WannaCry Ransomware

HOW TRIPWIRE HELPS

WannaCry, also known as WannaCrypt, WanaCrypt0r 2.0 and Wanna Decryptor, is a piece of malware in the form of ransomware that targets Microsoft Windows operating systems. On Friday 12th May 2017, WannaCry was launched as a large cyber attack that infected approximately a quarter of a million computers in over 150 countries around the world in just one week.

WannaCry demanded ransom payments by the cryptocurrency, Bitcoin, and had support for 28 languages, indicating this malware was targeting a very large part of the global population. It has been described as being one of the largest cyber attacks in history.

Similar to most ransomware outbreaks, the attack will spread itself by users clicking on a loaded hyperlink solicited by phishing emails or drive-by advertisement. Once it has infected a Windows operating system, it uses an Server Message Block (SMB) exploit that was discovered by the US National Security Agency to spread through a local network, targeting systems that have not had the latest security patches applied.

CHRONOLOGY OF EVENTS

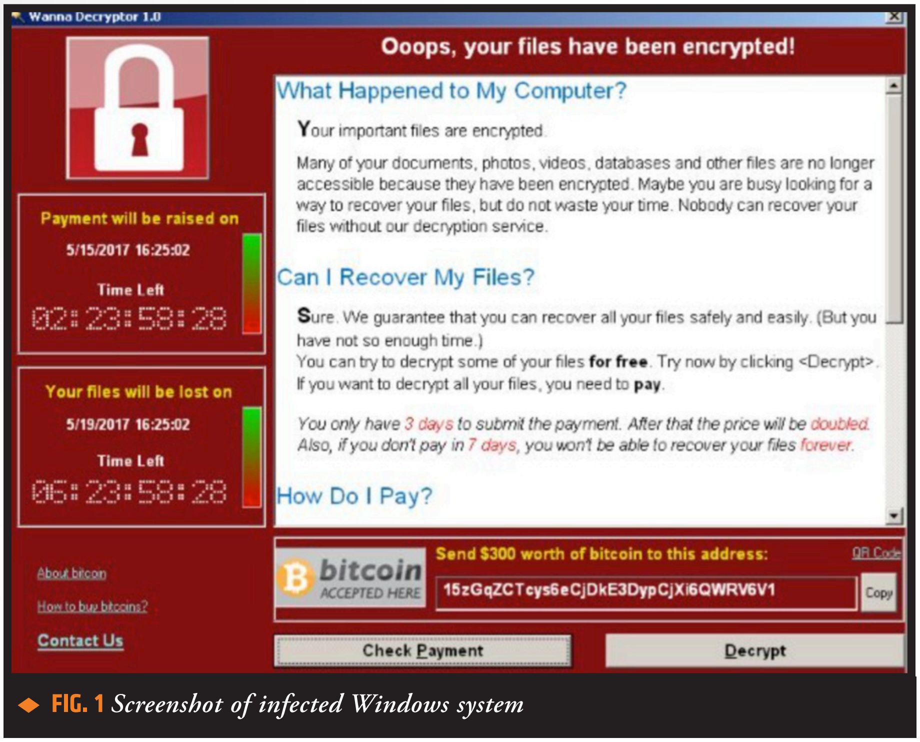
On January 16, 2017, US-CERT released an advisory on the SMB vulnerability.

On March 14, 2017, Microsoft released a critical patch to remove the underlying vulnerability for supported Windows Operating systems. Due to the significant impact of this cyber attack, Microsoft took an unusual step of releasing a security patch for out of support operating systems such as Windows XP and Windows 2003, as it was recognized that a lot of companies were still running out of support operating systems.

On April 14, 2017, the hacker group “Shadow Brokers” released EternalBlue exploit code to the world.

On May 12, 2017, WannaCry was launched, impacting business and large organizations globally.

Also on May 12, 2017, Marcus Hutchins, a security researcher, discovered the initial malware had a kill switch. By registering the domains identified in the malware, it temporarily halted the spread of the malware. However, new variants of the malware have been released without the kill switch.



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 try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
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.

How Do I Pay?

Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

Send $300 worth of bitcoin to this address:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

◆ FIG. 1 *Screenshot of infected Windows system*

OPERATION OF ATTACK

The WannaCry threat is composed of two main parts, a worm module and a ransomware module.

THE WORM MODULE

The worm module uses the Microsoft Windows Server Message Block (SMB) Server Remote Code Execution Vulnerability to spread, CVE-2017-0144. All versions of Microsoft Windows running SMBv1 are impacted. Malware that exploits SMB flaws could be extremely dangerous inside organization networks because the file sharing component may help the ransomware spread rapidly from one infected machine to another.

MS17-010 Security advisory details that patch needs to be applied to repair the vulnerability. This patch was released on the March 14, 2017 and is referenced in knowledge base article 4013389.

Once executed, the worm will attempt to contact one of the following remote locations, known as kill-switch domains:

- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

If the remote location is reachable, the worm module will exit immediately. These locations are known as the kill switch domains. Subsequent releases of the worm have had the kill switch reference removed.

Once executed, the worm registers itself as a service that is scheduled to start automatically.
Service name: mssecsvc2.0
Display name: Microsoft Security Center (2.0) Service
Path: {path-to-worm} -m security
Startup type: SERVICE_AUTO_START

The ransomware module is embedded inside the worm.

Once the worm is executed, it will attempt to drop the ransomware module to the local machine. It will see if the file “TASKSCHE.EXE” exists and rename it to C:\WINDOWS\qeriuwjhrf

The ransomware module is called C:\WINDOWS\TASKSCHE.EXE

The worm module will try to download and install Tor (online anonymity network designed to conceal a user’s identity and online activities). The known locations it downloads it from are as follows:

- dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip
- www.dropbox.com/s/yw3rvyotvb4gcnh/t1.zip?dl=1

Some variants of the worm already contained a copy of the Tor application and do not need to download it from remote sites.

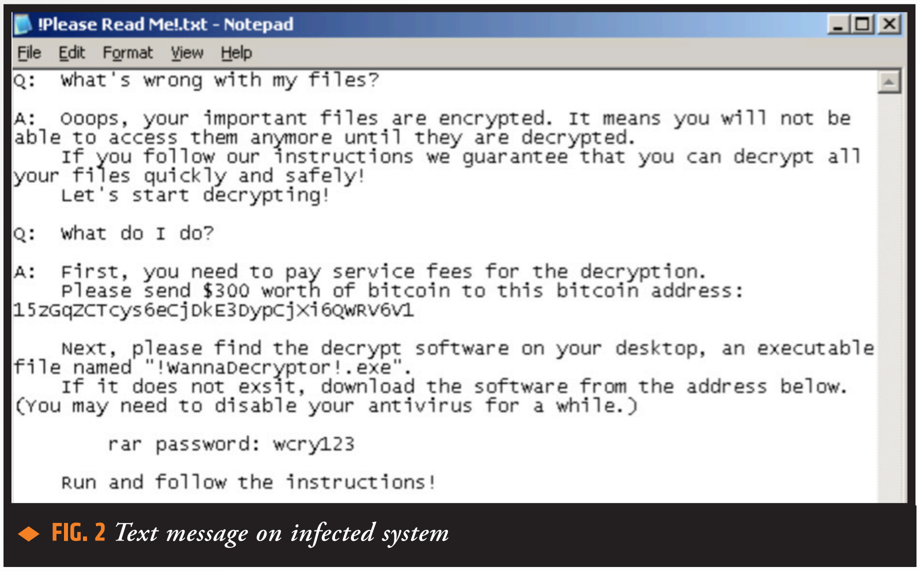
Once the Tor application is downloaded, tor.exe is extracted and saved as “taskhosts.exe” and executed to establish a connection to the Tor network. The following Tor domains are known to be associated with the worm:

- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- xxlvbrloxvriy2c5.onion
- 76jdd2i r2embyv47.onion
- cwwnhwhlz52maqm7.onion

The worm will attempt to propagate by scanning IP addresses of other computers. It looks for TCP/445 open on the following IP address ranges:

- Any IP address on the same subnet as the compromised computer (Local Area Network)
- Randomly generated IP addresses, which spread to any computer.

Once it establishes contact with the computer, it will attempt to use the SMB remote code execution vulnerability (CVE-2017-0144) to spread. The malware will attempt exploit SMBv1. However, the malicious code



```
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:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

    Next, please find the decrypt software on your desktop, an executable
file named "!WannaDecryptor!.exe".
    If it does not exsit, download the software from the address below.
(You may need to disable your antivirus for a while.)

        rar password: wcry123

    Run and follow the instructions!
```

FIG. 2 *Text message on infected system*

will use SMBv2. During the attack, both SMBv1 and SMBv2 packets are used. By disabling SMBv1 or SMBv2 prevents the infection; however, while disabling the old protocol SMBv1 has no significant impact on modern systems, disabling SMBv2 can cause a few problems. It's highly recommended to disable SMBv1 for the current cyber attack and future attacks.

THE RANSOMWARE MODULE

When the code is first executed, it copies itself to the following locations on the victim's machine:

- %SystemDrive%\ProgramData\[RANDOM_STRING]\tasksche.exe
- %SystemDrive%\Intel\[RANDOM_STRING]\tasksche.exe

The ransomware module may then create the following files:

- {path-to-ransomware}\!WannaDecryptor!.exe
- {path-to-ransomware}\c.wry
- {path-to-ransomware}\f.wry
- {path-to-ransomware}\m.wry
- {path-to-ransomware}\r.wry
- {path-to-ransomware}\t.wry
- {path-to-ransomware}\u.wry
- {path-to-ransomware}\TaskHost
- {path-to-ransomware}\00000000.eky
- {path-to-ransomware}\00000000.pky
- {path-to-ransomware}\00000000.res
- %Temp%\0.WCRYT
- %Temp%\1.WCRYT
- %Temp%\2.WCRYT
- %Temp%\3.WCRYT
- %Temp%\4.WCRYT
- %Temp%\5.WCRYT
- %Temp%\hibsys.WCRYT
- %UserProfile%\Desktop\!WannaCryptor!.bmp
- C:\Intel\zirjvfpqmgcm054\TaskData\Tor\taskhsvc.exe
- C:\Intel\zirjvfpqmgcm054\TaskData\Tor\tor.exe
- C:\Intel\zirjvfpqmgcm054\taskdl.exe
- C:\Intel\zirjvfpqmgcm054\tasksche.exe
- C:\Intel\zirjvfpqmgcm054\taskse.exe
- C:\Intel\zirjvfpqmgcm054\@WanaDecryptor@.exe
- C:\Intel\zirjvfpqmgcm054\msg\m_bulgarian.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_chinese (simplified).wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_chinese (traditional).wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_croatian.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_czech.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_danish.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_dutch.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_english.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_filipino.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_finnish.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_french.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_german.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_greek.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_indonesian.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_italian.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_japanese.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_korean.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_latvian.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_norwegian.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_polish.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_portuguese.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_romanian.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_russian.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_slovak.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_spanish.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_swedish.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_turkish.wnry
- C:\Intel\zirjvfpqmgcm054\msg\m_vietnamese.wnry
- C:\Intel\zirjvfpqmgcm054\b.wnry (copy of @WanaDecryptor@.bmp)
- C:\Intel\zirjvfpqmgcm054\c.wnry
- C:\Intel\zirjvfpqmgcm054\f.wnry
- C:\Intel\zirjvfpqmgcm054\r.wnry (copy of @Please_Read_Me@.txt)
- C:\Intel\zirjvfpqmgcm054\s.wnry
- C:\Intel\zirjvfpqmgcm054\t.wnry

- C:\Intel\zirjvfpqmgcm054\u.wnry
- The ransomware module may create the following registry keys on the victim’s machine:
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\”Microsoft Update Task Scheduler” =””{path-to-ransomware}\[RANSOMWARE_EXECUTABLE]” /r”
- HKEY_LOCAL_MACHINE\SOFTWARE\WannaCryptor\”wd” = “[PATH_TO_RANSOMWARE]”
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\”zirjvfpqmgcm054” = “”C:\Intel\zirjvfpqmgcm054\tasksche.exe””
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\zirjvfpqmgcm054\Security\”Security” = “[HEX_VALUE]”
- HKEY_LOCAL_MACHINE\SOFTWARE\WannaCryptor\”wd” = “{path-to-ransomware}”

The ransomware module will also change the wallpaper to a file on the user’s desktop called “!WannaCryptor!.bmp.” This is the registry key that will be modified:

- HKEY_CURRENT_USER\Control Panel\Desktop\”Wallpaper” = %UserProfile%\Desktop\!WannaCryptor!.bmp

A new service is created which will enable it to be restarted when the computer starts:

Service name: {random}
Display name: {random}
Path: cmd.exe /c {path-to-ransomware}
Startup type: SERVICE_AUTO_START

The malware will also attempt to stop a number of services to release the locks on files that will be victim of encryption.

Known file extensions used are:

- .wnry
- .wcry
- .wncry
- .wncryt

The following files are dropped inside every folder where files are encrypted:

- Please_Read_Me@.txt
- @WanaDecryptor@.exe.lnk
- !WannaDecryptor!.exe.lnk
- !Please Read Me!.txt

Ransom payment is between $300–600 in Bitcoin payment. The known bitcoin wallet addresses which are hard coded in to the ransomware module are:

- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

The ransomware module creates mutexes (mutant objects) in memory to ensure only one instance of the module can run:

- Global\WINDOWS_TASKOSHT_MUTEX0
- Global\WINDOWS_TASKCST_MUTEX
- Global\MsWinZonesCacheCounterMutexA

THE KNOWN SHA256 HASHES OF THE WANNACRY ARE AS FOLLOWS:

- 01b628fa60560c0cb4a332818cb380a65d0616d19976c084e0c3eaa433288b88
- 02932052fafe97e6acaaf9f391738a3a826f5434b1a013abbfa7a6c1ade1e078
- 03363f9f6938f430a58f3f417829aa3e98875703eb4c2ae12feccc07fff6ba47
- 0345782378ee7a8b48c296a120625fd439ed8699ae857c4f84befeb56e727366
- 03b41fac10c02b67c99a9f2a462055df590f26f86a5dfe1b15940a6bcfad0d83
- 043e0d0d8b8cda56851f5b853f244f677bd1fd50f869075ef7ba1110771f70c2
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
- 09dc146765eb44849c4fca7eed228efc82a02132968245e613e163799c318a23
- 0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
- 0b1ea4458dbc6e6f71c8c548da2d2ef21cc51d938240b2168252c188a797d5dc
- 0bb221bf62d875cca625778324fe5bd6907640f6998d21f3106a0447aabc1e3c
- 0c2d3094ce5f7b2d5aa1788503e37b8db2e550d10a87650e6a0c4dcca2af8ff6
- 0d9eb4c1de7622e13ccd4dcde11fec95d6662152f6ef5e3ebf1fdc8195596175
- 0fc245e8a1134e31b7687fb7501faa05628813c87b9561ee26f2092cb76e5a36
- 11011a590796f6c52b046262f2f60694310fa71441363d9116ada7248e58509a
- 112e2973f11414b94df3ec9547eaa717765d7c06646bc606f2a6d48407013422
- 11d0f63c06263f50b972287b4bbd1abe0089bc993f73d75768b6b41e3d6f6d49
- 12d67c587e114d8dde56324741a8f04fb50cc3160653769b8015bc5aec64d20b
- 146f61db72297c9c0facffd560487f8d6a2846ecec92ecc7db19c8d618dbc3a4
- 149601e15002f78866ab73033eb8577f11bd489a4cea87b10c52a70fdf78d9ff
- 16493ecc4c4bc5746acbe96bd8af001f733114070d694db76ea7b5a0de7ad0ab
- 16a2a471038f5e4e79c816ceb0c2eb272463c37268b7b4e845f287f5027f070d
- 190d9c3e071a38cb26211bfffeb6c4bb88bd74c6bf99db9bb1f084c6a7e1df4e
- 191f3e94249f21fb596b4dba7eb197ab89bacae93f1b1fdbd9db733904bd5438
- 1be07198c324c9732d4e2676945ec021eeacd78775aea2100f49ca0483d3f901
- 1be0b96d502c268cb40da97a16952d89674a9329cb60bac81a96e01cf7356830
- 1e6753f948fa648ef9e0d85795b7f090968ee1f240efc0628283776ea55ccb0f
- 1f21838b244c80f8bed6f6977aa8a557b419cf22ba35b1fd4bf0f98989c5bdf8
- 201f42080e1c989774d05d5b127a8cd4b4781f1956b78df7c01112436c89b2c9
- 22ccdf145e5792a22ad6349aba37d960db77af7e0b6cae826d228b8246705092
- 23e5e738aad10fb8ef89aa0285269aff728070080158fd3e7792fe9ed47c51f4
- 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
- 2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
- 26fd072fda6e12f8c2d3292086ef0390785efa2c556e2a88bd4673102af703e5
- 285411b4f4df1af43dac8cc84309ff7d0c252aa282686a0d4eb4641f58f6133f
- 2adc900fafa9938d85ce53cb793271f37af40cf499bcc454f44975db533f0b61
- 2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
- 2c95bef914da6c50d7bdedec601e589fbb4fda24c4863a7260f4f72bd025799c
- 2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
- 2d8b8a8000817d3cfe118c68c4d99068e8bcb7fa64df88e1698e1db73a268373
- 302c232e07e6a30ae1612360570d1fbfdea1631e2589f8f23e7aa931c83c2550
- 31c2024d0df684a968115e4c3fc5703ef0ea2de1b69ece581589e86ba084568a
- 3dcbb0c3ede91f8f2e9efb0680fe0d479ff9b9cd94906a86dec415f760c163e1
- 3e6de9e2baacf930949647c399818e7a2caea2626df6a468407854aaa515eed9
- 3f33734b2d34cce83936ce99c3494cd845f1d2c02d7f6da31d42dfc1ca15a171
- 40b37e7b80cf678d7dd302aaf41b88135ade6ddf44d89bdba19cf171564444bd
- 4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
- 452ecb2ea7b73fa14756fed95602b18a31c8858d60e1def81244bb2ceb2551ed
- 498b8b889bb1f02a377a6a8f0e39f9db4e70cccad820c6e5bc5652e989ae6204
- 49f2c739e7d9745c0834dc817a71bf6676ccc24a4c28dcddf8844093aab3df07
- 4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
- 4b76e54de0243274f97430b26624c44694fbde3289ed81a160e0754ab9f56f32
- 4c69f22dfd92b54fbc27f27948af15958adfbc607d68d6ed0faca394c424ccee
- 4d67e6c708062e970d020413e460143ed92bebd622e4b8efd6d6a9fdcd07bda8
- 5078f8440c25ddb5b85beb8edeae143c716a1a01c8a49c5a8d856cf507510c96
- 519ad66009a6c127400c6c09e079903223bd82ecc18ad71b8e5cd79f5f9c053e
- 552aa0f82f37c9601114974228d4fc54f7434fe3ae7a276ef1ae98a0f608f1d0
- 57c12d8573d2f3883a8a0ba14e3eec02ac1c61dee6b675b6c0d16e221c3777f4
- 57e3e45af5b9e84b8a548765f90e2232d471535f2844f5196107a24de9f63624
- 593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af
- 5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
- 5afa4753afa048c6d6c39327ce674f27f5f6e5d3f2a060b7a8aed61725481150
- 5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
- 5c7f6ad1ec4bc2c8e2c9c126633215daba7de731ac8b12be10ca157417c97f3a
- 5d26835be2cf4f08f2beeff301c06d05035d0a9ec3afacc71dff22813595c0b9
- 5d8123db7094540954061ab1fbc56eedcd9e01110b62d0f54206e3e75a39776a
- 5dee2ac983640d656f9c0ef2878ee34cda5e82a52d3703f84278ac372877346d
- 5f2b33deee53390913fd5fb3979685a3db2a7a1ee872d47efc4f8f7d9438341f
- 63bd325cc229226377342237f59a0af21ae18889ae7c7a130fbe9fd5652707af
- 63c8a30963265353532d80a41cae5d54b31e5c2d6b2a92551d6f6dcadd0dedeb
- 646a30f6c9a5e5e3801cfa926c87fc18da395aac86ec0bfd3d0305b45333d384
- 64cd767309a68a963679a5d2807adc364793d229a5e3dd5c63269d48d823a78c
- 67eaab37318df65a2ee8480b4a408f7ba823a2f15eb6d23af0aca28a9cca1d27
- 67eedfe3f13e2638de7d028aaf1e116410562cc5d15a9e62a904f758770dc6bf
- 68a033e7f563a015386435ca54fe03df4929eea561c5fef2419312d838906af9
- 6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7
- 6cb7e4f6539ee9f9107922549d83860399ffc1eb3adb177defde52b1eec1eb3d
- 6cefed15f21b9e2a50536ed1b58f94b889c58c71e64bfd304183f9e49354ab25
- 6db650836d64350bbde2ab324407b8e474fc041098c41ecac6fd77d632a36415
- 6ed7f244f54f500c1606ba09d92fc2e6989eb9222423e6e8b5e94d3e65ab0376
- 70c0f32ed379ae899e5ac975e20bbbacd295cf7cd50c36174d2602420c770ac1
- 7108d6793a003695ee8107401cfb17af305fa82ff6c16b7a5db45f15e5c9e12d
- 72f20024b2f69b45a1391f0a6474e9f6349625ce329f5444aec7401fe31f8de1
- 76a3666ce9119295104bb69ee7af3f2845d23f40ba48ace7987f79b06312bbdf
- 78e3f87f31688355c0f398317b2d87d803bd87ee3656c5a7c80f0561ec8606df
- 7966d843e5760ece99bd32a15d5cd58dc71b1324fdc87e33be46f377486a1b4b
- 7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
- 7bb9ea2c0f53fa96883c54fa4b107764a6319f6026e4574c9feec2cb7d9e7d21
- 7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff
- 7e369022da51937781b3efe6c57f824f05cf43cbd66b4a24367a19488d2939e4
- 7e491e7b48d6e34f916624c1cda9f024e86fcbec56acda35e27fa99d530d017e
- 812fedc37236d3d91ff8fd3d34cf8f185f2ce3d6c55acbe8529a80230e535253
- 8321dfdf54fa41c6ef19abe98df0f5ef80387790e8df000f6fd6dc71ea566c07
- 845d0e178aeebd6c7e2a2e9697b2bf6cf02028c50c288b3ba88fe2918ea2834a
- 84b1d8023123d575eccd1b917d93a5ca9d70e41dcc14c88a6a6b21ecae7bd57d
- 85466f30e0bdf20bcf6a9860a75ce3ad28673e984ee0e3edaa2123e80b9b6d44
- 85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
- 871d6c43cc02afc9fa156ab9aa8a2d15fbff0e4c22cb633ccdde57e1116986df
- 88be9ee3ce0f85086aec1f2f8409247e8ab4a2a7c8a07af851f8df9814adeee5
- 8ef566726496c895c55f4c565363fe607f0f7c7dd3d38b584b1f0ad439c922bb
- 90245f11ccd958849f9237bc51a6e28dfa0cedff9d74b8273f7d77be5b4cc3b9
- 940dec2039c7fca4a08d08601971836916c6ad5193be07a88506ba58e06d4b4d
- 99c0d50b088df94cb0b150a203de6433cb97d4f8fd3b106ce442757c5faa35c4
- 9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
- 9bd38110e6523547aed50617ddc77d0920d408faeed2b7a21ab163fda22177bc
- 9cc32c94ce7dc6e48f86704625b6cdc0fda0d2cd7ad769e4d0bb1776903e5a13
- 9f670327f8810a5de0a83d56a211f0f0251c348a9178de5e9ce783780abe7ac6
- 9fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b50977
- 9fc129c37c545ec23b3c59e3319d31509cb9ecdd2eeed90ff8a1a99a39bfcd1c
- a0356696877f2d94d645ae2df6ce6b370bd5c0d6db3d36def44e714525de0536
- a0be20c014e384c5f38847723d11a20c82a34315f8303a2825df6f352ca29503
- a141e45c3b121aa084f23ebbff980c4b96ae8db2a8d6fde459781aa6d8a5e99a
- a1d23db1f1e3cc2c4aa02f33fec96346d9d5d5039ffc2ed4a3c65c34b79c5d93
- a2726df3632eba623ebb76c373ec44ba733af9483326bab4cc6a6efc67f5d566

- a373b58673e8434d7ee58f277336482738dbda610874c9b8b992969f67ad334e
- a3900daf137c81ca37a4bf10e9857526d3978be085be265393f98cb075795740
- a50d6db532a658ebbebe4c13624bc7bdada0dbf4b0f279e0c151992f7271c726
- a582f0fc7b605f4d9370677ec4618b62bc77dd72711f76c18b3856e2f3145e18
- a75bb44284b9db8d702692f84909a7e23f21141866adf3db888042e9109a1cb6
- a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
- a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
- aa98d85b6a5a50c91899824a6f6fac52d9580e91e1d6390610d520f66d1ce49f
- ac7f0fb9a7bb68640612567153a157e91d457095eadfd2a76d27a7f65c53ba82
- aea79945c0f2f60de43193e1973fd30485b81d06f3397d397cb02986b31e30d9
- aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c
- b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
- b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
- b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
- b4d607fae7d9745f9ced081a92a2dcf96f2d0c72389a66e20059e021f0b58618
- b55d23b9df8ffe5678234a2ebc473afb3024015c2a79dfef33a1824d08396139
- b66db13d17ae8bcaf586180e3dcd1e2e0a084b6bc987ac829bbff18c3be7f8b4
- b845c58ec3a55933e967b0d4f00c2c0d1f91174cf9f301ca2c889c9f80a3bd1c
- b8611a4468acb1c980282182eb10d2d9de7518753d1621018f0b99d337028af8
- b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
- bb829a0394fb865eed381eb77ac9de039ad19e0f2318baaf9483b4f817250021
- bbc793daa67196de6bcf441ced5df0745300ba6bc8ca43da32e9000b42055b9e
- bc8136b40b4164afcbcb4e14f6fd54ca02275ff75b674eb6fd0a8f436f9b1181
- bd9f4b3aedf4f81f37ec0a028aabcb0e9a900e6b4de04e9271c8db81432e2a66
- be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
- c1f929afa37253d28074e8fdaf62f0e3447ca3ed9b51203f676c1244b5b86955
- c354a9a0bbb975c15e884916dce251807aae788e68725b512a95f7b580828c64
- c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
- c73633e55a1d66af88a3dc2d46e7d47e0a47ce0bab0930a70b97b003adafc9af
- c9e9dc06f500ae39bfeb4671233cc97bb6dab58d97bb94aba4a2e0e509418d35
- ca29de1dc8817868c93e54b09f557fe14e40083c0955294df5bd91f52ba469c8
- cb5da96b3dfcf4394713623dbf3831b2a0b8be63987f563e1c32edeb74cb6c3a
- ceb51f66c371b5233e474a605a945c05765906494cd272b0b20b5eca11626c61
- d06292618fa7ff675d8e4d0989e28387653b8196d5e4cbe9a3bf4b8c07421ea2
- d37ab2f01db94d29e94d148ee7c90aa1aa8783fda65062ba457c36ca42ae6662
- d8489f8c16318e524b45de8b35d7e2c3cd8ed4821c136f12f5ef3c9fc3321324
- d849067bf9365d99088cbb935a98477cd38519e3ab8ac1bfe662588f8177d22d
- d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127
- dca3aaeb2070f63e2ee7c6971e41ef3a9ac2f93885d9cdc317b76035e9114cc6
- dff26a9a44baa3ce109b8df41ae0a301d9e4a28ad7bd7721bbb7ccd137bfd696
- e0ec1ad116d44030ad9ef5b51f18ff6160a227a46ffcf64693335c7fb946fad6
- e13cc9b13aa5074dc45d50379eceb17ee39a0c2531ab617d93800fe236758ca9
- e14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079
- e1ea721788c025755fcefee42347f1e2ff42a6cb374df04c5ea310cc5258d044
- e2d1e34c79295e1163481b3683633d031cab9e086b9ae2ac5e30b08def1b0b47
- e58b5c6e6cb8798a528d5bb76f7d13eaad206506da12c860bc33553cf0f1c251
- e64178e339c8e10eac17a236a67b892d0447eb67b1dcd149763dad6fd9f72729
- e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96
- e989935bb173c239a2b3c855161f56de7c24c4e7a79351d3a457dbf082b84d7b
- ec9d3423338d3a0bfccacaf685366cfb8a9ece8dedbd08e8a3d6446a85019d3a
- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
- ed12621045bc438241b4a1b12da4a7f2f8f841324083b7d2405d80dbbe8fa2f2
- eeb9cd6a1c4b3949b2ff3134a77d6736b35977f951b9c7c911483b5caeb1c1fb
- f5cbff5c100866dd744dcbb68ee65e711f86c257dfcc41790a8f63759220881e
- f6101718090f0f7796ed000b9a612f6c4ef4ab920ee99ac25bbb4e3eaaa41b75
- f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494
- f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
- faea58c7f806db86d3ab5590b57f0112a55e028d41f544fb6622cb057196d930
- fb1cec49c659a35d8529e318437ff46e33fe52d8e39e921bc2e6b6b775fd2626
- fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a

LIST OF USER FILES AFFECTED BY WANNACRY

- 123
- .3dm
- .3ds
- .3g2
- .3gp
- .602
- .7z
- .ARC
- .PAQ
- .accdb
- .aes
- .ai
- .asc
- .asf
- .asm
- .asp
- .avi
- .backup
- .bak
- .bat
- .bmp
- .brd
- .bz2
- .cgm
- .class
- .cmd
- .cpp
- .crt
- .cs
- .csr
- .csv
- .db
- .dbf
- .dch
- .der
- .dif
- .dip
- .djvu
- .doc
- .docb
- .docm
- .docx
- .dot
- .dotm
- .dotx
- .dwg
- .edb
- .eml
- .fla
- .flv
- .frm
- .gif
- .gpg
- .gz
- .hwp
- .ibd
- .iso
- .jar
- .java
- .jpeg
- .jpg
- .js
- .jsp
- .key
- .lay
- .lay6
- .ldf
- .m3u
- .m4u
- .max
- .mdb
- .mdf
- .mid
- .mkv
- .mml
- .mov
- .mp3
- .mp4
- .mpeg
- .mpg
- .msg
- .myd
- .myi
- .nef
- .odb
- .odg
- .odp
- .ods
- .odt
- .onetoc2
- .ost
- .otg
- .otp
- .ots
- .ott
- .p12
- .pas
- .pdf
- .pem
- .pfx
- .php
- .pl
- .png
- .pot
- .potm
- .potx
- .ppam
- .pps
- .ppsm
- .ppsx
- .ppt
- .pptm
- .pptx
- .ps1
- .psd
- .pst
- .rar
- .raw
- .rb
- .rtf
- .sch
- .sh
- .sldm
- .sldx
- .slk
- .sln
- .snt
- .sql
- .sqlite3
- .sqlitedb
- .stc
- .std
- .sti
- .stw
- .suo
- .svg
- .swf
- .sxc
- .sxd
- .sxi
- .sxm
- .sxw
- .tar
- .tbk
- .tgz
- .tif
- .tiff
- .txt
- .uop
- .uot
- .vb
- .vbs
- .vcd
- .vdi
- .vmdk
- .vmx
- .vob
- .vsd
- .vsdx
- .wav
- .wb2
- .wk1
- .wks
- .wma
- .wmv

The malware is not difficult to remove but it is difficult to decrypt. So removing the infection cannot restore the files to the original unencrypted state. Best to have implemented a good back up strategy.

HOW TRIPWIRE HELPS

Tripwire offers foundational controls to help preempt and protect against ransomware attacks.

- Tripwire® Enterprise can help you identify which systems have SMB running and whether SMBv1 has been disabled or not. It can monitor the endpoints for creating of files that match specific file hashes or monitor registry keys in real-time, providing early detection of a potential attack. Tripwire Enterprise can validate the patch has been implemented. It integrates with third party software, such as ticketing solutions and service management tools and SIEMs, and can aid with the escalation of a detected threat.
- Tripwire IP360™, Tripwire's vulnerability management solution, can profile the network and identify systems that have weakened security controls like the vulnerability in MS17-010 which focuses on the SMBv1 exploit.

SOURCES FOR RESEARCH

The following sites provided information to put this brief together.

- https://securelist.com/blog/research/78411/wannacry-faq-what-you-need-to-know-today/
- https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99
- https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/
- https://www.redsocks.eu/news/ransomware-wannacry/
- https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
- http://bgr.com/2017/05/15/wanna-cry-ransomware-virus-windows-wannacry-explainer/

LINKS TO RESOURCES

- Microsoft Security Bulletin MS17-010 – Critical
  - https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- KB4013389 Security update for Windows SMB Server
  - https://support.microsoft.com/en-gb/help/4013389/title
- CVE-2017-0144 Vulnerability
  - https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
- Ransomware Attack – Am I Safe Against 'WannaCry'?
  - https://www.tripwire.com/state-of-security/featured/ransomware-attack-safe-wana-decrypt0r/
- Customer Guidance for WannaCrypt attacks
  - https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

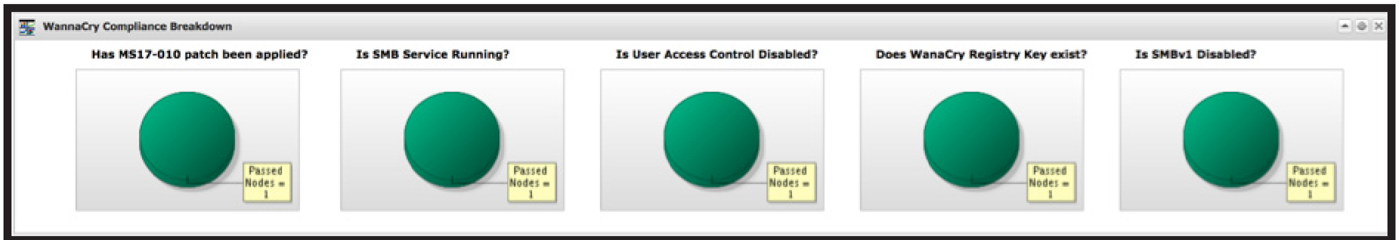

WannaCry Compliance Breakdown
Has MS17-010 patch been applied?
Passed Nodes = 1
Is SMB Service Running?
Passed Nodes = 1
Is User Access Control Disabled?
Passed Nodes = 1
Does WanaCry Registry Key exist?
Passed Nodes = 1
Is SMBv1 Disabled?
Passed Nodes = 1

FIG. 3 *Tripwire Enterprise report showing response to WannaCry*

◆ Tripwire is a leading provider of security, compliance and IT operation solutions for enterprises, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. Learn more at tripwire.com. ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER