Famous cyber attacks of the past decade

There are two basic types of ransomware, but hackers also have many other ways to attack an information technology system.

Two basic forms of ransomware

Ransomware attack is a form of hackers using ransomware to encrypt and control access to important assets in a business's information technology system in order to demand a ransom to restore rights. access that. Talking to VTC News, Ms. Vo Duong Tu Diem, Vietnam Regional Director of Kaspersky, said that to protect businesses, users need to distinguish two basic types of ransomware:

Locker ransomware : This form will partially disable the user's mouse and keyboard, but still allow them to see the ransom request screen. However, other functions of the computer will not be available.

Crypto ransomware : Instead of blocking basic computer functions, this malware encrypts critical business data, such as information about customers, partners, supply chains, employees, and strategies. Business strategies, images, videos. Attackers take advantage of the importance of data to demand ransom, otherwise all important information will be deleted.

The common characteristic of ransomware attacks is that hackers have infiltrated the database for a long time and are hidden here, without creating any suspicious activities in order to bypass the supervision of organizations and businesses. Karma. They will "lay low" long enough to grasp the importance and scale of the information, and when the time is ripe, they will encrypt the most important data to force the victim to pay the ransom.

Typical cyber attacks

Over the past decade, cyber criminals have caused ransomware attacks and used many methods to spread malicious code into the information systems of many different businesses and organizations globally, not just Vietnam. Male. Below are some typical examples of the dangers and risks that ransomware attacks pose to businesses:

Email phishing attacks : In 2016, a series of ransomware attacks called Locky targeted large hospitals, leaving these facilities unable to access patient data. In some cases, they are forced to transfer patients to other hospitals. Typically, victims are scammed via email and this attack encrypts all important documents and images, for example patient records, until the ransom (usually Bitcoin or other cryptocurrency) is paid. valuable and highly stable element) is paid.

Operating system vulnerabilities : Outdated systems are one of the main reasons why businesses are vulnerable to ransomware attacks, typically the famous ransomware infection campaign called WannaCry in 2017. This attack started in the UK and spread to nearly 150 countries worldwide, mainly targeting state agencies and large businesses. According to Interpol, WannaCry malware has attacked 230,000 computers in 150 countries. As a result, the Telefonica phone network in Spain was paralyzed and the departure schedules of many trains and ticket vending machines were seriously disrupted.

"Drive-by-attacks" : After the WannaCry ransomware incident in 2017, another type of ransomware called Bad Rabbit appeared, mainly targeting countries such as Russia and Eastern Europe. The tricks of the hacker group spreading Bad Rabbit are very sophisticated: they require users to run the Adobe Flash installer (actually disguised malware) from a website that has been previously attacked. After completing the installation, the malware begins to infect the user's computer. The attacker demanded a ransom of 0.05 Bitcoin, equivalent to 280 USD at the exchange rate at that time.

Recommendation from experts

Following the recent ransomware attack, security experts offer these recommendations to help businesses protect themselves against similar attacks:

Data backup: Make sure business data is always backed up to prevent it from being lost, stolen or accidentally deleted. When backing up, use external devices and disconnect them from the computer immediately afterward because data will be encrypted if it remains connected to the malware-infected device. Backing up will help businesses avoid data loss and ransom demands.

Update systems regularly: The 2017 WannaCry attack occurred largely because businesses did not update their systems regularly. This allows attackers to exploit the vulnerability. As a result, these vulnerabilities still exist and can be attacked.

Invest in cyber security training for employees: Employees who are fully equipped with cyber security knowledge will be able to respond to cyber attacks. Businesses should invest in training programs to raise employee awareness to help them effectively protect cybersecurity.

Use network security solutions: There are currently many software solutions from reputable security firms (foreign as well as Vietnamese) that can help detect and protect information systems and users from attacks. ransomware attacks at every stage of the attack thanks to a multi-layered security system.