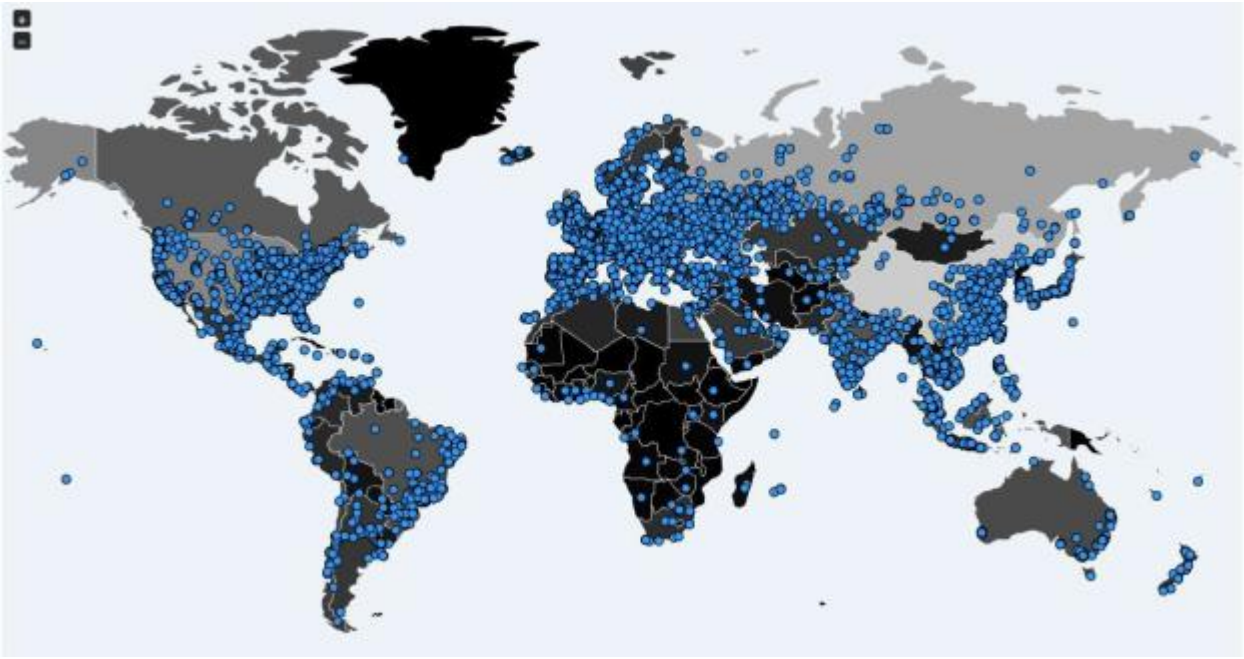
WannaCry Ransomware

Compiled by National KE-CIRT/CC

(15 May 2017)



Map of the attacks over the last 24 hours. Source: intel.malwaretech.com

Contents

Malware names 4
WannaCry – Summary of the Incident and Mitigation 4
Vulnerable systems 4
Worldwide infections 5
Prevention 6
Recovery 6
Technical analysis: Distribution 7
Technicalanalysis: Encryption 8
Embedded Password Protected Zip File 8
File Marker 10
UAC Prompt 12
Wana Decrypt0r 2.0 Lock Screen 12
Payment not made Response 13
Contact Us Form 13
Desktop Wallpaper 14
@Please_Read_Me@.txt Ransom Note 14
Kill-switch and kill-mutex 15
Malware versions 15
Recommendations 15
Malware indicators 17
SHA256 hashes 17
Command and Control servers (on the TOR network) 18
Kill-switch domains 18
Threat-Level Scoring 19
Threat Relevance Spheres 19
Malware analysis sources 20
International advisories 20
English newsreferences 20
WannaCry international outbreak 20
Microsoft's response 22
Alleged new malware version without kill-switch 22
Another alleged new malware versions without kill-switch 22
National KE-CIRT/CC news references 22
FIRST is the Forum of Incident Response and Security Teams. 22
ThaiCERT 22

Malware names

Wana Decrypt0r, WCry, WannaCry, WannaCrypt, and WanaCrypt0r

WannaCry – Summary of the Incident and Mitigation

On May 12, 2017, a cyber offensive, targeting a variety of organizations and institutions worldwide, disseminated ***WannaCry*** ransomware. The ransom note, written in different languages, demanded US$300-600 from the victims to decrypt their files. Infection cases were detected in multiple countries worldwide. The massive attack affected a wide variety of sectors, including health, government, industry, transportation, communications, financial institutions, among others. According to the reports, **more than 200,000 systems worldwide were infected in the attack**.[1] However, it appears that only one of every 1000 victims payed the ransom to the attackers.[2]

The ransomware is called Wanna Decrypt0r also known as WannaCry or WCRY. It encrypts users files using Advanced Encryption Standard (AES) and RSA encryption ciphers meaning the hackers can directly decrypt system files using a unique decryption key. Once one user has unwittingly installed this particular flavor of ransomware on their own Computer, it tries to spread to other computers in the same network. In order to do so, WanaCrypt0r uses a known vulnerability in the Operating System, jumping between Computers.

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:
<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>
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/>

[1] https://intel.malwaretech.com/botnet/wcrypt/?t=24h&bid=all
[2] https://twitter.com/x0rz/status/863478391554572290

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>

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>

Recovery

- *From BleepingComputer[2]:* Your best bet is to recover from backups, and if those do not exist, try a program like Shadow Explorer 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 here: How to recover files and folders using Shadow Volume Copies.
- 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.

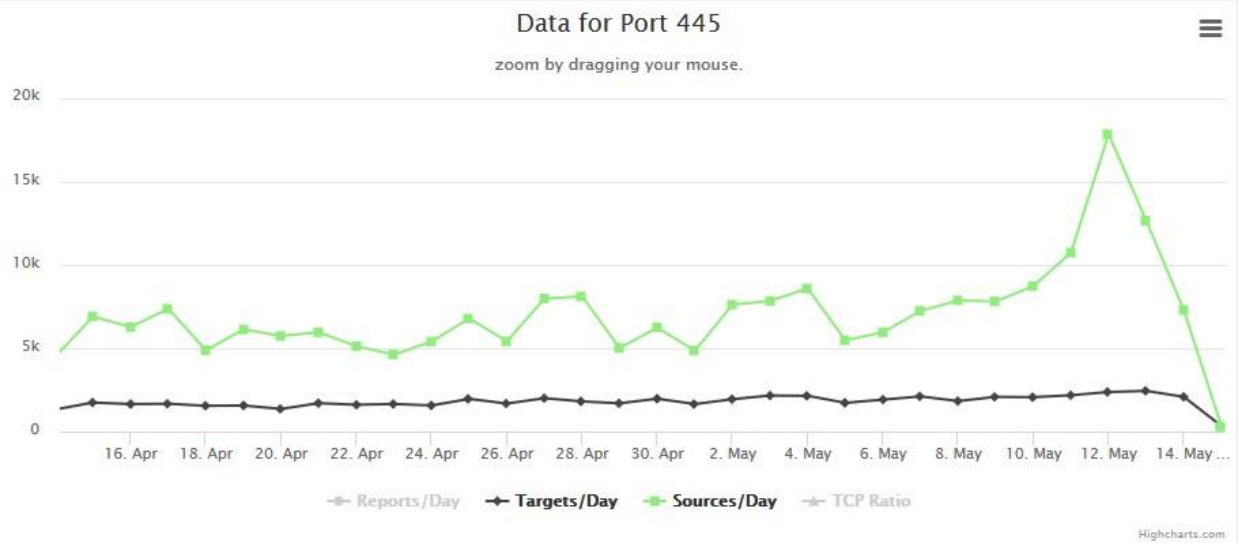
[1] It is Good Practice to filter all NetBIOS traffic (TCP/137, TCP/139, TCP/445, UDP/137 and UDP/138), but WannaCry only leverages port TCP/445.
[2] <https://www.bleepingcomputer.com/news/security/wana-decryptor-wanacrypt0r-technical-nose-dive/>

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.

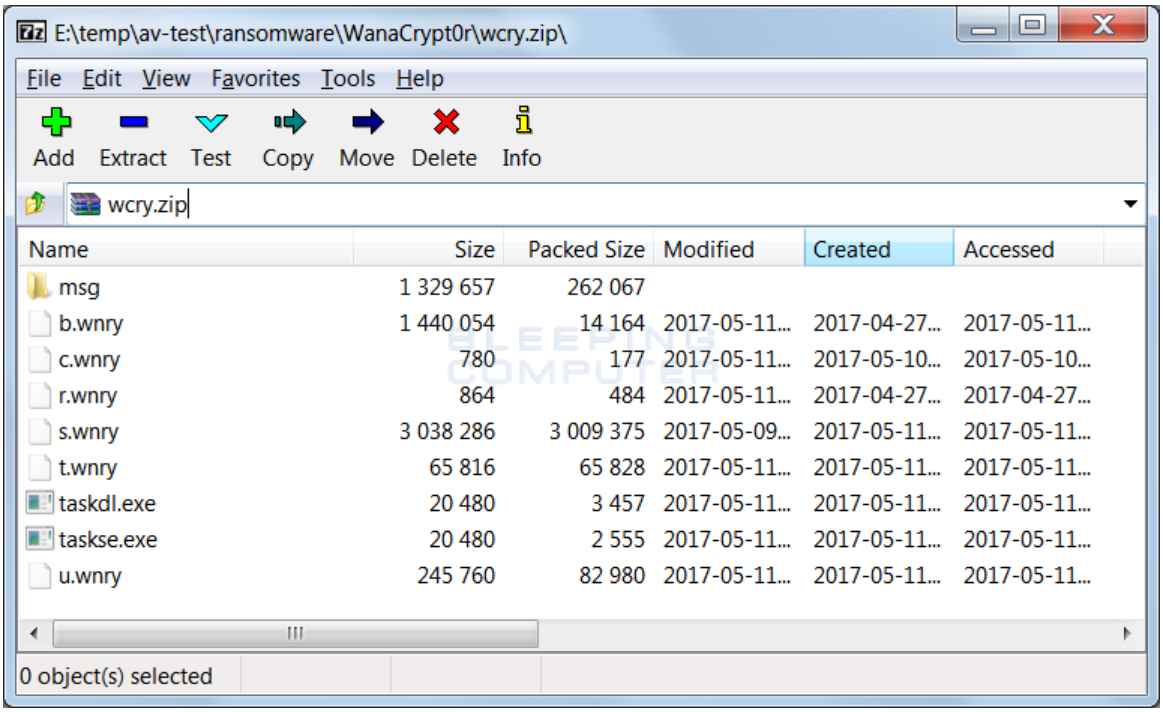


(From <https://isc.sans.edu/port.html?port=445>)

Technicalanalysis: Encryption

From BleepingComputer[3]:

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.



Embedded Password Protected Zip File

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, xxlvbrloxvriy2c5.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.

[3] <https://www.bleepingcomputer.com/news/security/wana-decryptor-wanacrypt0r-technical-nose-dive/>

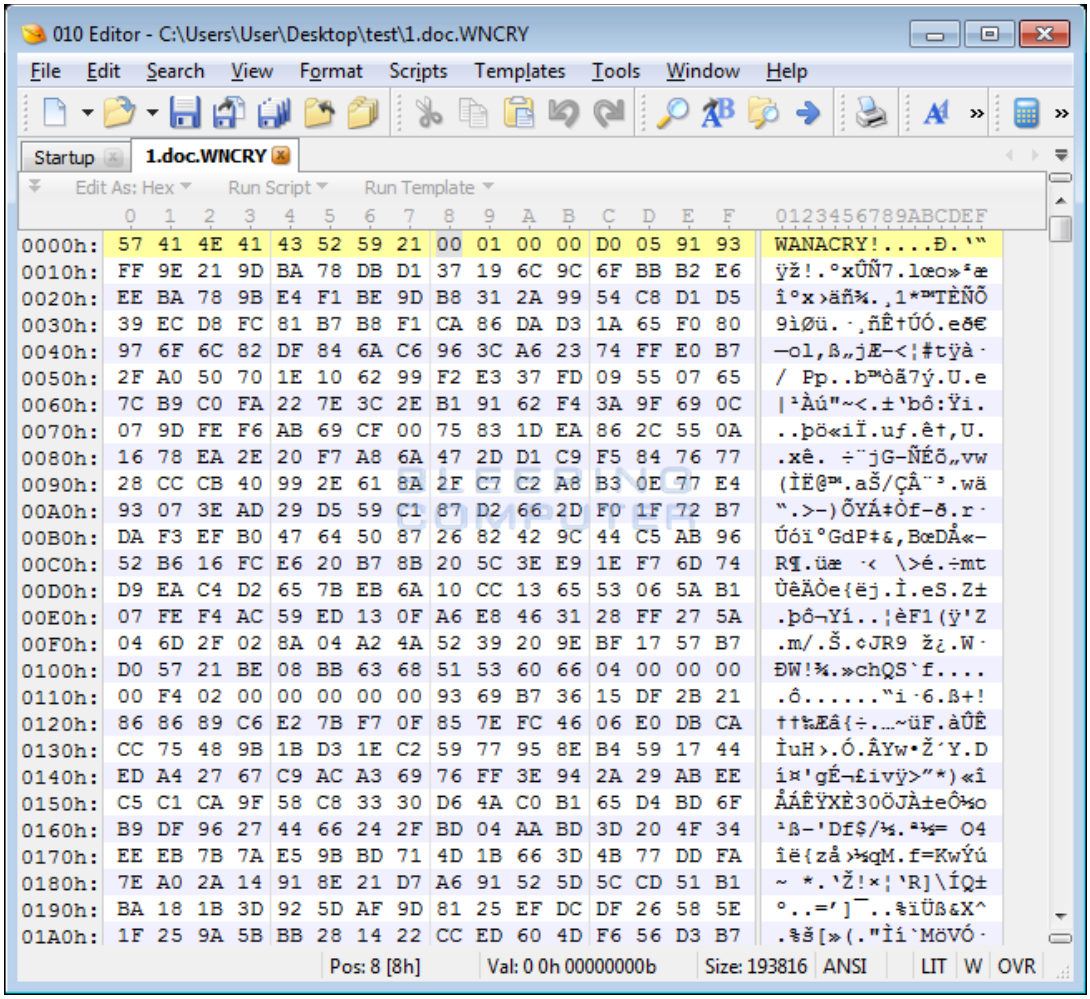
The commands that are executed to terminate the database and exchange server processes are:

```
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:

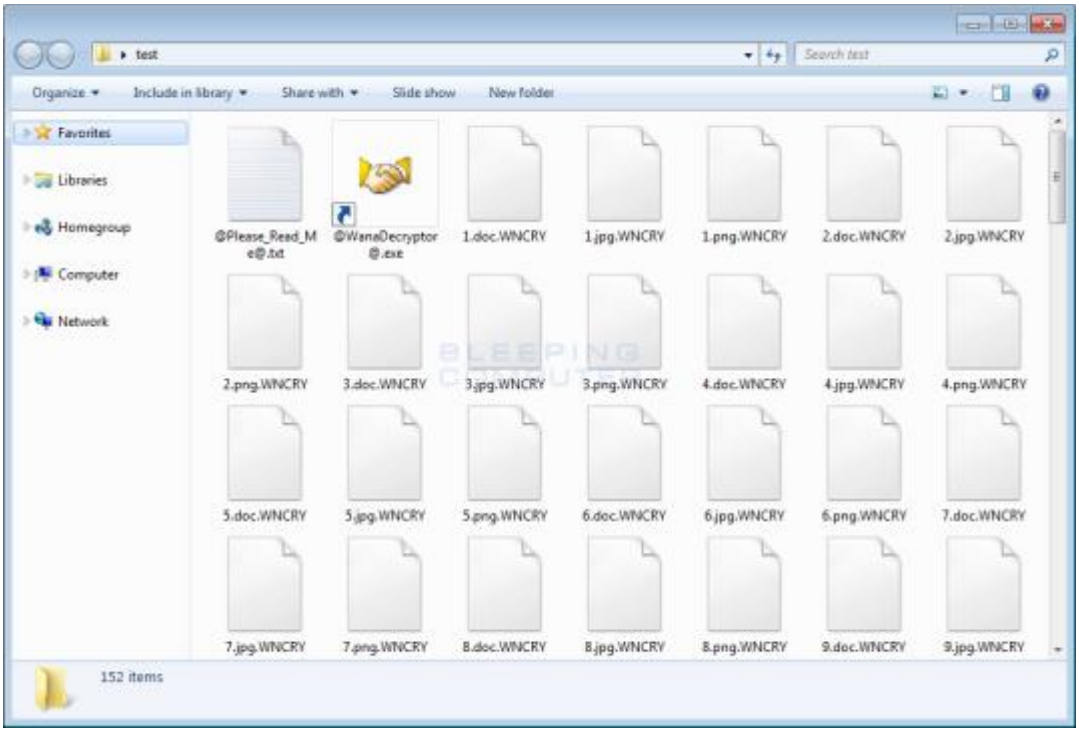
.der, .pfx, .key, .crt, .csr, .pem, .odt, .ott, .sxw, .stw, .uot, .max, .ods, .ots, .sxc, .stc, .dif, .slk, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm, .mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .frm, .myd, .myi, .ibd, .mdf, .ldf, .sln, .suo, .cpp, .pas, .asm, .cmd, .bat, .vbs, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .java, .jar, .class, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mkv, .flv, .wma, .mid, .djvu, .svg, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png, .bmp, .jpg, .jpeg,
.vcd, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .tbk, .PAQ, .ARC, .aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .hwp, .snt, .onetoc2, .dwg, .pdf, .wks, .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.

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



File Marker

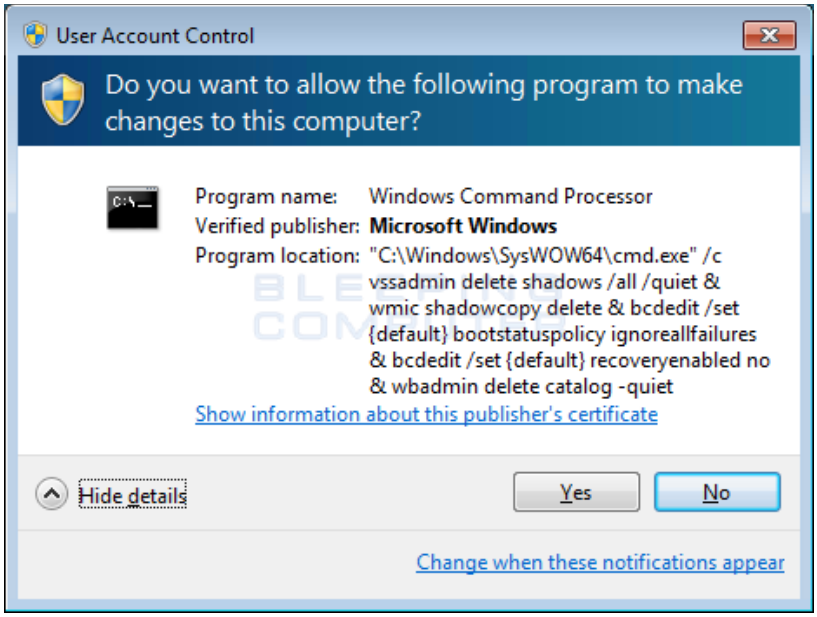
It will then append the **.WNCRY** extension to the encrypted file to denote that the file has been encrypted. For example, a file called **test.jpg** would be encrypted and have a new name of **test.jpg.WNCRY.**



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} 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.

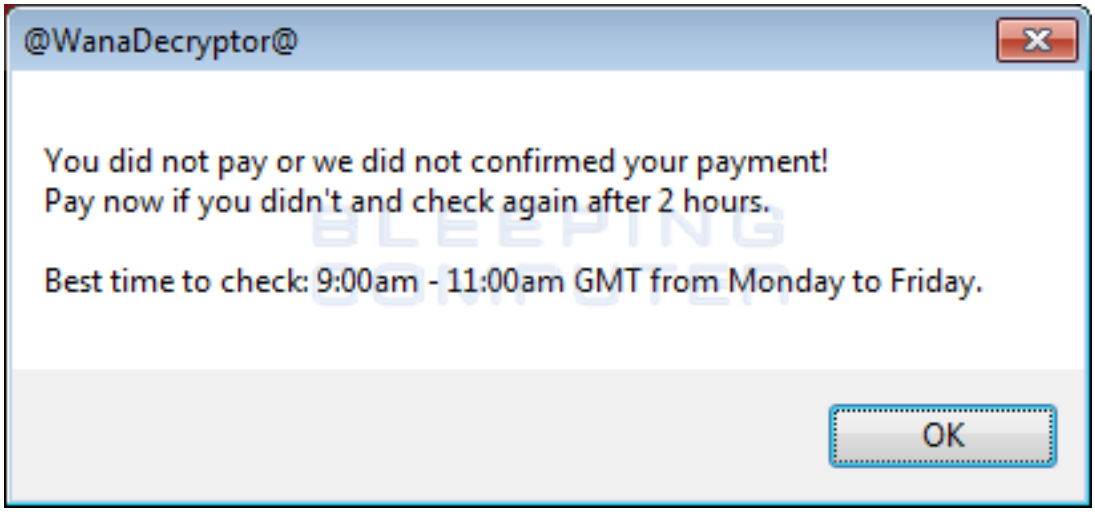


UAC Prompt

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.

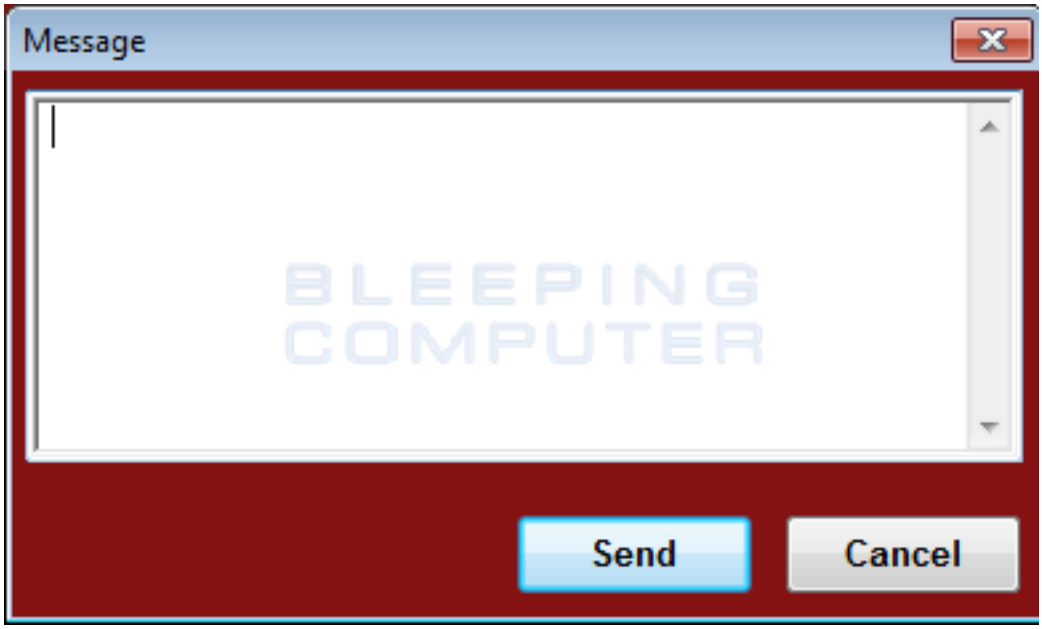
Wana Decrypt0r 2.0 Lock Screen

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.



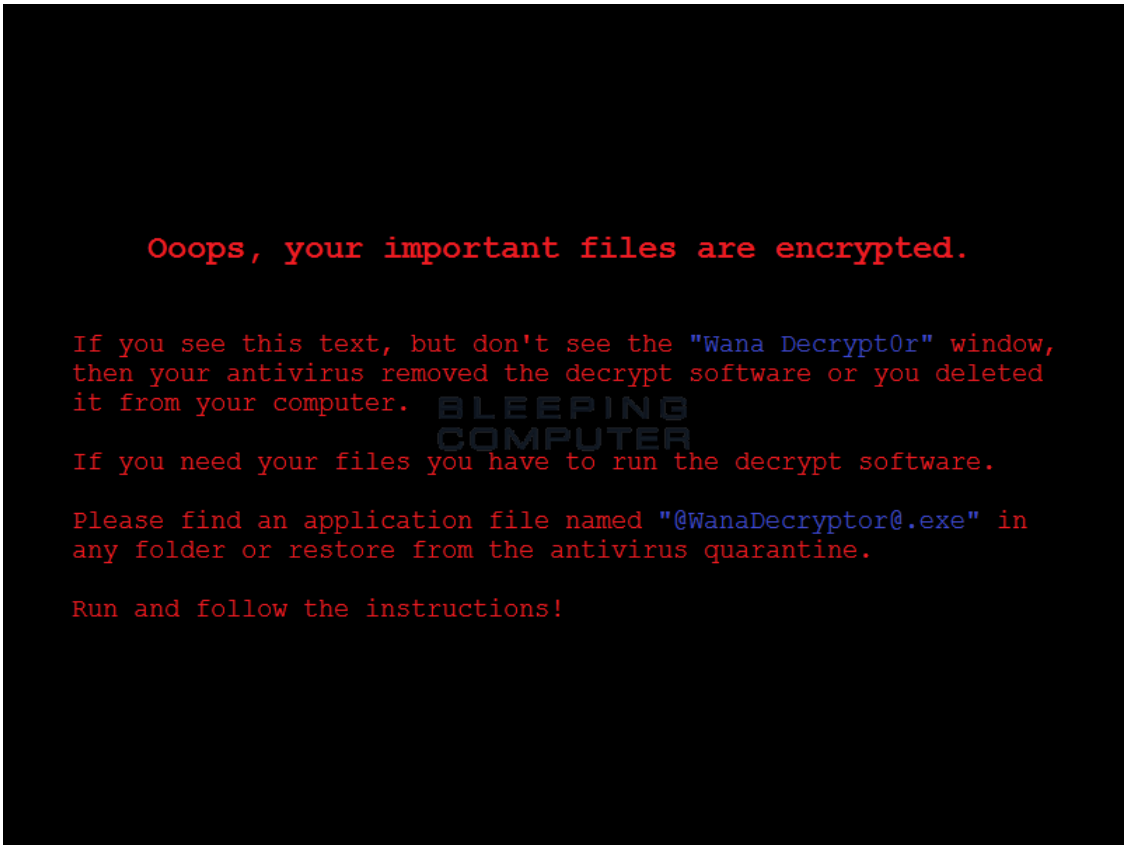
Payment not made Response

There are three hard coded bitcoin addresses in the WanaCrypt0r ransomware. These bitcoin addresses are 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94, 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw, and 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn. 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.



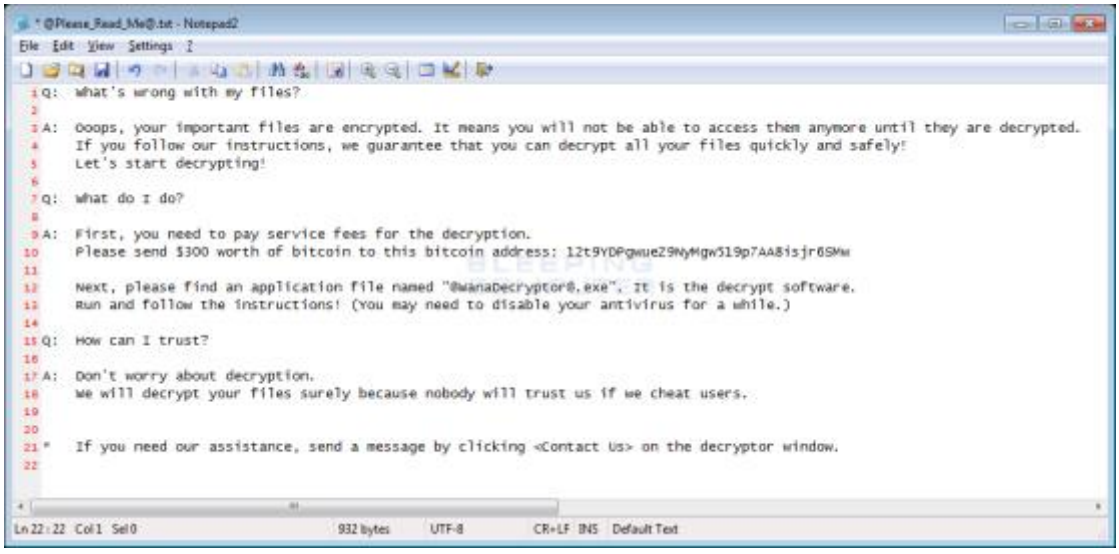
Contact Us Form

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



Desktop Wallpaper

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



@Please_Read_Me@.txt Ransom Note

Kill-switch and kill-mutex

- The malware stops if it finds the domain "www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]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. 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[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com" becomes
  "www[.]iffferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com"

A report appeared in the media about a new version (dubbed "2.0" in the media) on Saturday 13 May[4]. This version was said not to have the kill-switch domain. This was retracted as an error the next day[5].

A report appeared in the media about another new version (dubbed "#3" in the media) on Sunday 14 May[6]. This version was also said not to have a kill-switch domain.

Recommendations

1. Microsoft released a security update (MS17-010) for the above-mentioned vulnerability on March 14, 2017, as well as an additional patch for the Windows Server 2003, Windows 8, and Windows XP, on May 12, 2017:
   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
2. In the Firewall settings, it is important to ensure that the SMB services are not accessible from the Internet (TCP port 445, UDP ports 137, 138, and 139). In addition, it is recommended to disconnect systems that cannot be updated from external communication channels, or even disable the SMB when possible.
3. It is recommended to not block the traffic from the below-mentioned onion domain, which functions as a 'kill-switch' for the ransomware:
   (www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com).
4. Create the mutex "MsWinZonesCacheCounterMutexA" to stop the ransomware from executing.[3]
5. Do not open suspicious email attachments, and/or click on any links that were sent by unidentified senders.
6. If you use a Virus Scanner in your organization, make sure to implement the 'reconstruction'

[3] https://twitter.com/gN3mes1s/status/863149075159543808, https://blog.qualys.com/securitylabs/2017/05/12/how-to-rapidly-identify-assets-at-risk-to-wannacry-ransomware-and-eternalblue-exploit

definition in the filtering system in order to receive emails that contain office attachments.

7. You should consider blocking the option to run ‘macros’ on the organizational level through the GPO.
8. All files should be backed up on a regular basis, and preserve the updated backups on a drive disconnected from the network.
9. You should ensure that all the latest security updates are implemented on the organizational systems, and that they are synchronized.
10. You should limit the number of personnel with administrator privileges within the organization as much as possible.
11. You should examine file changes at end stations and at servers for the extensions .wnry/.wcry/.wncryt/.wncry and check if the files have been encrypted.
12. **Relevant YARA and Snort rules are attached to this document.**
13. **Relevant IOCs are also attached to this document.**

[4] <http://thehackernews.com/2017/05/wannacry-ransomware-cyber-attack.html>
[5] <https://twitter.com/craiu/status/863718940870139904> and <https://twitter.com/threatintel/status/863766609328050177>
[6] <http://news.softpedia.com/news/wannacry-ransomware-variant-with-no-kill-switch-discovered-515693.shtml>

Malware indicators

SHA256 hashes

593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af
5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
5d26835be2cf4f08f2beeff301c06d05035d0a9ec3afacc71dff22813595c0b9
62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7
7108d6793a003695ee8107401cfb17af305fa82ff6c16b7a5db45f15e5c9e12d
72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
76a3666ce9119295104bb69ee7af3f2845d23f40ba48ace7987f79b06312bbdf
78e3f87f31688355c0f398317b2d87d803bd87ee3656c5a7c80f0561ec8606df
7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff
7e369022da51937781b3efe6c57f824f05cf43cbd66b4a24367a19488d2939e4
85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
97ebce49b14c46bebc9ec2448d00e1e397123b256e2be9eba5140688e7bc0ae6
9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
9cc32c94ce7dc6e48f86704625b6cdc0fda0d2cd7ad769e4d0bb1776903e5a13
9e60269c5038de8956a1c6865ebea8627a440a6e839f61e940a8d5f2c6ea4982
9fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b50977
a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
a3900daf137c81ca37a4bf10e9857526d3978be085be265393f98cb075795740
a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c
b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
b66db13d17ae8bcaf586180e3dcd1e2e0a084b6bc987ac829bbff18c3be7f8b4
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
ca29de1dc8817868c93e54b09f557fe14e40083c0955294df5bd91f52ba469c8
d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa
d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127
dff26a9a44baa3ce109b8df41ae0a301d9e4a28ad7bd7721bbb7ccd137bfd696
e14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079
e18fdd912dfe5b45776e68d578c3af3547886cf1353d7086c8bee037436dff4b
e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96
eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
eeb9cd6a1c4b3949b2ff3134a77d6736b35977f951b9c7c911483b5caeb1c1fb
f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494

f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a

Command and Control servers (on the TOR network)

57g7spgrzlojinas.onion

76jdd2ir2embyv47.onion

cwwnhwhlz52ma.onion

gx7ekbenv2riucmf.onion

sqjolphimrr7jqw6.onion

xxlvbrloxvriy2c5.onion

Kill-switch domains

Do not block these domains, but only monitor.

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

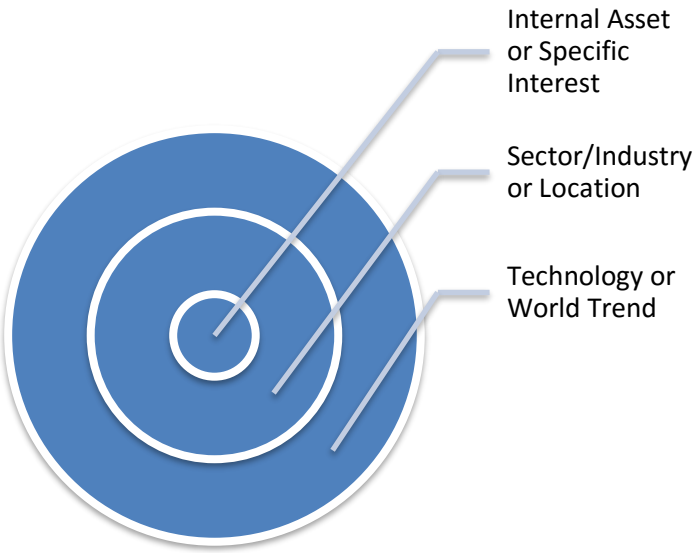
Threat-Level Scoring

Cyber threat levels are rated in accordance with the Multi-State Information Analysis Center (MS-ISAC) threat-level system:

Threat Level	Threat Description
Severe	Specific risk of hacking, virus, or other malicious activity.
High	High risk of malicious activity that targets or compromises core infrastructure.
Elevated	Significant risk due to increased malicious activity that compromises systems or diminishes service.
Guarded	General risk of increased hacking, virus or other malicious activity.
Low	No unusual activity exists beyond normal concern for malicious activity.

Threat Relevance Spheres

Cyber threat relevance spheres depict the understanding of the relationship between the reported threats and the customer's interests:



Malware analysis sources

<https://www.bleepingcomputer.com/news/security/wana-decryptor-wanacrypt0r-technical-nose-dive/>
<http://blog.talosintelligence.com/2017/05/wannacry.html>
<https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/>
<https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/>
<https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html>
<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/>

International advisories

<https://www.ncsc.gov.uk/news/statement-international-ransomware-cyber-attack>
<https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported>
<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://auscert.org.au/resources/blog/ongoing-global-ransomware-attack>
<https://www.csa.gov.sg/singcert/news/advisories-alerts/wanacrypt0r-aka-wannacry--what-you-need-to-know-and- the-actions-to-take>
<https://circl.lu/pub/tr-41/#proactive-measures-for-the-wannacry-ransomware>

English newsreferences

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://digital.nhs.uk/article/1491/Statement-on-reported-NHS-cyber-attack>
<https://www.infosecurity-magazine.com/news/massive-ransomware-attack-hits-nhs/>
<https://arstechnica.com/information-technology/2017/05/nhs-ransomware-cyber-attack/>
<https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/>
<https://www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid- massive-ransomware-outbreak/>
<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>
<http://www.reuters.com/article/us-britain-security-hospitals-fedex-idUSKBN1882UJ?feedType=RSS&feedName=technologyNews>
<http://www.reuters.com/article/us-portugal-cyber-idUSKBN1882AP?feedType=RSS&feedName=technologyNews>
<https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0>
<https://www.dhs.gov/news-releases/press-releases>
<http://www.csoonline.com/article/3196237/security/a-ransomware-attack-is-spreading-worldwide-using-alleged-nsa-exploit.html>
<https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over- 50000-attacks-so-far-today>
<https://isc.sans.edu/diary/Massive+wave+of+ransomware+ongoing/22412>

<https://www.cyberscoop.com/unprecedented-ransomware-outbreak-spreads-across-england-and-spain/>
<http://www.darkreading.com/attacks-breaches/wannacry-rapidly-moving-ransomware-attack-spreads-to-74-countries/d/d-id/1328874>
<https://www.infosecurity-magazine.com/news/nhs-ransomware-attack-goes-global/>
<https://www.bleepingcomputer.com/news/security/wana-decrypt0r-ransomware-using-nsa-exploit-leaked-by- shadow-brokers-is-on-a-rampage/>
<https://blog.malwarebytes.com/cybercrime/2017/05/wanacrypt0r-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-decrypter-2-0-ransomware-attack-what-you-need-to-know/>
<http://researchcenter.paloaltonetworks.com/2017/05/palo-alto-networks-protections-wanacrypt0r-attacks/>
<https://arstechnica.com/security/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/>
<http://news.softpedia.com/news/global-ransomware-attack-takes-down-british-nhs-company-networks-more-515677.shtml>
<http://thehackernews.com/2017/05/wannacry-ransomware-unlock.html>
<https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/>
<https://threatpost.com/leaked-nsa-exploit-spreading-ransomware-worldwide/125654/>
<http://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcry-ransomware-attack-hits-various-countries/>
<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/rain-1/989428fa5504f378b993ee6efbc0b168>
<http://www.bangkokpost.com/news/world/1248938/asia-assesses-ransomware-damage>
<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/>
<https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack>
<https://www.bleepingcomputer.com/news/security/wana-decrypt0r-ransomware-outbreak-temporarily-stopped-by-accidental-hero-/>
<http://news.softpedia.com/news/wannacry-ransomware-spread-halted-by-hero-researcher-515690.shtml>
<https://securingtomorrow.mcafee.com/executive-perspectives/wannacry-old-worms-new/>
<http://www.mailguard.com.au/blog/global-cyber-attack-wannacry-ransomware-creates-havoc>
<http://www.darkreading.com/partner-perspectives/malwarebytes/wanacrypt0r-hits-worldwide-/a/d-id/1328876>
<https://www.itnews.com.au/news/british-hospitals-telefonica-hit-by-ransomware-with-nsa-exploit-461566>
<http://www.reuters.com/article/us-renault-cybercrime-idUSKBN1890AK?feedType=RSS&feedName=technologyNews>
<http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/index.html>
<https://www.helpnetsecurity.com/2017/05/12/massive-ransomware-campaign/>
<https://blog.fox-it.com/2017/05/13/faq-on-the-wanacry-ransomware-outbreak/>
<https://www.itnews.com.au/news/wannacrypt-ransomware-what-you-need-to-know-461717>
<https://www.bleepingcomputer.com/news/security/honeypot-server-gets-infected-with-wannacry-ransomware-6- times-in-90-minutes/>
<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>
<https://securityintelligence.com/wannacry-ransomware-spreads-across-the-globe-makes-organizations-wanna-cry- about-microsoft-vulnerability/>
<http://news.softpedia.com/news/europol-warns-wannacry-spread-to-go-up-on-monday-515694.shtml>
<https://www.theregister.co.uk/2017/05/14/microsoft_to_spooks_wannacrypt_was_inevitable_quit_hoarding/>
<https://www.bleepingcomputer.com/news/government/microsoft-exec-blames-wannacry-ransomware-on-nsa-vulnerability-hoarding-program/>

Microsoft's response

<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/>
<http://www.csoonline.com/article/3196725/security/microsoft-patches-windows-xp-and-server-2003-due-to-wannacrypt-attacks.html>
<https://www.infosecurity-magazine.com/news/microsoft-xp-patch-wannacry/>
<https://www.itnews.com.au/news/microsoft-releases-wannacrypt-patch-for-windows-xp-server-2003-461640>
<https://www.bleepingcomputer.com/news/security/microsoft-releases-patch-for-older-windows-versions-to-protect- against-wana-decrypt0r/>
<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/>

Alleged new malware version without kill-switch

Note: this research has been retracted. No version without kill-switch has been found yet.
<http://thehackernews.com/2017/05/wannacry-ransomware-cyber-attack.html>
<https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance>
<https://motherboard.vice.com/en_us/article/round-two-wannacry-ransomware-that-struck-the-globe-is-back>
<https://twitter.com/craiu/status/863718940870139904>

Another alleged new malware versions without kill-switch

<http://news.softpedia.com/news/wannacry-ransomware-variant-with-no-kill-switch-discovered-515693.shtml>

National KE-CIRT/CC news references

FIRST is the Forum of Incident Response and Security Teams.
ThaiCERT

The National Cybersecurity Centre (NCC) is Kenya's national cyber crime management trusted point of contact, and is globally recognized. Members of the public are therefore advised to contact National Cybersecurity Centre (NCC) via the email address incidents@ke-cirt.go.ke or through the dedicated hotlines +254-703-042700/+254-730-172700, to report such incidences or seek advice on potential cyber threat.