How to handle the emergency WannaCry malicious code from the National Information Security Department

The Information Security Department has issued guidelines for emergency handling of WannaCry extortion codes for users as well as organizations and businesses to avoid damage caused by this malicious code. Vietnam is currently on the list of 20 countries attacked by this malicious code.

The Information Security Department has issued guidelines for emergency handling of WannaCry extortion codes for users as well as organizations and businesses to avoid damage caused by this malicious code. Vietnam is currently on the list of 20 countries attacked by this malicious code.

Department of Information Security (Ministry of Information and Communications) said, currently, malicious code named WannaCry exploits some vulnerabilities in Windows operating system to attack computers with the goal of encrypting data for ransom , affecting many organizations and individuals on a global scale. Department of Information Security - Ministry of Information and Communications instructs organizations and individuals to implement this emergency handling method as follows:

For individuals:

Specifically, for individuals who need to make immediate updates to the version of the operating system Windows is using. Particularly for Windows XP-based computers, use the latest update specifically for this case at:

> https://www.microsoft.com/en-us/download/details.aspx?id=55245&WT.mc_id=rss_windows_allproducts

or search by update keyword KB4012598 on the Microsoft home page.

1. Microsoft released an emergency patch to prevent ransomware from attacking

Individuals also need to update the programs Antivius is using right away. For computers without Antivirus software, install and use a copyrighted Antivirus software immediately. The Information Security Department recommends that users be cautious when receiving email with attachments and strange links sent in emails, on social networks, chat tools .

Users need to be cautious when opening attachments even when received from familiar addresses. Use online or copyrighted malware testing tools on your computer with these files before opening them. Users do not open paths with an .hta extension or an unclear path, shortened links and concurrently store important data (backup).

Handling Wannacry in businesses and organizations:

1. For organizations and businesses, especially for system administrators, it is necessary to immediately check the servers and temporarily block (services) the services using ports 445/137/138/139 .

See also: How to close the port / Port 445 on Windows 2000 / XP / 2003 to prevent ransomware WannaCry

1. Organizations and businesses need to take measures to update early, appropriate according to each specific for the organization's windows servers.
2. Create snapshots for virtualized servers in anticipation of being hacked.
3. Organizations and businesses must take measures to update workstations using Windows operating systems.
4. Update the database for the current Antivirus Endpoint servers. For systems that do not yet use these tools, it is necessary to use Endpoint software with the latest copyright and updates immediately for workstations.
5. Organizations and enterprises take advantage of available information security solutions in organizations such as Firewall, IDS / IPS, SIEM . to monitor, monitor and protect the system during sensitive times. this.
6. Update updates from security vendors for available solutions. Also, prevent and monitor domains that are being used by the WannaCry malware, to identify infected computers in the network to take timely measures:

   http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/

This domains have been sinkholed, the Information Security Department will constantly update this list on the website.

1. How to remove / fix ransomware WannaCry

Organizations and businesses consider blocking the use of Tor in the network and take measures to store (backup) important data immediately. Organizations and businesses warn people and take measures as mentioned above for users. Contact the authorities as well as organizations and businesses in the field of information security for assistance when needed.