WannaCry Ransomware

Compiled by ThaiCERT, a member of the Electronic Transactions Development Agency

Version 1.0 (15 May 2017)

TLP:WHITE

Malware tracking by MalwareTech
WannaCry Ransomware

Contents
Malware names.......................................................................................................................... 3
Management summary .................................................................................................................. 3
Vulnerable systems....................................................................................................................... 3
Worldwide infections ................................................................................................................... 3
Prevention.................................................................................................................................... 4
Recovery....................................................................................................................................... 4
Technical analysis: Distribution .................................................................................................... 5
Technical analysis: Encryption ...................................................................................................... 6
Kill-switch and kill-mutex .............................................................................................................. 13
Malware versions ......................................................................................................................... 13
Tracking ransom payments of this malware campaign ............................................................... 13
Malware indicators ...................................................................................................................... 14
   SHA256 hashes ........................................................................................................................ 14
   Command and Control servers (on the TOR network) ............................................................ 15
   Kill-switch domains ................................................................................................................ 15
Malware analysis sources ........................................................................................................... 16
International advisories ............................................................................................................... 16
English news references ............................................................................................................. 16
   WannaCry international outbreak .......................................................................................... 16
   Microsoft’s response ............................................................................................................. 18
   Alleged new malware version without kill-switch ................................................................. 18
   A new malware versions without kill-switch ....................................................................... 18
   Copycats ................................................................................................................................ 18
WannaCry Ransomware

Malware names
Wana Decrypt0r, WCry, WannaCry, WannaCrypt, and WanaCrypt0r

Management summary
WannaCry is a unique form of ransomware that is able to spread itself to other systems as a worm.

A large outbreak occurred on Friday 12 May. To date, more than 200,000 systems have been infected in over 100 countries.

The malware uses exploits that were supposedly leaked by a group that calls itself “ShadowBrokers” a couple of months ago. The result of leaking exploits very often gives rise to malicious actors who use them for their nefarious purposes – which is what happened in this case.

The vulnerability being exploited has already been fixed by Microsoft on 14 March, but not everyone is up-to-date with patches. Also, older versions of Windows that are no longer supported by Microsoft are also vulnerable. Microsoft provided an emergency patch for those older versions on 12 May (the day of the outbreak).

This widespread attack is of high severity, and although the vulnerability being exploited by the attackers should have been patched a while back, many organizations have been hit and the count keeps rising. New versions and variants of this malware are constantly being released, making mitigation harder.

Vulnerable systems
Windows XP through 8.1 (Windows 10 is not vulnerable)

Microsoft released a patch MS17-010 (ETERNALBLUE) on 14 March:
Microsoft released a patch for the older unsupported Windows versions on 12 May:
<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>

Worldwide infections
The kill-switch domain has been registered by the researcher MalwareTech and is being used as a sinkhole.
As such, infections can be observed through the following URL:
<https://intel.malwaretech.com/botnet/wcrypt/?t=24h&bid=all>
WannaCry Ransomware

Prevention

- Patch your systems
- Make backups
- Do not expose the SMB protocol to the outside world. Block TCP/445\(^1\).
- The vulnerability can also be closed by completely disabling SMBv1 support. See [https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012](https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)

Recovery

- You can recover from backups, and if those do not exist, try a program like [Shadow Explorer](https://www.bleepingcomputer.com/tutorials/how-to-recover-files-and-folders-using-shadow-volume-copies/) in the hopes that the ransomware did not properly delete your Shadow Volume Copies. If a user did not click Yes at the UAC prompt, then there is a chance those are still available to recover from. A guide on recovery files from Shadow Volume Copies can be found at [https://www.bleepingcomputer.com/tutorials/how-to-recover-files-and-folders-using-shadow-volume-copies/](https://www.bleepingcomputer.com/tutorials/how-to-recover-files-and-folders-using-shadow-volume-copies/)
- There is a detailed manual to remove this malware from the system available at [https://www.pcrisk.com/removal-guides/10942-wcry-ransomware#a2](https://www.pcrisk.com/removal-guides/10942-wcry-ransomware#a2)
- If your systems have been affected, DOUBLEPULSAR will have also been installed, so this will need to also be removed. A script is available that can remotely detect and remove the DOUBLEPULSAR backdoor, at [https://github.com/countercept/doublepulsar-detection-script](https://github.com/countercept/doublepulsar-detection-script)

---

\(^1\) It is Good Practice to filter all NetBIOS traffic (TCP/137, TCP/139, TCP/445, UDP/137 and UDP/138), but WannaCry only leverages port TCP/445.
WannaCry Ransomware

Technical analysis: Distribution

It is still unclear what the initial infection vector is. Microsoft's analysis reports:

- We haven't found evidence of the exact initial entry vector used by this threat, but there are two scenarios we believe are highly possible for this ransomware family:
  - Arrival through social engineering emails designed to trick users to run the malware and activate the worm-spreading functionality with the SMB exploit
  - Infection through SMB exploit when an unpatched computer can be addressed in other infected machines

Once the malware is on a system, its worm capability will try to spread further through SMB. After initializing the functionality used by the worm, two threads are created. The first thread scans hosts on the LAN. The second thread gets created 128 times and scans hosts on the wider Internet. The scanning thread tries to connect to port 445, and if so creates a new thread to try to exploit the system using the ETERNALBLUE SMB vulnerability (MS17-010). If the exploitation attempts take over 10 minutes, then the exploitation thread is stopped.

From Talos Intelligence\(^2\): WannaCry make use of DOUBLEPULSAR which is a persistent backdoor that is generally used to access and execute code on previously compromised systems. This allows for the installation and activation of additional software, such as malware. This backdoor is typically installed following successful exploitation of SMB vulnerabilities addressed as part of Microsoft Security Bulletin MS17-010. This backdoor is associated with an offensive exploitation framework that was released as part of the Shadow Brokers cache that was recently released to the public. Since its release it has been widely analyzed and studied by the security industry as well as on various underground hacking forums.

WannaCry appears to primarily utilize the ETERNALBLUE modules and the DOUBLEPULSAR backdoor. The malware uses ETERNALBLUE for the initial exploitation of the SMB vulnerability. If successful it will then implant the DOUBLEPULSAR backdoor and utilize it to install the malware. If the exploit fails and the DOUBLEPULSAR backdoor is already installed the malware will still leverage this to install the ransomware payload.

(From <https://isc.sans.edu/port.html?port=445>)

\(^2\) <http://blog.talosintelligence.com/2017/05/wannacry.html>
When a computer becomes infected with Wana Decrypt0r, the installer will extract an embedded file into the same folder that the installer is located in. This embedded resource is a password-protected zip folder that contains a variety of files that are used by and executed by WanaCrypt0r.

The WanaDecrypt0r loader will then extract the contents of this zip file into the same folder and perform some startup tasks. It will first extract localized version of the ransom notes into the msg folder. The currently supported languages are:

- Bulgarian
- Chinese (simplified)
- Chinese (traditional)
- Croatian
- Czech
- Danish
- Dutch
- English
- Filipino
- Finnish
- French
- German
- Greek
- Indonesian
- Italian
- Japanese
- Korean
- Latvian
- Norwegian
- Polish
- Portuguese
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Turkish
- Vietnamese

WanaCrypt0r will then download a TOR client from https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip and extract it into the TaskData folder. This TOR client is used to communicate with the ransomware C2 servers at gx7ekbenv2riucmf.onion, 57g7spgrzlojinas.onion, xxlvbrlovrriy2c5.onion, 76jdd2ir2embyv47.onion, and cwwnhwhlz52maqm7.onion.

In order to prep the computer so that it can encrypt as many files as possible, WanaCrypt0r will now execute the command `icacls . /grant Everyone:F /T /C /Q` in order to change give everyone full permissions to the files located in the folder and subfolders under where the ransomware was executed. It then terminates processes associated with database servers and mail servers so it can encrypt databases and mail stores as well.

---

WannaCry Ransomware

The commands that are executed to terminate the database and exchange server processes are:

```plaintext
taskkill.exe /f /im mysqld.exe
taskkill.exe /f /im sqlwriter.exe
taskkill.exe /f /im sqlserver.exe
taskkill.exe /f /im MSExchange*
taskkill.exe /f /im Microsoft.Exchange.*
```

Now, Wana Decrypt0r is ready to start encrypting the files on the computer. When encrypting files, WanaDecrypt0r will scan all drives and mapped network drives for files that have one of the following extensions:


When encrypting a file it will add the **WANACRY!** string, or file marker, to the beginning of the encrypted file.
WannaCry Ransomware

It will then append the `.WNCRY` extension to the encrypted file to denote that the file has been encrypted. For example, a file called `test.jpg` would be encrypted and have a new name of `test.jpg.WNCRY`. 
WannaCry Ransomware

When encrypting files, it will also store a @Please_Read_Me@.txt ransom note and a copy of the @WanaDecryptor@.exe decryptor in every folder that a file was encrypted. We will take a look at those files later.

Finally, WanaCrypt0r will issue some commands that clear the Shadow Volume Copies, disable Windows startup recovery, clear Windows Server Backup history. The commands that are issued are:

```
C:\Windows\SysWOW64\cmd.exe /c vssadmin delete shadow /all /quiet &
wmic shadowcopy delete & bcdedit /set {default} boostatuspolicy
ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin
delete catalog -quiet
```

As these commands require Administrative privileges, victims will see a UAC prompt similar to the one below.
Finally, the installer will execute the `@WanaDecryptor@.exe` program so that the Wana Decrypt0r 2.0 lock screen will be displayed. This screen contains further information as to how the ransom can be paid and allows you to select one of the languages listed above. Once you see this screen and realize you are infected, it is important to terminate all the malware processes as Wana Decrypt0r will continue to encrypt new files as they are made.
WannaCry Ransomware

When you click on the **Check Payment** button, the ransomware connects back to the TOR C2 servers to see if a payment has been made. Even if one was made, the ransomware will automatically decrypt your files. If payment has not been made, you will see a response like the one below.

![Payment not made Response](image)

There are three hard coded bitcoin addresses in the WanaCrypt0r ransomware. These bitcoin addresses are 13AM4VW2dhXyGxeQepoHkHSQy6NgaEb94, 12t9YDPgwueseZ9NyMgw519p7AA8isjr6SMw, and 115p7UMMngoj1pMvkpHijcRdJNXj6LrLr. Maybe I am missing something, but what I do not understand is if so many people are utilizing the same bitcoin address, how will the ransomware developers be able to differentiate the victims that have paid from those who have not? For example, people have paid ransom to my assigned bitcoin address, yet the program still states I did not pay.

The Wana Decryptor 2.0 screen also has a **Contact Us** label that opens a form where you can contact the ransomware developer.

![Contact Us Form](image)
WannaCry Ransomware

The ransomware will also configure your Desktop wallpaper to display another ransom note as shown below.

![Desktop Wallpaper](image)

**Ooops, your important files are encrypted.**

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

![@Please_Read_Me@.txt Ransom Note](image)

Last, but not least, a ransom note will be left on the desktop that contains more information and answers to frequently asked questions.
WannaCry Ransomware

Kill-switch and kill-mutex

- The malware stops if it finds the domain "www.\{iuqerfsodp9lfajaposdf\}hgosurjaewrwegwea.]\com" exists. It does exist, as it has been registered by a malware researcher.
  
  Note: Organizations that use proxies will not benefit from the kill-switch, unless it is a transparent proxy. The malware is not proxy-aware, so it will not be able to connect to the kill-switch domain and thus the malware will not be stopped.
- The malware tries to create a mutex named “MsWinZonesCacheCounterMutexA”. If it exists already, the encryption phase will not be done.

Malware versions

- The first version broke out on Friday 12 May around 21:00 local time.
  First Variant: .wcry
  Second Variant: .WCRY (+ .WCRYT for temp)
  Third Variant: .WNCRY (+ .WNCRYT for temp)
- A new version, with different kill-switch domain, has been observed on 14 May. This domain has been registered and points to a sinkhole as well. Only 2 letters differ: “www.\{iuqerfsodp9lfajaposdf\}hgosurjaewrwegwea.]\com” becomes “www.\{iuqerfsodp9lfajaposdf\}hgosurjaewrwegwea.]\com”
- A new version was found on Sunday 14 May that has the kill-switch domain check edited out. Analysis has been provided by Rendition Infosec to back up this statement.

A report appeared in the media about a new version (dubbed “2.0” in the media) on Saturday 13 May. This version was said not to have the kill-switch domain. This was retracted as an error the next day.

Tracking ransom payments of this malware campaign

The malware has 3 hardcoded bitcoin wallet addresses where the ransom money has to be paid to. Since bitcoin transactions are publicly viewable, they can be monitored:

<https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw>
<https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNX6LrLn>
<https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy8NqaEb94>

5 <https://www.renditioninfosec.com/2017/05/wanacrypt0r-worm-with-kill-switch-patched-out/>
6 <http://thehackernews.com/2017/05/wannacry-ransomware-cyber-attack.html>
7 <https://twitter.com/craiu/status/863718940870139904> and <https://twitter.com/threatintel/status/863766609328050177>
WannaCry Ransomware

Malware indicators

SHA256 hashes

593bbccc8f34047da9960b8456094c0ea6f96aaf16f1626b813484207df8bb8af
5ad4ef9d0cde0126cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acac5c1f4f69c95cf9725d969f9f9efc79d70bd0f2624e06ca5bcbac4d2211046ed6
5d26835be2cf4f08f2bef3f01c0d65035d0a9ec3afacc71df22813595c0b9
62d828ee000e4f670ba322644c2351fe31af5b88a98f22c27e423d3cfd1d9b1
6bf18397e172a92a2bb18bedf1873e4892b00e4a1b22e48ae08fac5408db1a7
7108d7693a003695ee8107401cfb17af3059a82f66c167a5db5f56c59e12d
72af21d8139a80f317e851a60027f9df208871ed334c12637f49d819ab4b033dd
76a3666ce119295104bb69ee7af3f2845d23f40ba48ace7987f790b06312bbf
78e3f87f31688355c0f398317bd87d03dbd87ee3656c5a70c80f0561e8606df
7a828a3daf2aebf153d84930890d498072b7e507c702e4cdd86cafb727cafc545
7c465e7abcccf49f4147add808f24269464e0e1ca4823f16e8c19e009f00ff
7e369022da51937781b3e6c657f824f05cf43cb66ba4a23676a194882939e4
85ec324b8f78021ecfc9b4117c4f19b82e61bb09f3f64f2ab4579f9e19b186
9588f2ef06b7e1ce8509f32d8eddfaf1804a19cc1b9c0d6a48a39f8d8cf9d67
97ebe49b14c46bebc9ec24480e1e397123b256e2be9ba51406887e7bc0a6
9b60c622546dc45cca64df9353b71c26dc4f84866f6a811944dbc4e23db935640
9cc32c94ce7d6e48f86706256b6cc0fda02dcd76e9d4d0bb1776903e5a13
9e02626a5c038de8656e5ebe8627a440a6e839f61e940a8d5f26e9a4982
9fbf3911eb53f687065d5329d845423dfd3cc4a199f5d07c4b50977
a1d9cd6f189beff28a0a49b10f8fe4510128471f00434e238ddc7f875894906b
a3900daf13781ca37aaf1e08e95752d63978be085e265393f98c0b075795740
a9897345b68191fd3f6f8efeb52e6a77abc2367432abb648b9ea0a9d78046e5b
a939e7a13238bd038cbec635f39619db566145498fe6e0a6e6766d14b3d
aee20f9188a5c3954625383c6b0e6623ec90d53f3dec4e1001646e27664002
b3c393ae1b4425f137b5db0df7d65f416da45c0e8518ef7e209a6d386dc60bac7
b43b2340b2833b3df6d7ca032b13cc2354d6e27e092873bf8af2693c
b47e281bffbe0758f8c625bed5c50a27ee80065ceadd766b010d226206f0
b66db13d17ae8bcb05969e753e3dcd1e2e0a846b6c987ac829bff18c3be7f8b4
b9c5d43398090e0ad9a00d4d3db26df44a32819a54a84666b9560d18319c2
be22645c61949ad6a077373a7d6cd85e3fae44315632f161adac499d5a8e684
b365dada345cfcaff3d62950572a484c5f2213933d68e4a5130b8bb7badaaf9
c029de1d8c817869c93e54b09f557fe1e4004083c0955294df5bd9f152b0a49c8
d5e0e8694d0c548d68b78c3d50f4ab51ce6dbadb106d6a6a794c3e746f4fa
d8a9879a99a7c7b12e636a8c27f965fb16b3d892a86a9f1b608ce7f11f7127
dff26a944baa3ce109b8df41ae0a0301d9e4a28ad7b7721bb7ccd137bff69
e14f1a655d9254d0d651cd2a3af576bffdf371ccf6b828ee483b1bd6d21079
e18f9d12fe5b45776e6d5783caf3547886cfd135d7086c8bee037436df4f
e8450d69f098b2c39c6d01039db4020a208d6924ed292f092894a96
eb47c6a937221411bb88dafa3590a9897fb234160087089a064066a65f2b0cd4
e01e1ebcbe9eb5beba545af4d01bf5f1017616184048439ce65be8e08e41aa
eeb9c6aal4c43949b2ff3134a77d6736b35977f951597c7114835ba6e1c1fb
f7c7b5e4b05ea5bd0017803f40af13bed224c40bf6d0b8906784df5bd63494
WannaCry Ransomware

f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a

Command and Control servers (on the TOR network)

57g7spgrzlojinasonion
76jdd2ir2embyv47.onion
cwwnhwh1z52ma.onion
gx7ekbenv2riucmf.onion
sqjolphimrr7jqw6.onion
xxlvbrloxvriy2c5.onion

Kill-switch domains

Do not block these domains, but only monitor. Make sure the domain resolves (can be added locally) if you run a transparent proxy. Resolving is sufficient, no interaction is needed, to stop the malware.

www.iuqerfsodp9ifjaposdfjgosurijfaewrwegwa.com
www.ifferfsodp9ifjaposdfjgosurijfaewrwegwa.com
WannaCry Ransomware

Malware analysis sources
<http://blog.talosintelligence.com/2017/05/wannacry.html>
<https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/>
<https://blog.didierstevens.com/2017/05/13/quickpost-wcry-killswitch-check-is-not-proxy-aware/>
<https://blog.fox-it.com/2017/05/12/massive-outbreak-of-ransomware-variant-infects-large-amounts-of-computers-around-the-world/>
<https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis/>
<https://www.anomalii.com/blog/wanacry#When:02:43:00Z>

International advisories
<https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported>
<https://www.us-cert.gov/ncas/alerts/TA17-132A>
<http://blog.fortinet.com/2017/05/12/protecting-your-organization-from-the-wcry-ransomware>
<https://www.thaichert.or.th/alerts/user/2017/ai2017us001.html>
<https://circle.lu/pub/tr-41/#proactive-measures-for-the-wannacry-ransomware>
<https://www.pcmag.com/reviews/removal-guides/10942/wcry-ransomware#a2>
<https://isc.sans.edu/diary/22420>

English news references
WannaCry international outbreak
<http://www.bbc.co.uk/news/health-39899646>
<https://twitter.com/search?f=images&vertical=news&q=nhs%20ransomware>
<https://www.theregister.co.uk/2017/05/12/nhs_hospital_shut_down_due_to_cyber_attack/>
<https://arstechnica.com/information-technology/2017/05/nhs-ransomware-cyber-attack/>
<http://www.reuters.com/article/us-spain-cyber-idUSKBN1881TJ?feedType=RSS&feedName=technologyNews>
<https://www.theregister.co.uk/2017/05/12/spain_ransomware_outbreak/>
<https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/>
<http://www.reuters.com/article/us-britain-security-hospitals-idUSKBN18820S?feedType=RSS&feedName=technologyNews>
<http://www.reuters.com/article/us-britain-security-hospitals-microsoft-idUSKBN1882SZ?feedType=RSS&feedName=technologyNews>
WannaCry Ransomware

<https://isc.sans.edu/diary/Massive+wave+of+ransomware+ongoing/22412>
<http://blog.malwarebytes.com/cybercrime/2017/05/wannaencrypt0r-ransomware-hits-it-big-just-before-the-weekend/>
<https://motherboard.vice.com/en_us/article/a-massive-ransomware-explosion-is-hitting-targets-all-over-the-world/>
<http://researchcenter.paloaltonetworks.com/2017/05/60000-ransomware-attacks-worldwide/>
<https://krebsonsecurity.com/2017/05/global-ransomware-attack-earned-nsa-exploit-spreading-wannacrypt0r-attacks/>
<http://thehackernews.com/2017/05/wannacry-ransomware-unlock.html>
<https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/>
<https://www.welivesecurity.com/2017/05/13/wanna-cryptor-ransomware-outbreak/>
<https://www.arbornetworks.com/blog/asert/wannacry/>
<https://twitter.com/MalwareJake/status/863263885280673792>
<https://gist.github.com/rainbro/9056775>
<https://krebsonsecurity.com/2017/05/global-wana-ransomware-outbreak-earned-perpetrators-26000-so-far/>
<https://www.troyhunt.com/everything-you-need-to-know-about-the-wannacrypt-ransomware/>
<https://labsblog.f-secure.com/2017/05/04/wcry-knows-and-unknowns/>
<https://www.darkreading.com/partner-perspectives/malwarebytes/wannacry0r-ransomware-worldwide-a/d/id/1328876>
<http://www.reuters.com/article/us-rentault-cybercrime-idUSKBN1890AK?feedType=RSS&feedName=TechnologyNews>
<https://www.helpnetsecurity.com/2017/05/12/massive-ransomware-campaign/>
<https://blog.fox-it.com/2017/05/13/faq-on-the-wannacry-ransomware-outbreak/>
<https://nakedsecurity.sophos.com/2017/05/14/wannacry-benefits-from-unlearned-lessons-of-slammer-conficker/>
<http://www.reuters.com/article/us-cyber-attack-insurance-idUSKCN18B00H?feedType=RSS&feedName=TechnologyNews>
WannaCry Ransomware

Microsoft’s response

Alleged new malware version without kill-switch

Note: this research has been retracted. No version without kill-switch has been found yet.

A new malware versions without kill-switch

Note: this time it is real.

Copycats