Download and sell Windows patches for all versions to avoid being hit by a massive cyber attack, affecting 150 countries and still spreading

A large-scale network attack is spreading globally, downloading Windows updates immediately for prevented versions.

This software is a form of ransomware, which works by encrypting the victim's data and requires a sum of money to redeem. Network security company Avast told CNN that they found ransomware on at least 99 countries from the UK to Japan. To date, these ransomware-affected organizations have included the UK National Health Service (NHS), Spain's Telefónica telecom company and FedEx shipping company.

Download the Windows patch and see the affected versions:

1. *https://technet.microsoft.com/en-us/library/security/ms17-010.aspx* (includes all Windows versions)

Urgent: How to handle emergency WannaCry malware from the National Information Security Department

These files are most vulnerable to attack by WannaCry:

1. Common office file extensions (.ppt, .doc, .docx, .xlsx, .sxi).
2. Office formats are less common and country specific (.sxw, .odt, .hwp).
3. Storage formats, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv)
4. Email and email database (.eml, .msg, .ost, .pst, .edb).
5. Database files (.sql, .accdb, .mdb, .dbf, .odb, .myd).
6. Source code and developer's project file (.php, .java, .cpp, .pas, .asm).
7. Encryption keys and certificates (.key, .pfx, .pem, .p12, .csr, .gpg, .aes).
8. Graphic design authors, authors and photographers (.vsd, .odg, .raw, .nf, .svg, .psd).
9. Virtual machine file (.vmx, .vmdk, .vdi).

Latest update on WannaCry:

1. WannaCry has affected many Vietnamese organizations, the main reason is not closing port 445 on Windows and not updating the latest patch.
2. After entering the computer, WannaCry not only locks data, steals important information, but also hijacks social networking accounts, email, and chat to spread ransomware links to friends on the list.
3. If only one device on the LAN is attached, other highly capable machines will be infected even if users on other machines do not click the link or download the file to the computer.

The attack caused chaos across the UK. Many hospitals were closed and shut down without warning. Employees must switch to manual work with paper and pen.

Both NHS and Telefónica confirmed they were attacked, ransomware seemed to be WannaCry and he demanded a ransom of at least $ 300 to unlock the encrypted data. Slowly one day the ransom will double and then delete the data.

They say the cause comes from a flaw in a Windows software developed by the NSA (National Security Agency), the US intelligence organization. Although the flaw was leaked a few months ago and Microsoft also released a patch, the affected organizations probably did not update the software.

MalwareTech has published an online map that monitors infections worldwide, notably **Vietnam has also appeared** on this map. Readers can see here: *https://intel.malwaretech.com/botnet/wcrypt/*

CCN-CERT, a team responding to emergency situations on computers in Spain, has given advice on Microsoft's response and patch to fix it.

The organization said: "Ransomware, a version of WannaCry, attacks the computer by encrypting all files and using remote execution commands via SMB that has been delivered to the Windows machine on the same system."

About 85% of Telefónica's computers have been affected. The Portuguese telecommunications company was also attacked on Friday but did not affect the service.

Please update Windows to the latest version to receive the patch. If the computer has been hacked, try using No More Ransome's tools to decode the data. With the NMR's 15 free Ransomware decoding tools, you won't need to ransom the file anymore