CERT-MU Advisory

CERT-MU

Following the Security Alert sent by CERT-MU on 14th May 2017, please find below the Technical Advisory on the Wanna Cry Global Ransomware Attack:

THE MASSIVE WANNA CRY GLOBAL RANSOMWARE ATTACK

Original Issue Date: 14th May 2017

Updated: 15th May 2017

Severity Rating: High

DESCRIPTION

The world is experiencing a massive global ransomware cyber-attack dubbed as **"WannaCrypt"** or **"WannaCry"** (Ransom: Win32/WannaCrypt). The malware is a new variant of the Ransom.CryptXXX family and exploits a vulnerability in Microsoft's Windows operating system. WannaCrypt spreads aggressively across networks and holds files to ransom. About 104 countries in the world including U.K, Russia, Ukraine, India, China, Italy, and Egypt have been affected. In Spain, major companies including telecommunications firm Telefónica were infected. Thousands of computer systems around the world have been shut down.

The malware appears to have originally spread via email as compressed file attachment. Once executed, it can easily spread across networks exploiting a flaw in the Windows SMB Server.

AFFECTED SYSTEMS

Unpatched Windows Systems are at risk of infection.

TECHNICAL DETAILS OF THE ATTACK

1. **When the Trojan is executed, it drops the following files:**

   [PATH_TO_TROJAN]\!WannaDecryptor!.exe

   [PATH_TO_TROJAN]\c.wry

[PATH_TO_TROJAN]\f.wry

[PATH_TO_TROJAN]\m.wry

[PATH_TO_TROJAN]\r.wry

[PATH_TO_TROJAN]\t.wry

[PATH_TO_TROJAN]\u.wry

[PATH_TO_TROJAN]\TaskHost

[PATH_TO_TROJAN]\00000000.eky

[PATH_TO_TROJAN]\00000000.pky

[PATH_TO_TROJAN]\00000000.res

%Temp%\0.WCRYT

%Temp%\1.WCRYT

%Temp%\2.WCRYT

%Temp%\3.WCRYT

%Temp%\4.WCRYT

%Temp%\5.WCRYT

%Temp%\hibsys.WCRYT

Note: [PATH_TO_TROJAN] is the path where the Trojan was originally executed.

2. **The Trojan then creates the following registry entries:**

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"Microsoft Update Task Scheduler" = ""[PATH_TO_TROJAN]\[TROJAN_EXE_NAME]" /r"

   HKEY_LOCAL_MACHINE\SOFTWARE\WannaCryptor\"wd" = "[PATH_TO_TROJAN]"

3. **The Trojan also sets the following registry entry:**

   HKEY_CURRENT_USER\ControlPanel\Desktop\"Wallpaper"= %UserProfile%\Desktop\!WannaCryptor!.bmp"

4. **The Trojan creates the following mutexes:**

   Global\WINDOWS_TASKOSHT_MUTEX0

   Global\WINDOWS_TASKCST_MUTEX

5. **The Trojan then terminates the following processes using taskkil /f /iml:**

   sqlwriter.exe

   sqlserver.exe

   Microsoft.Exchange.*

   MSExchange*

6. **It then searches for and encrypts files with the following extensions:**

   .123, .3dm, .3ds, .3g2, .3gp, .602, .7z, .ARC, .PAQ, .accdb, .aes, .ai, .asc, .asf, .asm, .asp, .avi, .backup, .bak, .bat, .bmp, .brd, .bz2, .cgm, .class, .cmd, .cpp, .crt, .cs, .csr, .csv, .db, .dbf, .dch, .der, .dif, .dip, .djvu, .doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .dwg, .edb, .eml, .fla, .flv, .frm, .gif, .gpg, .gz, .hwp ,.ibd, .iso, .jar, .java, .jpeg, .jpg, .js, .jsp, .key, .lay, .lay6, .ldf, .m3u, .m4u, .max, .mdb, .mdf, .mid, .mkv, .mml, .mov, .mp3, .mp4, .mpeg, .mpg, .msg, .myd, .myi, .nef, .odb, .odg, .odp, .ods, .odt, .onetoc2, .ost, .otg, .otp, .ots, .ott, .p12, .pas, .pdf, .pem, .pfx, .php, .pl, .png, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .psd, .pst, .rar, .raw, .rb, .rtf, .sch, .sh, .sldm, .sldx, .slk, .sln, .snt, .sql, .sqlite3, .sqlitedb, .stc, .std, .sti, .stw, .suo, .svg, .swf, .sxc, .sxd, .sxi, .sxm, .sxw, .tar, .tbk, .tgz, .tif, .tiff, .txt, .uop, .uot, .vb, .vbs, .vcd, .vdi, .vmdk, .vmx, .vob, .vsd, .vsdx, .wav, .wb2, .wk1, .wks, .wma, .wmv, .xlc, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .zip

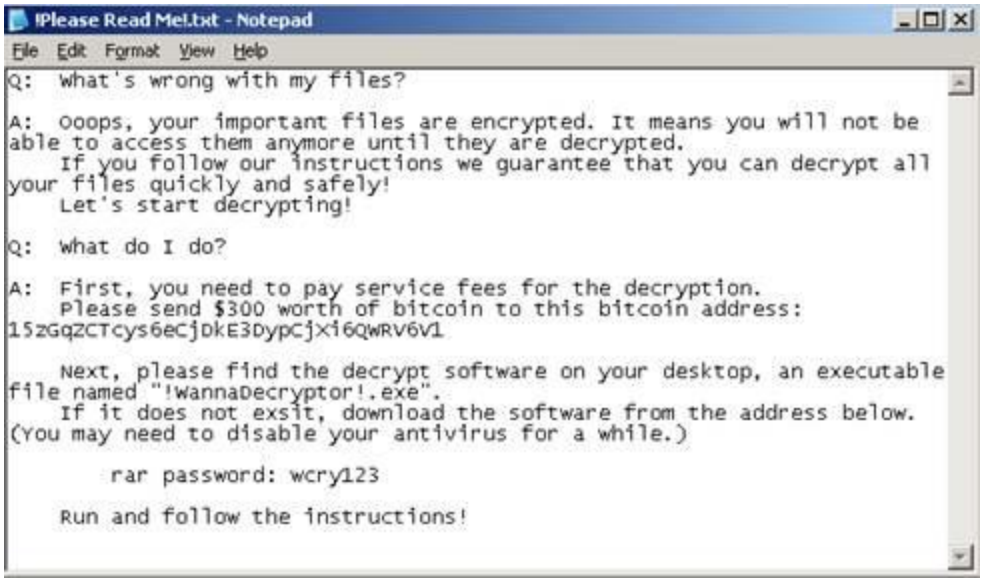
   Encrypted files have .WCRY appended to the end of the file names.

7. **The Trojan then deletes the shadow copies of the encrypted files.**

8. **The Trojan drops the following files in every folder where files are encrypted:**

   !WannaDecryptor!.exe.lnk
   !Please Read Me!.txt

   The contents of the **!Please Read Me!.txt** is a text version of the ransom note with details of how to pay the ransom. This is shown below:



9. **The Trojan downloads Tor and uses it to connect to a server using the Tor network.**

10. **It then displays a ransom note explaining to the user what has happened and how to pay the ransom.**

HOW TO DETECT THE ATTACK?

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

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.

PRECAUTIONS TO BE TAKEN TO PROTECT FROM THIS RANSOMWARE CAMPAIGN

i. Aggressively patch and update Anti-Virus signatures with a priority on those in the last 60 days (including MS17-010).

ii. Warn users not to open attachments/enable macros on suspicious emails. This may be the entry vector so diligence is warranted.

iii. If you suspect you may be a victim, install Windows Defender; and run to remove the malware on systems.

iv. If patching is not possible (i.e. if the machines cannot be updated with the March MS17-010), temporarily block SMB connections to limit the spread. This will likely impact your organization's services. The following workarounds may be helpful in your situation:

- Disable SMBv1
- For customers running Windows Vista and later, see Microsoft Knowledge Base Article 2696547.

Alternative method for customers running Windows 8.1 or Windows Server 2012 R2 and later

For Client Operating Systems:

- Open Control Panel, click Programs, and then click Turn Windows features on or off.

- In the Windows Features window, clear the SMB1.0/CIFS File Sharing Support checkbox, and then click OK to close the window.
- Restart the system.

For Server Operating Systems:

- Open Server Manager and then click the Manage menu and select Remove Roles and Features.
- In the Features window, clear the SMB1.0/CIFS File Sharing Support check box, and then click OK to close the window.
- Restart the system.

IMPACT OF WORKAROUND

The SMBv1 protocol will be disabled on the target system.

HOW TO UNDO THE WORKAROUND

Retrace the workaround steps, and select the SMB1.0/CIFS File Sharing Support check box to restore the SMB1.0/CIFS File Sharing Support feature to an active state.

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu