C /Q

The various components dropped to disk are listed below:

- **taskdl.exe –** Initial cleaner component used before the actual encryption begins. Looks for file in the install dir of the ransomware and RecycleBin and removes any files with extensions ".WNCRYT"
- **taskse.exe –** Component that attempts to synchronize execution between machines. It waits for a signal and runs scripts concurrently. Use to connect to remove desktops by WTSEnumerateSessionsA, and create process.
- **b.wnry** – Contains the wallpaper that is displayed
- **c.wnry** – BitCoin Wallets, CNC, etc
- **r.wnry** – Ransomware note
- **m.wnry** – RTF containing the decryption instructions
- **s.wnry** – An archive that contains a TOR client, used for payments
- **t.wnry** – An encrypted file that contains the encryption routine used by malware for file encryption
- **u.wnry / @WannaDecryptor@.exe –** Encryptor/Decryptor component of the ransomware. Loads t.wnry and executes it in memory
- **m.vbs –** Used to create a shortcut to the decryptor on the desktop.
- **<Random_filename>.bat: -** BAT file that is used to create the .vbs file.
- **Msg Folder –** Contains language-specific decryption instructions

Once encryption is complete, the malware displays the following ransom message:

The following is the desktop wallpaper.



In the folder that contains the encrypted files, it also contains a text version of this message:

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

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

Q:  What do I do?

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

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

Q:  How can I trust?

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


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

Network Activity

We found that the main dropper malware generates random IP addresses, not limited to the local network. The following is an example propagation attempt.

DB349B97...	user-PC	54321	[redacted]	.192.203	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54318	[redacted]	.158.149	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54311	[redacted]	5.237	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54387	[redacted]	.113.121	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54310	[redacted]	35.2	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54309	[redacted]	.134.247	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54306	[redacted]	.0.241	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54305	[redacted]	5.215	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54483	[redacted]	.117.169	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54485	[redacted]	209.232	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54490	[redacted]	.7.193	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54491	[redacted]	33.170	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54492	[redacted]	2.205	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54494	[redacted]	.212.239	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54495	[redacted]	6.195	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54554	[redacted]	.82.21	445	TCP	SYN Sent	mssecsvc2.0
DB349B97...	user-PC	54533	[redacted]	.107.15	445	TCP	SYN Sent	mssecsvc2.0

This fact means the malware can spread not only to other machines in the same network, but also across the Internet if they allow NetBIOS packets from outside networks. This could be one reason for the widespread infection seen in this outbreak. This explains why many folks are unsure about the Initial vector of the malware.
Another interesting characteristic of the malware is that once a machine with an open NetBIOS port is found, the malware will send three NETBIOS session setup packets to it. One of them has the proper IP of the machine being exploited, and the other two contain two IP addresses hardcoded in the malware body:

```
SMB       185 Negotiate Protocol Response
SMB       157 Session Setup AndX Request, User: .\
SMB       175 Session Setup AndX Response
SMB       149 Tree Connect AndX Request, Path: \\192.168.0.1\IPC$
SMB       104 Tree Connect AndX Response
SMB Pip   132 PeekNamedPipe Request, FID: 0x0000
SMB        93 Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
```

The packet above contains the actual IP of the machine being exploited which uses the test network 192.168.0.0/24. The other two packets, as seen below, contain different IPs which the malware has in its code:

```
SMB      191 Negotiate Protocol Request
SMB      187 Negotiate Protocol Response
SMB      194 Session Setup AndX Request, User: anonymous
SMB      251 Session Setup AndX Response
SMB      150 Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
SMB      114 Tree Connect AndX Response
SMB      136 Trans2 Request, SESSION_SETUP
SMB       93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
```

```
SMB      191 Negotiate Protocol Request
SMB      187 Negotiate Protocol Response
SMB      194 Session Setup AndX Request, User: anonymous
SMB      251 Session Setup AndX Response
SMB      146 Tree Connect AndX Request, Path: \\172.16.99.5\IPC$
SMB      114 Tree Connect AndX Response
SMB     1138 NT Trans Request, <unknown>
SMB       93 NT Trans Response, <unknown (0)>
```

This activity and the presence of two hard-coded IP addresses, could be used to detect the exploit using Network Intrusion Prevention Systems.

After the above communication, the exploit has triggered and a sub dropper is transferred.

As explained prior, the sub dropper component is a 3.4-3.6MB file which contains several files in its resource section. One of these files is a Zip file containing the Tor Browser binaries. Tor browser is used to access the Onion URLs used by the malware to collect payments. The following Onion URLs are used:

- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- xxlvbrloxvriy2c5.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52maqm7.onion

The Payment is collected through Bitcoin. The following addresses are found in the samples

- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

The sub dropper infects files with specific extensions on the local machine, any removable drive connected to it, and any network share mounted locally.

It then attempts to find machines on the local network via NetBios broadcast messages and Master Browser queries. Once a machine is found, the malware connects to the IPC$ default share and attempts to log in. If it is successful, it tries to list all available shares and will attempt to infect them

It does so by copying itself to the remote share first, then encrypting all files with specific extensions it can find there.

Target File Types

.der .pfx .key .crt .csr .p12
.pem .odt .ott .sxw .stw .uot
.3ds .max .3dm .ods .ots .sxc
.stc .dif .slk .wb2 .odp .otp
.sxd .std .uop .odg .otg .sxm
.mml .lay .lay6 .asc .sqlite3
.sqlitedb .sql .accdb .mdb .db
.dbf .odb .frm .myd .myi .ibd .mdf .ldf
.sln .suo .cs .c .cpp .pas
.h .asm .js .cmd .bat .ps1
.vbs .vb .pl .dip .dch .sch
.brd .jsp .php .asp .rb .java
.jar .class .sh .mp3 .wav .swf

.fla .wmv .mpg .vob .mpeg .asf
.avi .mov .mp4 .3gp .mkv .3g2
.flv .wma .mid .m3u .m4u .djvu
.svg .ai .psd .nef .tiff .tif
.cgm .raw .gif .png .bmp .jpg
.jpeg .vcd .iso .backup .zip .rar
.7z .gz .tgz .tar .bak .tbk
.bz2 .PAQ .ARC .aes .gpg .vmx
.vmdk .vdi .sldm .sldx .sti .sxi
.602 .hwp .snt .onetoc2 .dwg .pdf
.wk1 .wks .123 .rtf .csv .txt
.vsdx .vsd .edb .eml .msg .ost
.pst .potm .potx .ppam .ppsx .ppsm
.pps .pot .pptm .pptx .ppt .xltm
.xltx .xlc .xlm .xlt .xlw .xlsb
.xlsm .xlsx .xls .dotx .dotm .dot
.docm .docb .docx .doc

Restart Mechanism

The ransomware done via the Run key in HKLM:

- cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "vlyxsemjujkp530" /t REG_SZ /d "\"<Install Dir>\tasksche.exe\"" /f

It also installs the service MSSECSVC2.0 under the following key:

- HTLM\SYSTEM\CurrentVersion\Services\mssecsvc2.0

Indicators of Compromise

Hashes

- DB349B97C37D22F5EA1D1841E3C89EB4 – Example main dropper
- 509C41EC97BB81B0567B059AA2F50FE8 – Example Sub dropper
- 9C514CAB458488A082070560C40D9DAB
- 4362E287CA45A4862B7FE9ECAF46E985
- 4FEF5E34143E646DBF9907C4374276F5
- B27F095F305CF940BA4E85F3CB848819
- 7BF2B57F2A205768755C07F238FB32CC
- 7F7CCAA16FB15EB1C7399D422F8363E8
- 8495400F199AC77853C53B5A3F278F3E
- 84C82835A5D21BBCF75A61706D8AB549
- 86721E64FFBD69AA6944B9672BCABB6D
- 9C7C7149387A1C79679A87DD1BA755BC
- 4DA1F312A214C07143ABEEAFB695D904
- D6114BA5F10AD67A4131AB72531F02DA
- F0D9FFEFA20CDADF5B47B96B7F8D1F60
- F107A717F76F4F910AE9CB4DC5290594

IP Addresses

- 212.51.134.123 :9001
- 5.199.142.236 : 9001
- 197.231.221.221:9001
- 128.31.0.39:9191
- 149.202.160.69:9001
- 46.101.166.19:9090
- 91.121.65.179:9001
- 2.3.69.209:9001
- 146.0.32.144:9001
- 50.7.161.218:9001

Mitigation

- Update patch MS17-010 (Microsoft guidance)
- Network Admins can check the presence of an attempted network infection by looking for two hardcoded IPs in packet requests: (192.168.56.20, 172.16.99.5)
- Ensure that your organization has not blocked access to the following domain:
  www[dot]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
  This domain has been sink holed. It was being used by the malware as a kill switch.
- Refer to the KB published by McAfee with more information on mitigation actions:
  https://kc.mcafee.com/corporate/index?page=content&id=KB89335
- Mitigating the threat at multiple levels like file, registry & URL could be achieved at various layers of McAfee products. Browse the product guidelines available here to mitigate the threats based on the behavior described below in the Characteristics and symptoms section.

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.