From MyCERT Advisories

MyCERT Alert – WannaCry Ransomware

Introduction

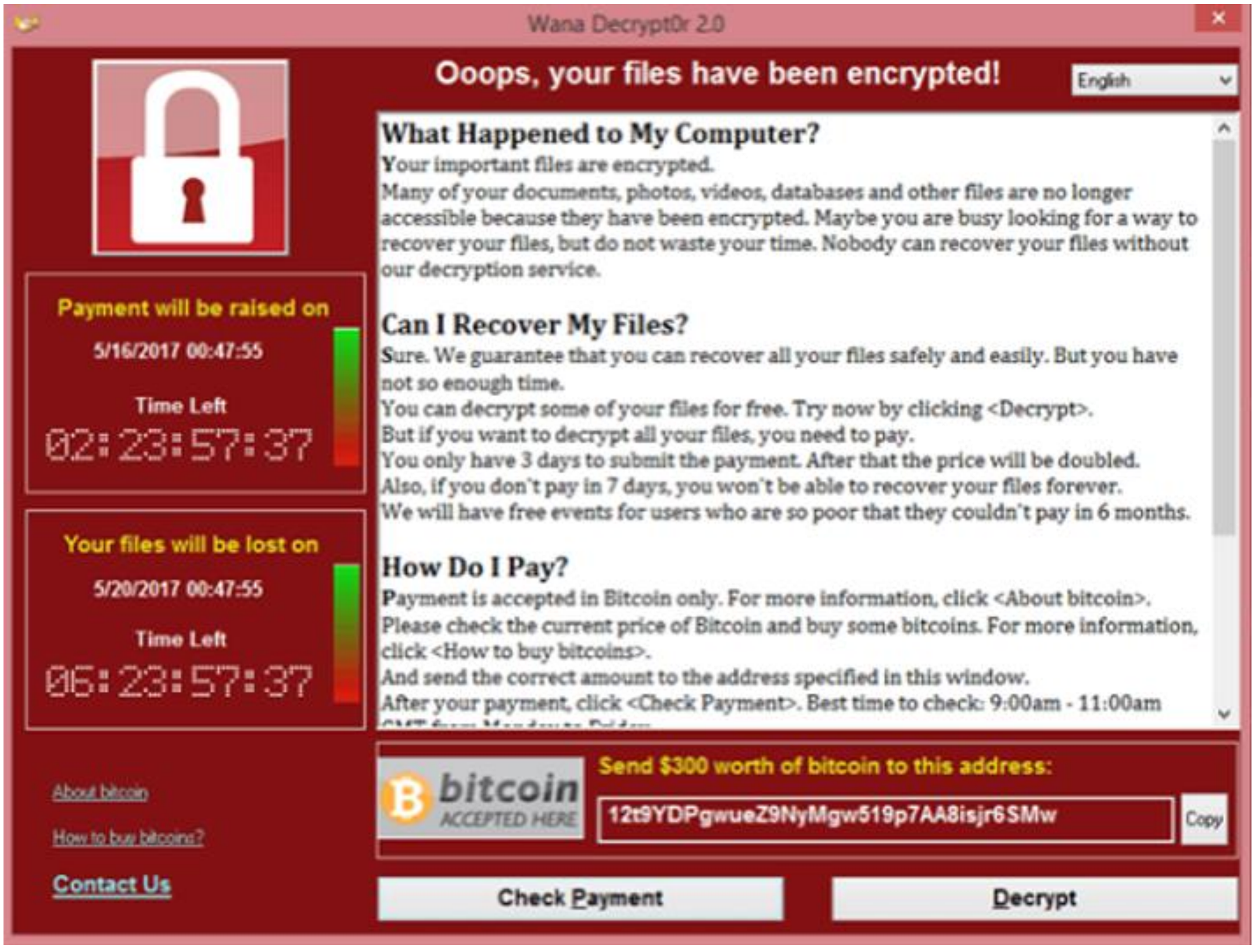
- **MyCERT** is aware of the outbreak of a ransomware called as WannaCry.
- This ransomware is also referenced online under various names – WCry, WanaCryptor, WannaCrypt or Wana Decryptor.
- Ransomware is type of malware that infects computing platform and restricts users' access until an amount of ransom is paid in order to unlock it.
- Victims got infected through emails that contains malicious attachment.
- Once the ransomware infected a system, the malware scans and infects other vulnerable systems within the network.

It exploits a vulnerability found in Windows, known as EternalBlue, that Microsoft patched in March (MS17-010). The vulnerability is in the Windows Server Message Block (SMB) service. https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Impact

- Files on infected computer are encrypted and the owner is unable to access the files until a ransom of $300 worth of Bitcoin is paid.
- Individuals and organizations are discouraged from paying the ransom, as this does not guarantee access will be restored.
- Figure 1 shows the ransomnote found on infected computer.
- Figure 2 shows the text file created by the ransomware that explaining what has happened and instructions on how to pay the ransom.
- 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



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

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?

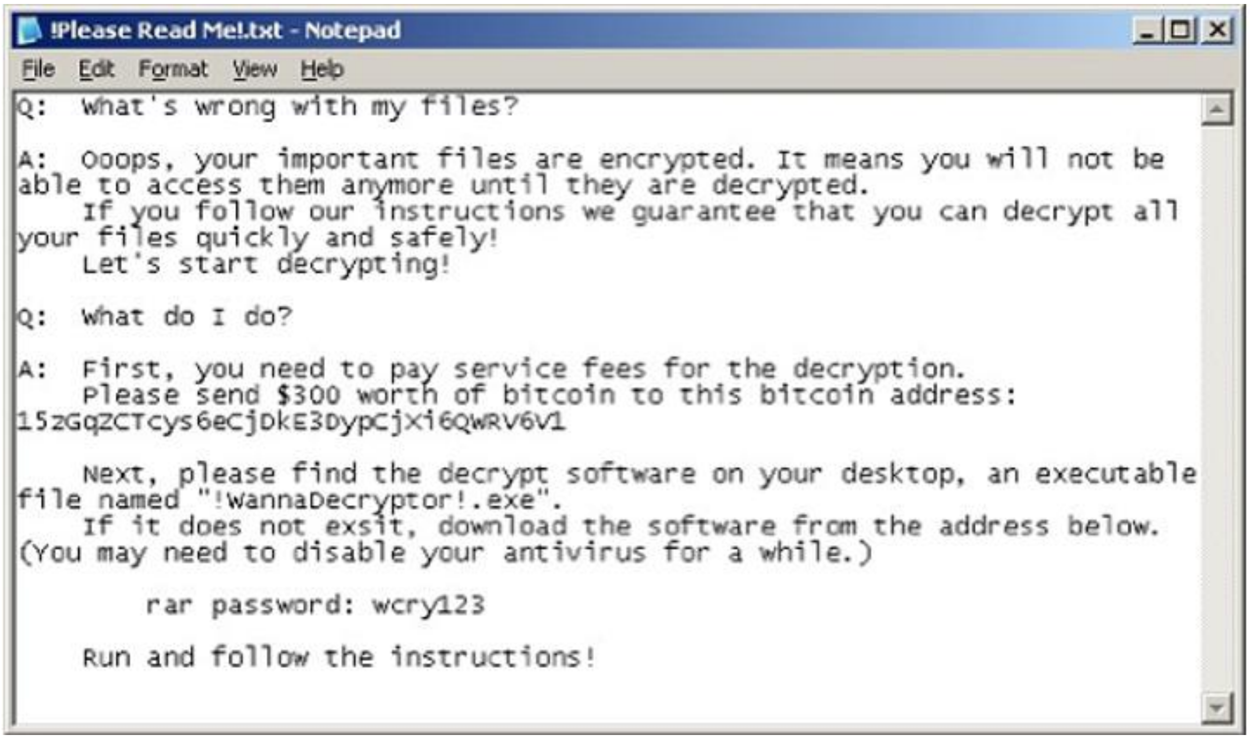
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the 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

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Figure 1: WannaCry ransomnote (source: Securelist.com)



```
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 exsit, 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!
```

Figure 2: A text file dropped by the ransomware
(Source: http://www.cyberswachhtakendra.gov.in)

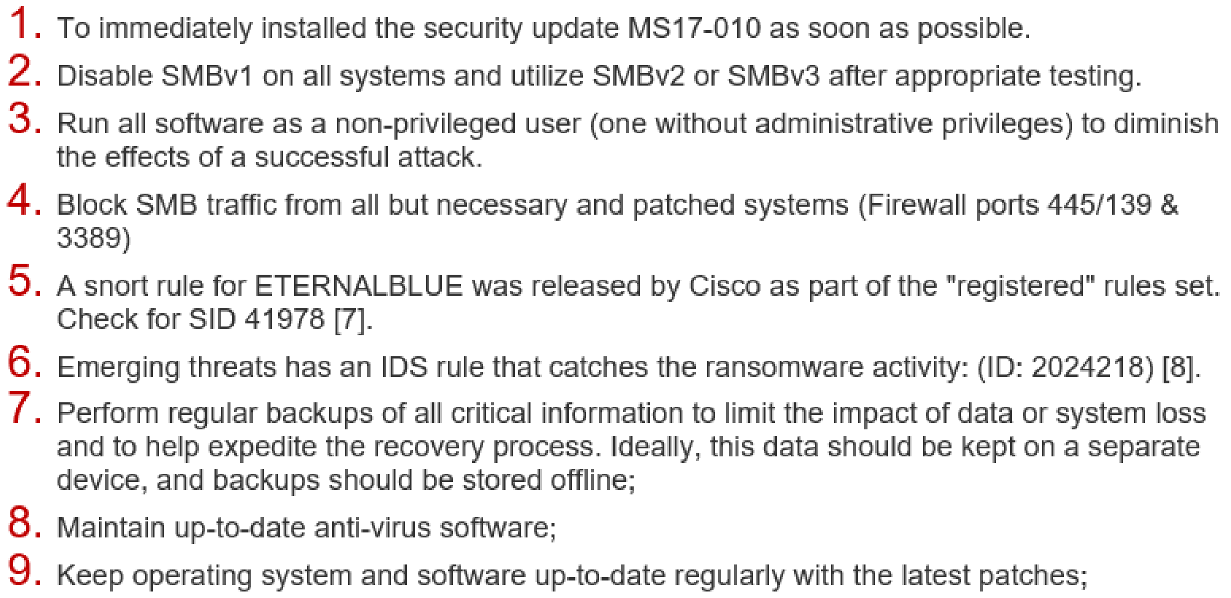
Affected Product

- Unpatched Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows 8.1
- Windows Server 2012
- Windows 10
- Windows Server 2012 R2
- Windows Server 2016

Recommendations

- Users of this product are advised to review and patch the vulnerability described in MS17-010: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- Microsoft Patch for Unsupported Versions such as Windows XP, Vista, Server 2003, Server 2008 can be referred here: http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

- Users are advised to take the following preventive measures to protect their computer from ransomware infection:



1. To immediately installed the security update MS17-010 as soon as possible.
2. Disable SMBv1 on all systems and utilize SMBv2 or SMBv3 after appropriate testing.
3. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
4. Block SMB traffic from all but necessary and patched systems (Firewall ports 445/139 & 3389)
5. A snort rule for ETERNALBLUE was released by Cisco as part of the "registered" rules set. Check for SID 41978 [7].
6. Emerging threats has an IDS rule that catches the ransomware activity: (ID: 2024218) [8].
7. 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;
8. Maintain up-to-date anti-virus software;
9. Keep operating system and software up-to-date regularly with the latest patches;

Generally, MyCERT advises the users of this software to be updated with the latest security announcements by the vendor and follow best practice security policies to determine which updates should be applied.

Source :
https://www.mycert.org.my/en/services/advisories/mycert/2017/main/detail/1263/index.html