

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

The Massive Wanna Cry Global Ransomware Attack

Original Issue Date: 14th May 2017

Severity Rating: High

Description:

A massive global ransomware attack dubbed as **“WannaCrypt”** or **“WannaCry”** (Ransom:Win32/WannaCrypt) exploiting a vulnerability in Microsoft's Windows operating system is currently in progress. The ransomware is a new variant of the Ransom.CryptXXX family and spreads aggressively across networks and holds files to ransom. The attack is spreading widely and impacting a large number of organisations across the world.

Affected Systems:

Windows Systems which do not have the latest security updates are at risk of infection.

Methodology of Attack:

1. WannaCry propagates to other computers by exploiting a known SMB remote code execution vulnerability in Microsoft Windows computers. (MS17-010). The malware spreads itself within corporate networks, without user interaction, by exploiting the vulnerability. The payload gets loaded in C:\ProgramData\, in a hidden folder with random name.
2. The malware encrypts files with the extensions listed below and appends .WCRY to the end of the file name:
.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, .xism, .xlsx, .xlt, .xltm, .xltx, .xlw, .zip

3. WannaCry encrypts data files and ask users to pay a US\$300 ransom in bitcoins. The ransom note indicates that the payment amount will be doubled after three days. If payment is not made after seven days, the encrypted files will be deleted. The Ransom demand screen displayed by WannaCry Trojan is shown below:



4. It also drops a file named ! **Please Read Me!.txt** which contains the ransom note. This is shown below for your reference:



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

Precautions to be taken to protect from this ransomware campaign:

- Aggressively patch and update Anti-Virus signatures with a priority on those in the last 60 days (including MS17-010).
- Warn users not to open attachments/enable macros on suspicious emails. This may be the entry vector so diligence is warranted
- If you suspect you may be a victim, install Windows Defender; and run to remove the malware on systems
- If you are experiencing major outage issues, contact your Microsoft Windows representative.
- 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.

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.

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>