

CURRENT ACTIVITIES**Wannacry / WannaCrypt Ransomware - CRITICAL ALERT**

Original Issue Date: May 13, 2017

Updated: May 14, 2017

It has been reported that a new ransomware named as "Wannacry" is spreading widely. Wannacry encrypts the files on infected Windows systems. This ransomware spreads by using a vulnerability in implementations of Server Message Block (SMB) in Windows systems. This exploit is named as ETERNALBLUE.

The ransomware called WannaCrypt or WannaCry encrypts the computer's hard disk drive and then spreads laterally between computers on the same LAN. The ransomware also spreads through malicious attachments to emails.

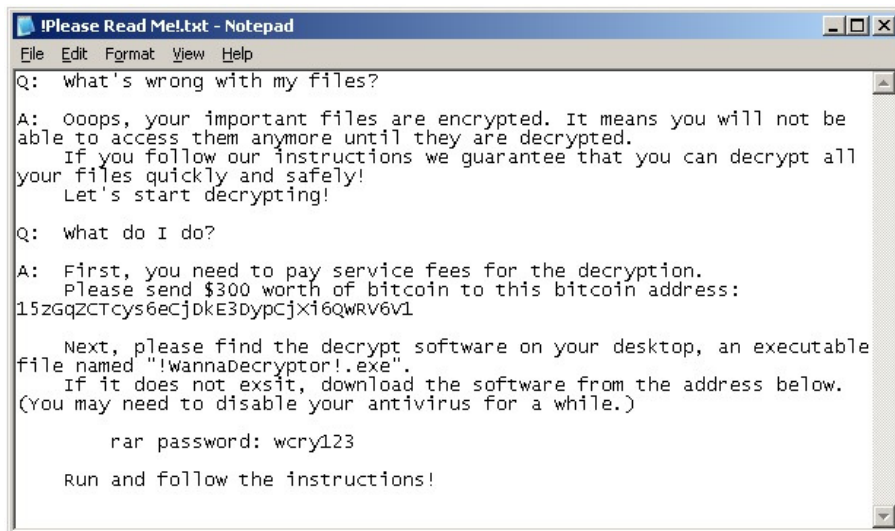
In order to prevent infection, users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin [MS17-010](#).

After infecting, this Wannacry ransomware displays following screen on infected system:



Source: Symantec

It also drops a file named !Please Read Me!.txt which contains the text explaining what has happened and how to pay the ransom.



```
IPlease Read Me.txt - Notepad
File Edit Format View Help
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 exist, 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!
```

Source: Symantec

WannaCry encrypts files with the following extensions, appending .WCry to the end of the file name:

- .lay6
- .sqlite3
- .sqlitedb
- .accdb
- .java
- .class
- .mpeg
- .djvu
- .tiff
- .backup
- .vmdk
- .sldm
- .sldx
- .potm
- .potx
- .ppam
- .ppsx
- .ppsm
- .pptm
- .xltm
- .xltx
- .xlsb
- .xlsm
- .dotx
- .dotm
- .docm
- .docb
- .jpeg
- .onetoc2
- .vsdx
- .pptx
- .xlsx
- .docx

The file extensions that the malware is targeting contain certain clusters of formats including:

1. Commonly used office file extensions (.ppt, .doc, .docx, .xlsx, .sxi).
2. Less common and nation-specific office formats (.sxw, .odt, .hwp).
3. Archives, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv)
4. Emails and email databases (.eml, .msg, .ost, .pst, .edb).
5. Database files (.sql, .accdb, .mdb, .dbf, .odb, .myd).
6. Developers' sourcecode and project files (.php, .java, .cpp, .pas, .asm).
7. Encryption keys and certificates (.key, .pfx, .pem, .p12, .csr, .gpg, .aes).
8. Graphic designers, artists and photographers files (.vsd, .odg, .raw, .nef, .svg, .psd).
9. Virtual machine files (.vmx, .vmdk, .vdi).

Indicators of compromise:

Ransomware is writing itself into a random character folder in the "ProgramData" folder with the file name of "tasksche.exe" or in "C:\Windows\" folder with the file-name "mssecsvc.exe" and "tasksche.exe".

Ransomware is granting full access to all files by using the command:
 Icacls . /grant Everyone:F /T /C /Q

Using a batch script for operations:
 176641494574290.bat

hashes for WANNACRY ransomware:

```
4fef5e34143e646dbf9907c4374276f5
5bef35496fcbdbe841c82f4d1ab8b7c2
775a0631fb8229b2aa3d7621427085ad
7bf2b57f2a205768755c07f238fb32cc
7f7ccaa16fb15eb1c7399d422f8363e8
8495400f199ac77853c53b5a3f278f3e
84c82835a5d21bbc75a61706d8ab549
86721e64ffbd69aa6944b9672bcabb6d
8dd63adb68ef053e044a5a2f46e0d2cd
b0ad5902366f860f85b892867e5b1e87
d6114ba5f10ad67a4131ab72531f02da
db349b97c37d22f5ea1d1841e3c89eb4
e372d07207b4da75b3434584cd9f3450
f529f4556a5126bba499c26d67892240
```

- *use endpoint protection/antivirus solutions to detect these files and remove the same*

Network Connections

The malware use TOR hidden services for command and control. The list of .onion domains inside is as following:

- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinias.onion
- Xxlvbrloxyvriy2c5.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52maq7.onion
- sqjolphimrr7jqw6.onion

Note: For update on latest Indicators of Compromises, please see references to security vendors given in references section

Specific Countermeasures to prevent Wannacry/WannaCrypt Ransomware:

Users and administrators are advised to take the following preventive measures to protect their computer networks from ransomware infection/ attacks:

- In order to prevent infection users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin [MS17-010](#).
- Microsoft Patch for Unsupported Versions such as Windows XP,Vista,Server 2003, Server 2008 etc.
<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598>
- To prevent data loss Users & Organisations are advised to take backup of Critical Data
- Block SMB ports on Enterprise Edge/perimeter network devices [UDP 137, 138 and TCP 139, 445] or Disable SMBv1.
<https://support.microsoft.com/en-us/help/2696547>
- Apply following signatures/rules at IDS/IPS alert tcp \$HOME_NET 445 -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:2;) (<http://docs.emergingthreats.net/bin/view/Main/2024218>)

```
alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Request (set)";
flow:to_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 18 07 c0|"; depth:16; fast_pattern;
content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:set,ETPRO.ETERNALBLUE; flowbits:noalert;
classtype:trojan-activity; sid:2024220; rev:1;)
```

```
alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response";
flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 98 07 c0|"; depth:16; fast_pattern;
content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE;
```

```
classtype:trojan-activity; sid:2024218; rev:1;)
```

- **Yara:**

```
rule wannacry_1 : ransom
{
  meta:
  author = "Joshua Cannell"
  description = "WannaCry Ransomware strings"
  weight = 100
  date = "2017-05-12"

  Strings:
  $s1 = "Ooops, your files have been encrypted!" wide ascii nocase
  $s2 = "Wanna Decryptor" wide ascii nocase
  $s3 = ".wcry" wide ascii nocase
  $s4 = "WANNACRY" wide ascii nocase
  $s5 = "WANACRY!" wide ascii nocase
  $s7 = "icacls . /grant Everyone:F /T /C /Q" wide ascii nocase

  Condition:
  any of them
}

rule wannacry_2{
  meta:
  author = "Harold Ogden"
  description = "WannaCry Ransomware Strings"
  date = "2017-05-12"
  weight = 100
  strings:
  $string1 = "msg/m_bulgarian.wnry"
  $string2 = "msg/m_chinese (simplified).wnry"
  $string3 = "msg/m_chinese (traditional).wnry"
  $string4 = "msg/m_croatian.wnry"
  $string5 = "msg/m_czech.wnry"
  $string6 = "msg/m_danish.wnry"
  $string7 = "msg/m_dutch.wnry"
  $string8 = "msg/m_english.wnry"
  $string9 = "msg/m_filipino.wnry"
  $string10 = "msg/m_finnish.wnry"
  $string11 = "msg/m_french.wnry"
  $string12 = "msg/m_german.wnry"
  $string13 = "msg/m_greek.wnry"
  $string14 = "msg/m_indonesian.wnry"
  $string15 = "msg/m_italian.wnry"
  $string16 = "msg/m_japanese.wnry"
  $string17 = "msg/m_korean.wnry"
  $string18 = "msg/m_latvian.wnry"
  $string19 = "msg/m_norwegian.wnry"
  $string20 = "msg/m_polish.wnry"
  $string21 = "msg/m_portuguese.wnry"
  $string22 = "msg/m_romanian.wnry"
  $string23 = "msg/m_russian.wnry"
  $string24 = "msg/m_slovak.wnry"
  $string25 = "msg/m_spanish.wnry"
  $string26 = "msg/m_swedish.wnry"
  $string27 = "msg/m_turkish.wnry"
  $string28 = "msg/m_vietnamese.wnry"
  condition:
  any of ($string*)
}
```

Best practices to prevent ransomware attacks:

- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser
- Restrict execution of powershell /WSCRIPT in enterprise environment Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled. script block logging, and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.

- Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA%, %PROGRAMDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations. Enforce application whitelisting on all endpoint workstations.
- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- Disable macros in Microsoft Office products. Some Office products allow for the disabling of macros that originate from outside of an organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can block macros originating from the Internet from running.
- 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.
- Maintain updated Antivirus software on all systems
- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level anti-exploitation tools.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
- Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.
- Disable remote Desktop Connections, employ least-privileged accounts.
- Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems, Check regularly for the integrity of the information stored in the databases.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations.
- Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption.
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers from CERT-IN empaneled auditors. Repeat audits at regular intervals.
- Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to CERT-In and Law Enforcement agencies.

Generic Prevention Tools:

- Sophos: Hitman.Pro
<https://www.hitmanpro.com/en-us/surfright/alert.aspx>
- Bitdefender Anti-Crypto Vaccine and Anti-Ransomware (discontinued)
<https://labs.bitdefender.com/2016/03/combo-crypto-ransomware-vaccine-released/>
- Malwarebytes Anti-Ransomware(formally Crypto Monitor)
<https://blog.malwarebytes.com/malwarebytes-news/2016/01/introducing-the-malwarebytes-anti-ransomware-beta/>
- Trendmicro Ransomware Screen Unlocker tool:
<https://esupport.trendmicro.com/en-us/home/pages/technical-support/1105975.aspx>
- Microsoft Enhanced mitigation and experience toolkit(EMET)
<https://www.microsoft.com/en-us/download/details.aspx?id=50766>

References

<https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/>
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Ransom_Wana.A
<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://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598>
<https://technet.microsoft.com/library/security/MS17-010>
<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks>
<https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware>
<https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/>
<http://blog.talosintelligence.com/2017/05/wannacry.html>
http://www.cyberswachhtakendra.gov.in/alerts/wannacry_ransomware.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
 Phone: +91-11-24368572

Postal Address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India