

## **What is WannaCry?**

First and foremost, let's clarify exactly what WannaCry is. This malware is a scary type of trojan virus called "ransomware." As the name suggests, the virus in effect holds the infected computer hostage and demands that the victim pay a ransom in order to regain access to the files on his or her computer.

## **What exactly does WannaCry do?**

RansomWare like WannaCry works by encrypting most or even all of the files on a user's computer. Then, the software demands that a ransom be paid in order to have the files decrypted. In the case of WannaCry specifically, the software demands that the victim pays a ransom of \$300 in bitcoins at the time of infection. If the user doesn't pay the ransom within three days, the amount doubles to \$600. After seven days without payment, WannaCry will delete all of the encrypted files and all data will be lost.

## **How was WannaCry created?**

You can thank the NSA for discovering the "EternalBlue" exploit that would later be used by the WannaCry trojan, and then for keeping under wraps to use for its own intelligence gathering purposes. The security hole was then made public last month when a group of hackers called Shadow Brokers released the details of the exploit to the public.

## **Is the attack over?**

No.

WannaCry was first discovered on Friday, May 12<sup>th</sup> 2017, and it had spread to an estimated 57,000 computers in more than 150 different countries around the world by the end of the day. European countries were hit the hardest, and business ground to a halt at several large companies and organizations, including banks, hospitals, and government agencies.

## **How can I protect myself from WannaCry?**

Regardless of which operating system you run, you should install any and all available security updates immediately. Specifically, Windows users with machines that run Windows XP, Windows 8, or Windows Server 2003 should immediately install [this security update](#) released on Friday by Microsoft.

## **What can I do if my computer is infected with WannaCry?**

Sadly, there is no fix for WannaCry available at this time. Antivirus companies and cybersecurity experts are hard at work looking for ways to decrypt files on infected computers, but no means of third-party decryption are available right now. Hopefully affected users have backups of their data available, because the only other option right now is to follow the instructions offered in the software to pay the ransom.