1.6 million computers in Vietnam were erased by the virus, losing nearly 15,000 billion in 2018

According to the survey results from network security company Bkav, in 2018, Vietnamese users lost 14,900 billion dong, up 21% compared to the damage of 2017.

According to the survey results from network security company Bkav, in 2018, Vietnamese users lost 14,900 billion dong, up 21% compared to the damage of 2017.

According to network security company Bkav, in Vietnam, the code of extortion extends mainly through email because 74% of domestic users do not open it in a safe isolation environment (Safe Run) but still keep the habit familiar to open attachments directly from email.

In addition, USB is also a popular means of spreading malware to computers in Vietnam. According to statistics, in 2018, 77% of USB storage devices in Vietnam are infected at least once.

In Vietnam, there are more than 60% of agencies and businesses infected with malicious code. The reason is that they have not equipped the overall antivirus solution, when an infected computer will spread to all other computers on the network.

Virtual money digging not only slows down your computer but also steals information, deletes data or even attempts to attack APT due to the ability to update and download other spyware programs.

Phishing on Facebook to steal accounts

In 2018, more than 83% of social network users in Vietnam met comments (comments) for bad purposes such as stealing Facebook accounts. Users are often attracted and curious to click on virtual accounts with eye-catching avatars and attractive comments like "make friends with me" or "get used to me" . This makes the victim have Can be deceived Facebook account.

As recommended by network security experts, users must check the link sent from strangers or friends before viewing, not access links from strangers.

Security flaws surged

The number of security holes in the software was announced in 2017 and 2018 to 15,700, a sudden increase of about 2.5 times the previous year. Manufacturers are quick to release security patches, but users have not updated them in time. For example, more than 50% of computers in Vietnam are still not patched with SMB vulnerabilities, despite being detected and warned since 2017.

Hacker took advantage of this to attack the network through vulnerabilities, thereby spreading viruses, installing spyware and performing APT attacks.

To ensure safety, security experts recommend that agencies and enterprises should equip solutions to control security and update policies for all computers in the system. For users, it is recommended to check and install patches for your device.

The appearance of malicious code using artificial intelligence (AI) in 2019

According to Bkav's forecast, 2019 may be the time when malicious code using artificial intelligence (AI) appears, in the original form, the PoC (Proof of Concept) prototype.

Software that encrypts money, deletes data, digs virtual money and attacks APT are still the biggest threats to Internet users. To maximize the spread, these types of malicious code can combine different modes of infection.

See more:

1. How to identify WannaCry malicious code from Vietnam Computer Emergency Response Center (VNCERT)
2. Security vulnerabilities - basic insights
3. Small antivirus programs for USB

4. How to check if the computer network is safe

You finished reading the article "**1.6 million computers in Vietnam were erased by the virus, losing nearly 15,000 billion in 2018**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
