WannaCry

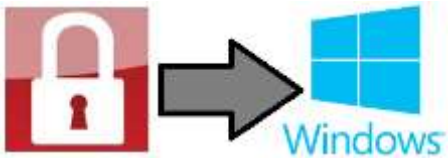
One of the "Broadest" and "Most Damaging" Cyberattacks in History

Awareness Leaflet

Massive Ransomware hits 99 countries so far, and it's still *SPREADING!*

WannaCry

It is a type of malicious software (specifically, it is a Ransomware) targeting Microsoft Windows.



WannaCry designed to extort money from victims by block the access to data that stored on victim's computer (*by encrypt it*) until a ransom is paid.

WannaCry shows to victims a note demanding $300 (*in bitcoin*) to have their data decrypted.

WannaCry encrypts many file types including (.docx (**MS Word**), .xlsx (**MS Excel**), .pptx (**MS PowerPoint**), .jpeg (**Photo**), .mpeg (**Video**) and more), appending ".WCRY" to the end of the file name.

In **12 May 2017**, a large cyberattack using WannaCry was launched; while initially popular in Russia, WannaCry infecting over 230,000 computers around world, demanding ransom payments in 28 languages.

There have been reports of infections in 99 countries, including the Russia, Ukraine, Taiwan, UK, US, China, Spain, and Italy; and it's still SPREADING!

UK hospitals, Chinese universities and global firms like Fedex were also infected.

WannaCry - Ransomware attack is typically carried out using a "Trojan", entering a victim's computer through, for example, a downloaded file!.

WannaCry - Trojan infects the victim's computer by encrypting all its files and, using a remote command execution vulnerability through SMB.

SMB (Server Message Block) mainly used for providing shared access to files, printers, serial ports and miscellaneous communications between nodes on a network.

Most usage of SMB involves computers running Microsoft Windows.

WannaCry is believed to use the **EternalBlue exploit (MS17-010),** which was developed by the U.S. National Security Agency to access computers running Microsoft Windows operating systems.

Check your computer system now,

ARE YOU AT RISK?

To Protect Your Computer System

To protect your computer system, do the following:

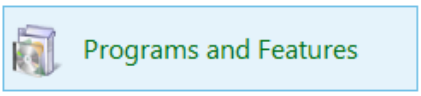
(1) First of all, update your Windows *against EternalBlue exploit*, using the following patch file: **technet.microsoft .com/library/security/ MS17-010**

(2) Make sure to have an updated Antivirus.

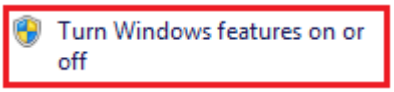
(3) Clear the SMB by follow the following steps:

a. Right Click on 'Start Button' and click on 'Control Panel',

b. Click on 'Programs and Features',



c. The click on 'Turn Windows features on or off' that located on the left side.



d. Clear the check box for 'SMB 1.0/CIFS File Sharing Support',

e. Restart your computer.

(4) Avoid clicking links, or open emails from unknown sources.

This awareness leaflet was prepared and design by Dr. Mazin S. Al-Hakeem
Head of Information Technology Department – Lebanese French University

www.lfu.edu.krd