PROTECTING YOURSELF

Introduction

The recent outbreaks of malware--WannaCry and NotPetya--are warnings that computer users must take care to protect their computers and personal data before it is too late. The three-prong defense of software updates, anti-malware software, and regular backups is key to protecting yourself from disaster before it strikes.

WannaCry and NotPetya

WannaCry is ransomware designed to take advantage of a vulnerability in SMB, a protocol designed by Microsoft for the sharing of files and printers between computers running Windows. Once the malware is installed on a Windows computer, it encrypts the user's files and then demands a ransom of $300 in Bitcoin in order get a key to decrypt the files. After seven days, the price increases to $600. It also attempts to spread itself to other Windows computers on the local network, as well as random computers on the Internet. Although Microsoft had released a security patch for this vulnerability on May 14, 2017, many computers around the world were affected, as they did not have the most recent security patches. A notable development is that although Microsoft has ceased to release regular patches for older, unsupported operating systems such as Windows XP and Server 2003, it did release special patches for these as well. (See Useful Links below for more information.)

NotPetya is ransomware that first appeared in June 2017. It infects the master boot record and encrypts the file system to prevent Windows from booting. It then requests a payment of $300 in Bitcoin in order to decrypt the computer. It is like WannaCry, in that it exploits a tool called EternalBlue, which is believed to have been developed by the NSA and later leaked by hackers on April 14, 2017. The same patch for protecting against WannaCry also protects against NotPetya. Unlike WannaCry, NotPetya cannot technically revert its changes. It appears to have been created more for causing damage and disruption of computer operations than making money as in the case of WannaCry.

Some victims have reportedly paid the ransom for malware such as WannaCry in order to regain access to critical data. However, experts generally recommend not paying the ransom. One reason is that there is no guarantee that the victim will be given the decryption key. Another is that the money could go to individuals, organized crime, terrorists, or rogue nations such as North Korea and be used to design more powerful malware tools. The recommendation is to restore from backups. In the worst case scenario, the victim may have to cut their losses and start over.

Protecting Yourself

Keeping Windows updated is important, as doing so can protect your computer from malware that is not stopped by anti-virus software. By default, Windows checks for and installs updates automatically. You may change this behavior by choosing whether updates are downloaded or installed automatically, and selecting a schedule for installing updates, so your work is not interrupted by unexpected reboots. If you select a time when not using the computer, you will want to be sure to leave the computer on.

Keeping up-to-date anti-virus software is also important. Although it may not detect every new threat (especially zero-day threats), it along with current Windows updates will help protect your computer from new malware threats. If you use an older operating system such as Windows XP, it is advisable that you upgrade to a newer version of Windows, or switch to alternate operating system such as Linux.

Lastly, making regular updates of your data is critical to recovering from such threats, as well as from theft, fire, flood, and hard drive failures. I highly recommend redundant backups. Backing up to multiple hard drives and flash drives is one way to protect yourself should one backup device fails or is lost. Storing them offsite is better yet, in case of fire, flood, or theft. Cloud backup services provide such security without the need of physically moving devices from your home or office to another location.

Please be aware that when using devices such as flash drives, USB hard drive, and network drives, you should unplug or turn them off when not using them. Any device that your computer is continuously connected to could be encrypted as well when ransomware hits. Some cloud solutions such as Microsoft OneDrive, Google Drive, and Dropbox can be vulnerable as well, as they provide a means of constantly synchronizing a folder on your computer with one in the cloud. This could allow for your data in the cloud to be lost to ransomware, once it encrypts the local copies.

Useful Links

Wikipedia on WannaCry: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Krebs on WannaCry: https://krebsonsecurity.com/2017/05/global-wana-ransomware-outbreak-earned-perpetrators-26000-so-far/

Wikipedia on Petya: https://en.wikipedia.org/wiki/Petya_(malware)

Krebs on Petya: https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/

WannaCry Patch for Windows XP, 8: https://krebsonsecurity.com/2017/05/microsoft-issues-wanacrypt-patch-for-windows-8-xp/

Security Update for Windows Operating Systems: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx