WannaCry remains one of the most dangerous global security threats

WannaCry is a ransomware that spreads itself on computers using Windows operating systems.

WannaCry is a ransomware that spreads itself on computers using Windows operating systems. After it was first discovered in May 2017, it quickly became one of the worst nightmares in the history of global cybersecurity, with millions of computers infected, causing billions of dollars in damage. , followed by the collapse of countless businesses that accidentally fell victim.

By the efforts of all mankind, WannaCry is said to have been 'defeated' by the end of 2017. The rise of other ransomware and the weakening of WannaCry made many people think that this ransomware was no longer is a remarkable threat.

However, according to a new report by PreciseSecurity.com, WannaCry is in fact still one of the largest and most destructive malware types available today. Specifically, up to 1/4 (23.56%) of all ransomware attacks recorded in 2019 are directly related to WannaCry, making it the typical common malicious element of year.

PreciseSecurance claims WannaCry has infected about 230,000 devices worldwide, causing damage estimated at up to $ 4 billion. The reason this malicious code can run globally is rooted in two main reasons:

1. Do not update the software, operating system to the new version.
2. The victim was tricked into clicking on a malicious link, downloading and opening a file containing malicious code in the system.

According to statistics, more than two-thirds of global internet management service providers report that ransomware is mainly transmitted via spam and phishing emails.

Specifically, spam email accounted for more than half (55%) of the total global email traffic in 2019. In addition, some other reasons are weak passwords, poor user knowledge and websites. malicious and clickbait.

Ransomware is a type of malware that, after infecting the victim's system, will immediately encrypt all data stored on the system. The hacker then asks the owner of the system to pay the ransom (usually electronic money) in exchange for the key to decrypt the data.

Most cyber security experts warn people not to pay a ransom for hackers because there is no guarantee they will get a decryption key after the transfer. Instead, businesses should ask for help from experienced security organizations, have important data backup options, and promote their staff education about the dangers of ransomware.

1. With NMR's 15 free Ransomware decoding tools, you won't need to pay a ransom for the file anymore