WannaCrypt Ransomware Infects Thousands of Computers Worldwide

On the morning of Friday May, 12 2017, a worldwide ransomware cyber attack called WannaCrypt or WannaCry was launched, infecting over 230,000 Windows computers in 150 countries currently to date. Many corporations and government agencies have been affected, including Britain's National Health Service and Telefonica of Spain, one of the world's largest telecom providers.

Ransomware is a type of malware which locks your PC and/or encrypts your important data files, leaving a note about what has occurred and demanding a payment (ransom) in order to regain access to the computer or decrypt the data files so they can be opened again.

The WannaCrypt ransomware exploits a Windows vulnerability in the SMB protocol (used for network file sharing) called 'Eternal Blue', which was discovered by the US National Security Agency and subsequently stolen and leaked out to the public. The ransomware uses the vulnerability to gain access to the machine, encrypt its files and then leave a ransom note asking for several hundred dollars payable in bitcoin to get the user's files back.

The ransomware is known to spread by tricking users into opening malicious email attachments or clicking on malicious web links. It is also actively searching out computers that are susceptible to the Windows vulnerability and may infect a machine without any user interaction.

Fortunately, there are steps that can be taken to prevent WannaCrypt from infecting your computer:

1. Keep Windows up to date: Microsoft released a security update MS17-010 in March that addresses the vulnerability that this malware is exploiting. By default, Windows computers are configured to install updates automatically, so if your computer is actively updating Windows you should already have the patch in place.
2. Keep your antivirus software up to date: Many major antivirus programs have been updated to detect and block or remove WannaCrypt. While most antivirus programs update automatically, you can manually open your antivirus program and check for updates just to be sure.
3. Don’t open email attachments that you are not expecting or click on links to unfamiliar sites. Check out my article Tips for Preventing Malware Infection for more info about this topic.
4. Always have a backup of your important files on a separate device such as a flash drive or external hard drive. As an added precaution, also have a file backup on a device that is disconnected from your computer, or subscribe to an online backup service such as Carbonite to keep a safe copy of your files offsite.

~Ted Eiler