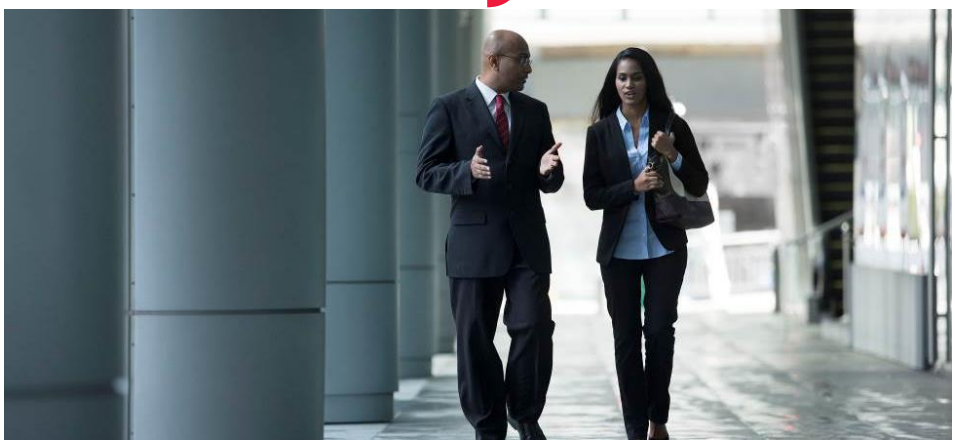
MAY 2017

NEWS ALERT

WannaCry Ransomware



WHAT IS RANSOMWARE

Ransomware is a type of malicious software that carries out cryptography (encryption) based extortion attack that blocks access to most commonly used or accessed data and files on systems until a ransom is paid and requesting payment to unlock the locked data.

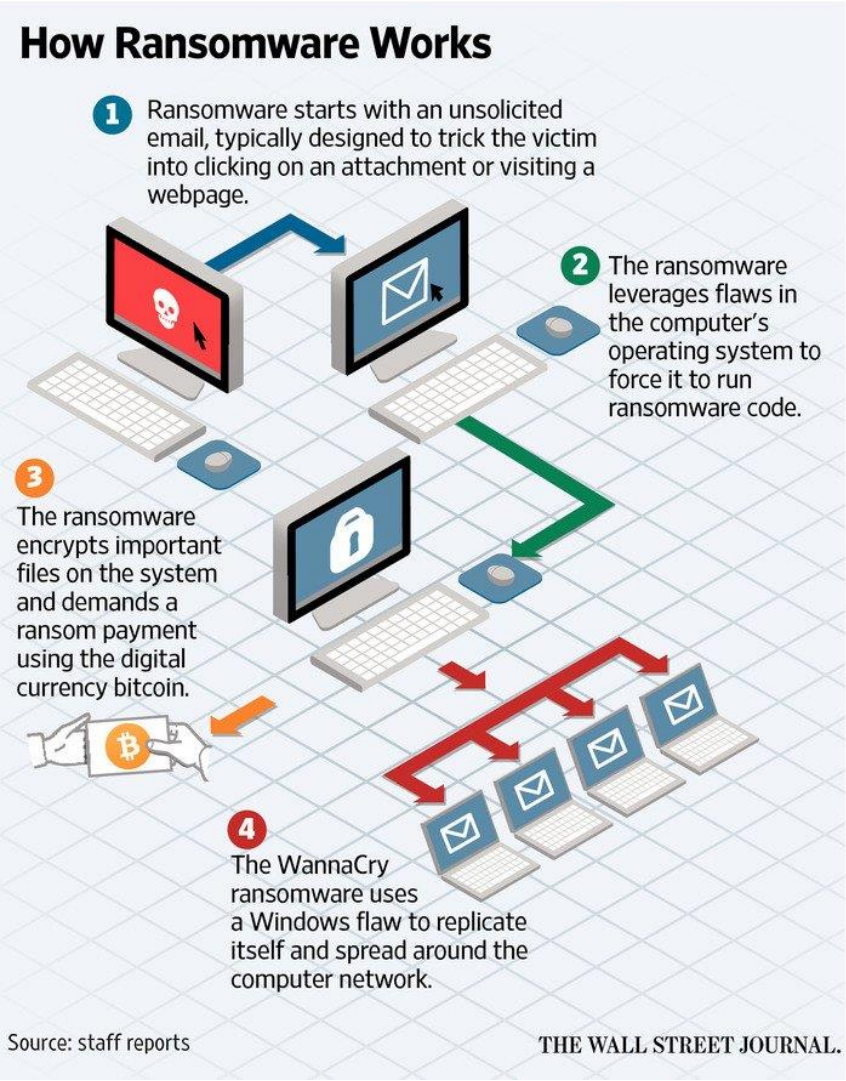
What is WannaCrypt ransomware?

WannaCrypt Ransomware, also known as WannaCry, WannaCrypt0r or Wcrypt is a ransomware which targets Windows operating systems.

Discovered on 12 May 2017, WannaCrypt was used in a large cyberattack and has since infected **over 200,000 Windows PCs across 150 countries as at 16 May 2017**.

An operating system infected with WannaCry

How Ransomware Works?



Source: The Wall Street Journal

How does WannaCrypt ransomware get into your computer?

WannaCrypt first gains access to the computer system via an email attachment and thereafter can spread rapidly through the Local Area Network (LAN). Therefore it is very crucial to not open unrecognised or spam (Phishing) emails to avoid such attacks.

The ransomware can encrypt your systems hard disk and attempts to spread to random computers on the internet and between computers in the same network.

The list of file extensions that can be infected by WannaCrypt

WannaCrypt searches the whole computer for any file with any of the following file name extensions shown below. It then renames them by appending ".WNCRY" to the file name.

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

How to protect against WannaCrypt threat?

- Microsoft recommends **upgrading to Windows 10** as it equipped with latest features and proactive mitigations.
- Install the **security update MS17-010** released by Microsoft. The company has also released **security patches for unsupported Windows versions** like Windows XP, Windows Server 2003, etc.
- Windows users are advised to be extremely wary of **Phishing email** and be very careful while **opening the email attachments** or **clicking on web-links**.
- Make **backups** and keep them securely
- **Windows Defender Antivirus** detects this threat as *Ransom:Win32/WannaCrypt* so enable and update and run Windows Defender Antivirus to detect this ransomware.
- Make use of some **Anti-WannaCry Ransomware Tools**.
- **Disable SMBv1** with the steps documented at **KB2696547**.
- Consider adding a rule on your router or firewall to **block incoming SMB traffic on port 445**
- Enterprise users may use **Device Guard** to lock down devices and provide kernel-level virtualization-based security, allowing only trusted applications to run.

WannaCrypt may have been addressed with appropriate Windows patches and precautions listed above but that does not mean in any way it has completely stopped this malware attack as there is every possibility of a newer variant of the malware with the possibility of further attacks by exploiting other aspects of the Windows operating systems.

For more information about protecting your organisation from ransomware, please contact:

SANJAY SIDHU
Head of Risk Advisory Services
sanjay@bdo.my

WOON TAI HAI
Executive Director
thvoon@bdo.my

BDO Consulting Sdn Bhd (269105-W)
Level 8, BDO @ Menara CenTARa
360 Jalan Tuanku Abdul Rahman
50100 Kuala Lumpur, Malaysia
T: +603 2616 2888 **F**: +603 2616 2970 **E**: bdo@bdo.my
www.bdo.my

References

Karthik Selvaraj, Elia Florio, Andrea Lelli, and Tanmay Ganacharya (Microsoft Malware Protection Center) *WannaCrypt Ransomware Worm Targets out-of-date Systems*, Available from: https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/ [12 May 2017]

Ayush Agrawal, *The WannaCry Ransomware & How to Avoid it*, Available from: http://manipalthetalk.org/tech/the-wannacry-ransomware-how-to-avoid-it/ [15 May 2017]

AnandK@TWC, *What is WannaCrypt ransomware, how does it work & how to stay safe*, Available from: http://www.thewindowsclub.com/what-is-wannacrypt-ransomware [14 May 2017]