

CRITICAL ALERT

Wannacry / WannaCrypt Ransomware

**Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India**

- Ransomware is a malware that encrypts contents on infected systems and demands payment in bitcoins.

- **WannaCry / WannaCrypt** encrypts the files on infected Windows systems.
- **There are two key components – a worm and a ransomware package**
- It spreads laterally between computers on the same LAN by using a vulnerability in implementations of **Server Message Block (SMB) in Windows systems.**
- It also spreads through malicious email attachments.
- This exploit is named as **ETERNALBLUE.**
- Initial ransom was of \$300 USD but the group is increasing the ransom demands upto \$600 in Bitcoin.

After infecting, Wannacry ransomware displays the following screen on infected system



An image used to replace user's desktop wallpaper as follows:

Oops, your important files are encrypted.

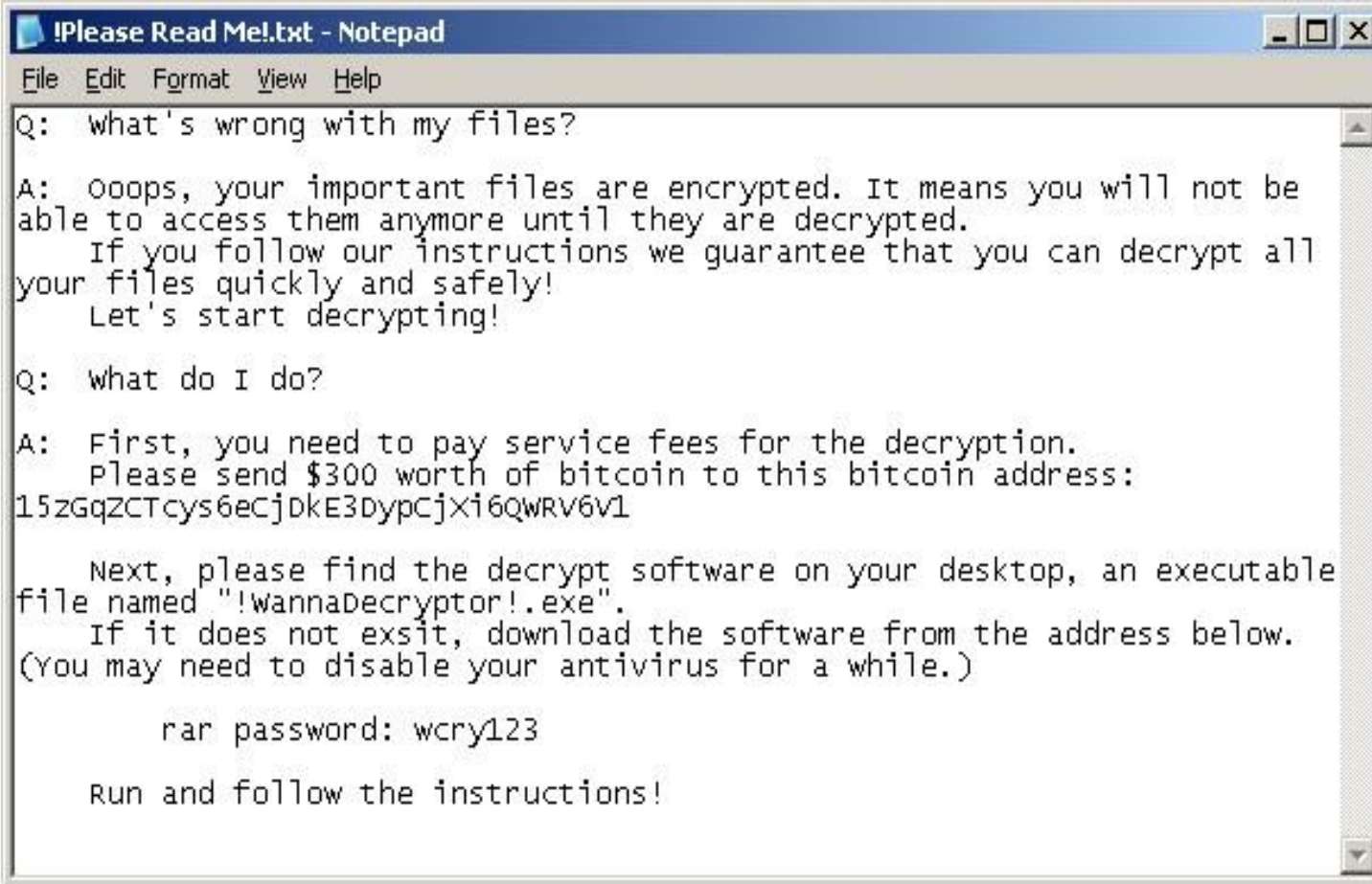
If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

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!

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



```
!Please 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!
```

The Wannacry / WannaCrypt Ransomware drops “user manuals” in different languages:

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

The ransomware encrypts the targeted files with the following extensions:

.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .ott, .sxw, .stw, .uot, .3ds, .max, .3dm, .ods, .ots, .sxc, .stc, .dif, .slk, .wb2, .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, .ps1, .vbs, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .3gp, .mkv, .3g2, .flv, .wma, .mid, .m3u, .m4u, .djvu, .svg, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png, .bmp, .jpg, .jpeg, .vcd, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .tbk, .bz2, .PAQ, .ARC, .aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .602, .hwp, .snt, .onetoc2, .dwg, .pdf, .wk1, .wks, .123, .rtf, .csv, .txt, .vsdx, .vsd, .edb, .eml, .msg, .ost, .pst, .potm, .potx, .ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltn, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotx, .dotm, .dot, .docm, .docb, .docx, .doc

It appends .WCRY to the end of the file name

The file extensions ransomware is targeting certain clusters of file formats :

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

Indicators of compromise (IoC)

- 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

Content of the VBScript

```
@echo off
echo SET ow = WScript.CreateObject("WScript.Shell")> m.vbs
echo SET om = ow.CreateShortcut("C:\Users\ADMINI~1\AppData\Local\Temp\@WanaDecryptor@.exe.lnk")>> m.vbs

echo om.TargetPath = "C:\Users\ADMINI~1\AppData\Local\Temp\@WanaDecryptor@.exe">> m.vbs

echo om.Save>> m.vbs
cscript.exe //nologo m.vbs
del m.vbs
del /a %0

m.vbs

SET ow = WScript.CreateObject("WScript.Shell")
SET om = ow.CreateShortcut("C:\Users\ADMINI~1\AppData\Local\Temp\@WanaDecryptor@.exe.lnk")
om.TargetPath = "C:\Users\ADMINI~1\AppData\Local\Temp\@WanaDecryptor@.exe"
om.Save
```

Measures 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**
<https://technet.microsoft.com/library/security/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>

- Restrict TCP port 445 traffic to where it is absolutely needed using router ACLs
- Use private VLANs if your edge switches support this feature
- Use host based firewalls to limit communication on TCP 445, especially between workstations

For Users

- Deploy antivirus protection
- Block spam
- 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.
- 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.
- Disable macros in Microsoft Office products.

For Organisations

- 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.
- Deploy 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.

Detailed countermeasures, best practices, prevention tools, IoCs, signatures/rules at IDS/IPS and Yara rules are mentioned on our website

http://www.cyberswachhtakendra.gov.in/alerts/wannacry_ransomware.html



← → 🔄 ⓘ www.cyberswachhtakendra.gov.in/alerts/wannacry_ransomware.html 🔍 ☆

certin Handling Computer Security Incidents

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Ministry of Electronics and Information Technology
Government of India

Home About Us CERT-In Security Tools Alerts Security Best Practices Partners FAQ's Contact Us

CRITICAL ALERT Original Issue Date: May 13, 2017
Virus Type: Ransomware

Wannacry/ WannaCrypt Ransomware

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.
<https://technet.microsoft.com/library/security/MS17-010>

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



Oops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure, We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking «Decrypt». But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click «About Bitcoin». Please check the current price of Bitcoin and buy some bitcoins. For more information, click «How to buy bitcoins». And send the correct amount to the address specified in this window. After your payment, click «Check Payment». Best time to check: 9:00am - 11:00am each day. «About Us»

Payment will be raised on 10/10/17 11:00:00
Time Left: 00:00:00

Your files will be lost on 10/10/17 11:00:00
Time Left: 00:00:00

If the system is infected by Wannacry / WannaCrypt Ransomware

- Immediately isolate the system from network
- Run cleanup tools mentioned on our website to disinfect the same
- Preserve the data even if it is encrypted
- Report incident to CERT-In and local law enforcement agency
- For any further questions, send email to

incident@cert-in.org.in

Thank you

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

Toll Free Phone: +91-1800-11-4949

Toll Free Fax: +91-1800-11-6969

www.cert-in.org.in, www.cyberswachhtakendra.gov.in