THE WANNACRY RANSOMWARE

Prepared By CERT-MU

May 2017
THE MASSIVE WANNACRY GLOBAL RANSOMWARE ATTACK

Maps showing WannaCry Infections around the world

MAY 2017
1.0 INTRODUCTION

The world has experienced a massive global ransomware cyber-attack known as “WannaCrypt” or “WannaCry” (Ransom: Win32/WannaCrypt) since Friday, May 12 2017. Hundreds of thousands computers worldwide have been hit and affected more than 150 countries. WannaCry is far more dangerous than other common ransomware types because of its ability to spread itself across an organisation’s network by exploiting a critical vulnerability in Windows computers, which was patched by Microsoft in March 2017 (MS17-010). The exploit, known as “Eternal Blue,” was released online in April in the latest of a series of leaks by a group known as the Shadow Brokers, who claimed that it had stolen the data from the Equation cyber espionage group.

The malware has the capability to scan heavily over TCP port 445 (Server Message Block/SMB), spreading similar to a worm, compromising hosts, encrypting files stored on them then demanding a ransom payment in the form of Bitcoin. It is important to note that this is not a threat that simply scans internal ranges to identify where to spread, it is also capable of spreading based on vulnerabilities it finds in other externally facing hosts across the internet.

Microsoft provided an emergency patch for older system versions on 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.

The threat is still under active investigation; the situation may change as we learn more. CERT-MU will continue to actively monitor and analyze this situation for new developments and respond accordingly.

2.0 AFFECTED SYSTEMS

Windows XP through 8.1 (Windows 10 is not vulnerable)

Microsoft released a patch MS17-010 (ETERNALBLUE) on 14 March. More information about the patch is available on:


Microsoft released a patch for the older unsupported Windows versions on 12 May, which can be found on:

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
3.0 MALWARE VERSIONS / VARIANTS

The first version broke out on Friday 12 May and the identified malware variants are as follows:

- VARIANT 1: .wcry
- VARIANT 2: WCRY (+ .WCRYT for temp)
- VARIANT 3: .WCNCRY (+ .WCNCRYT for emp)

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.[.]iuqerfsodp9ifjaosdfjhgosurijfaewrwergwea[.]com becomes www.[.]ijfferfsodp9ifjaosdfjhgosurijfaewrwergwea[.]com

A new version was found on Sunday 14 May that has the kill-switch domain check edited out. This was confirmed by the analysis 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.

4.0 TECHNICAL ANALYSIS OF THE ATTACK

4.1 Distribution of the WannaCry Ransomware

As per Microsoft’s analysis report, it is still unclear what the initial infection vector is:

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.
As per Cisco Intelligence, WannaCry made 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.

5.0 TECHNICAL ANALYSIS: ENCRYPTION

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:  
x7ekbenv2riucmf.onion  
- 7g7spgrzlojinasa.onion  
- xxlvbrlxvriy2c5.onion  
- 76jdd2ir2embyv47.onion  
- cwnnhwhlz52maqm7.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.

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

```
taskkill /ft /im mysqld.exe
taskkill /ft /im sqlwriter.exe
taskkill /ft /im sqlserver.exe
```

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,
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`.

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} bootstatuspolicy 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 Decryptor 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.

![Wana Decryptor 2.0 Lock Screen](image)

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 bitcoin addresses in the WanaCry ransomware and they are:

- 13AM4VW2dhxYqXeQepoHkHSQuy6NgaEb94
- 12t9YPuwZ9NyMqw519p7AA8isjr6SMw
- 115p7UMMngoj1pMvkJHijCdfJNj6Ln.

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

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

```
Oops, your important files are encrypted.

If you see this text, but don't see the "Wana Decryptor" 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 "@Wana Decryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!
```

Finally, a ransom note will be left on the desktop that contains more information and answers to frequently asked questions. This is shown in the screenshot below:
Cisco researchers first observed requests for one of WannaCry’s killswitch domains (iuqerfsodp9ifjaposdfjhosurijfaewrwegwea[.]com) starting at 07:24 UTC, then rising to a peak of just over 1,400 nearly 10 hours later.

The domain composition looks almost human typed, with most characters falling into the top and home rows of a keyboard. Communication to this domain might be categorized as a kill switch domain due to its role in the overall execution of the malware:
The above subroutine attempts an HTTP GET to this domain, and if it fails, continues to carry out the infection. However if it succeeds, then the subroutine exits. The domain is registered to a well-known sinkhole, effectively causing the sample to terminate its malicious activity.

The raw registration information re-enforces this as it was registered on 12 May 2017:

7.0 KILL-SWITCH AND KILL-MUTEX

A kill switch is an event that is used to stop a program from continuing to execute. In the case of WannaCry, the kill switch is a domain name that the Worm component of WannCry connects to when it starts.

When the WannaCry worm was released on March 12th, the kill switch domain was set to **www.[].iuqerfsodp9ifjaposdfhgosurijfaewrwegwea[].com**
The malware stops if it finds the following domain exists:

```
www.[.iuqerfsodp9ifjaposdfjhgosurifjaewrwegwea[.]com
```

It is to be noted that organisations 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.

### 8.0 Malware Indicators

**SHA256 hashes**

- 593bbcc8f34047da9960b84565904c0eaf69caaf16f1626b813484207df8bd8af 5ad4efdf0dec01d26cc6f327ce3ce0b4d4951d49b4a19aa097341aff2aacec 5c1f4f69c45cf79725d9969f9fcf79d07bd0f624e06ca5dbcbacd2211046ed6 5d26b835be2cf4f0f2b0e301c06d05035d0a9ec3ac3c871dff22813595c0b9 62d828ee000e4f670ba322644c2351fe3a1af5b8a98f2b2ce27e423dcf1d1b1 6bf1839a7e72a92a2b18befed1f873e4f829009a4e4b122e48ee80f54048db1a7 7108d6f9a3003695e8107401c8b17a305fa82ff6c16b7a5d45f15e59e12d 72af12d8139a80f317e851a60027fd208871ed334c12637f49819ab4b033dd 76a33666ce9119295104bb69ee7aaf3f2b45d23f4f0ba48ace7987f79b06312bbd 78e3f87f31668355c0f3983172bd87d803bd87ee3656c5a7c80f561ec8606df 7a828af62abf153d840938090d948072b7e507c702e4cdd8c6baf727cacf545 7c465e7a8b0c4f94147add808f24629644be11c0ba4823f16e8c19e0090f0f 7e369022da51937781b3eef6c57f824f05cf43c0d66b4a24367a194882d939e4 85ce324af78f201ece9c5811c748f19b82e611b039f6f4f2eab4579fe1fb9e186 9588f2ef06b7e1c850f93d28edda18041a9cc15b1c90d6da484a39f8dcd967 97e6c49b146466b9c2e2448d00e1e397123b256e2be9eba5140688e7bc0ae6 9b60c622564d45c45caadff95b71c26dcf4886df6a811944dcb4e23db9335640 9cc32c94ce7dc6e4886704625b6cc0fda0d2cd7ad769e40dbb1776903e5a13 9e60269c5038de8956a1c685ebea8627a4a40ae8396f1e940a85d2f2e6a4982 9fb39f162c21e1eb55bf38ee7d0e329d8f4523d3f6cd341a99f5d07cb450977 a1d9c6f188fbb28a04a9dbf08fe4510128471f004b3ee4283dcd7f78954906b a3900dafa137c81ca37a4af10e985752d693788e085be2b5339f98cb075795740 a89734568b619fd3f68f6c526a7a7ac2b2637432abbf46f89e9a09d708406de5b a93ee7a13238b0d338bcbec635f3919db566145498f6e60ea60e6e676d614bd3 aee20f9188a5c3954623583cb60e6623ce90d5c3d3fde4e1001646e27664002c b3c39aeb14425f1d7b0df76541d6a4c5e08158ef7e209aad63dcd60bac7 b438b23041bd2833b3d6fadbc70a32b13a23c54dd6de27e092873b58f2693c b47e281b8efbee0758f8c625bed5ca0d27ee8e0065ceeead76b00100d22606f0 b66db13d17ae8bca5f856180e33dce1e2e0a8486bcb978ac829bff18c3be7f8b4 b9c5d4339809ea09d9aa0d4d3d2d6d4f4423189a54abf846bb9b560d81391c25 be22645c61949ad6a077373a7d6cd85e3f9ae44315632f161adcc499d5a8e6844
The WannaCry Ransomware: White Paper

9.0 COMMAND AND CONTROL SERVERS (ON THE TOR NETWORK)

The malware uses the following C&C Servers to connect:
- 57g7spgrzlojinias.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52ma.onion
- gx7ekbenv2riucmf.onion
- sqjolphimrr7jqw6.onion
- xxlvbrlovxriy2c5.onion

10.0 IMPACT OF THE ATTACK

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including:
- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization’s reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim’s money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.
11.0 DETECTION OF THE ATTACK BY ANTI-VIRUS

Microsoft Anti-Malware products detect the present version of this WannaCry ransomware as *Ransom:Win32.WannaCrypt* from definition version 1.243.291.0

Various anti-virus software detect the malware as:

- Ransom.Wannacry
- Ransom.CryptXXX
- Trojan.Gen.8!Cloud
- Trojan.Gen.2

12.0 CAN THE ENCRYPTED FILES BE RECOVERED?

Decryption is not available at this time but security firms are working on it. Users are strongly recommended not to pay the ransom. Encrypted files should be restored from back-ups where possible.

13.0 WORKAROUNDS

**Recommended Steps for Prevention**

- Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate in-bound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users.
- Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.
- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary.
- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
• Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office suite applications.

• Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.

• Run regular penetration tests against the network, no less than once a year. Ideally, run these as often as possible and practical.

• Test your backups to ensure they work correctly upon use.

13.1 **Recommendations for Network Protection**

Apply the patch (MS17-010). If the patch cannot be applied, consider:

• Disabling SMBv1 and

• blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

*Note:* disabling or blocking SMB may create problems by obstructing access to shared files, data, or devices. The benefits of mitigation should be weighed against potential disruptions to users.

13.2 **Consider implementing the following best practices:**

• Segregate networks and functions.

• Limit unnecessary lateral communications.

• Harden network devices.

• Secure access to infrastructure devices.

• Perform out-of-band network management.

• Validate integrity of hardware and software.

13.3 **Recommended Steps for Remediation**

• Implement your security incident response and business continuity plan. Ideally, organizations should ensure they have appropriate backups so their response is simply to restore the data from a known clean backup.
13.4 Defending Against Ransomware Generally

Precautionary measures to mitigate ransomware threats include:

- Ensure anti-virus software is up-to-date.

- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.

- Scrutinize links contained in emails, and do not open attachments included in unsolicited emails.

- Only download software, especially free software - from sites you know and trust.

- Enable automated patches for your operating system and Web browser.
14.0 REFERENCES

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://securingtomorrow.mcafee.com/mcafee-labs/analysis-wannacry-ransomware/
https://www.anomalí.com/blog/wannacry/#When:02:43:00Z
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.thaicert.or.th/alerts/user/2017/al2017us001.html
https://circl.lu/pub/tr-41/#proactive-measures-for-the-wannacry-ransomware
https://www.pcrisk.com/removal-guides/10942-wcry-ransomware#a2
https://isc.sans.edu/diary/22420
http://www.bbc.co.uk/news/health-39899646
https://arstechnica.com/information-technology/2017/05/nhs-ransomware-cyber-attack/
http://www.reuters.com/article/us-spain-cyber-idUSKB1N1881TJ?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-portugal-cyber-idUSKB1N1882AP?feedType=RSS&feedName=technologyNews
https://isc.sans.edu/diary/Massive+wave+of+ransomware+ongoing/22412
https://blog.malwarebytes.com/cybercrime/2017/05/wanacryptor-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
https://nakedsecurity.sophos.com/2017/05/12/wanna-decryptor-2-0-ransomware-attack-what-you-need-to-know/
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/86326385280673792
https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168
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/2017/05/13/wcry-knowns-and-unknowns/
http://www.darkreading.com/partner-perspectives/malwarebytes/wanacrypt0r-hits-worldwide/a/d-id/1328876
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://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware
https://nakedsecurity.sophos.com/2017/05/14/wannacry-benefits-from-unlearned-lessons-of-slammer-conficker/
http://blog.trendmicro.com/wannacry-reality-of-patching/
https://www.helpnetsecurity.com/2017/05/14/wannacry-ransomware/
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
https://krebsonsecurity.com/2017/05/microsoft-issues-wanacrypt-patch-for-windows-8-xp/
https://arstechnica.com/security/2017/05/wcry-is-so-mean-microsoft-issues-patch-for-3-unsupported-windows-versions/
http://thehackernews.com/2017/05/wannacry-ransomware-windows.html
https://threatpost.com/microsoft-releases-xp-patch-for-wannacry-ransomware/125671/
http://thehackernews.com/2017/05/wannacry-ransomware-cyber-attack.html
https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance
https://twitter.com/craiu/status/863718940870139904
https://www.renditioninfosec.com/2017/05/wanacrypt0r-worm-with-kill-switch-patched-out/
http://blog.checkpoint.com/2017/05/14/wannacry-paid-time-off/
The Computer Emergency Response Team of Mauritius (CERT-MU)

National Computer Board
7th Floor, Stratton Court,
La Poudriere Street, Port Louis

Tel: 210 5520
Fax: 208 0119

Website: www.cert-mu.org.mu

Incident Reporting
Hotline: 800 2378
Email: incident@cert.ncb.mu

Vulnerability Reporting
Email: vulnerability@cert.ncb.mu

For Queries
Email: contact@cert.ncb.mu

Subscription to Mailing Lists
Email: subscribe@cert.ncb.mu