The Spyware and Malware War

Author: Brian Lisse

Malware is a general name given to any poisonous code that infects your computer without your permission. These unbidden infections entwine themselves into your computer's operating system, often causing system slowdowns, errors, or compromising your personal data. It has become quite common to receive a virus or malware-infected email from a trusted friend or family member. Likewise, many legitimate websites get hacked and embedded with poisonous code without the knowledge of the sites' owners.

In the early days of computers, malware was primarily just viruses. Created by early coders and programmers, it was purely malicious, much like someone egging your house or keying your car. Early virus writers did it to prove themselves and that they could do it, and sometimes because a simple program started replicating and spreading by mistake. Those days are long since over, and in the current era, most malware is made for the purpose of stealing from you and others.

Website-based infections have become very prevalent and the most common vector for infecting a computer. Many legitimate websites get hacked and embedded with poisonous code without the knowledge of the sites' owners. A user will often become infected just by browsing to an infected site. You need not click on anything at that page to get infected. The Java and ActiveX scripts automatically initiate the poisoned scripts and infect your system. Pop-up ads are routinely used to infect computers. Simply visiting the infected site is enough to infect your system. Flash based ads at sites like Yahoo, CBS Sports, Livestrong, ebay, etc. have been found to infect people's computers. Newer types of Malware can even encrypt all the data on your hard drive, rendering it completely useless. It is more vital than ever to have proper anti-malware and good backups that you can restore from, lest you lose everything! These various infections are incredibly invasive. Key loggers are specifically designed to monitor keystroke, stealing user names, passwords, credit card numbers, and banking account numbers without the user's knowledge.

Malware variants can take many forms such as:

1. **Viruses**- infecting the host computer, they gum it up, slowing down boot up and shutdown time, making your computer slow, sometimes generating blue screens or even lock-ups.

2. **Worms**- Spreading to your files, infecting your programs and operating system files, making them no longer function properly.

3. **Bots**- code that uses your computer to send out requests via the internet for concerted attacks on institutions (banks, Pentagon, big corporations, etc.)

4. **Keyloggers**- recording your keystrokes, they send that information to sites that collect it and sift through it for your passwords, bank accounts, credit card info, etc.

5. **Hijackers and Adware**- These products usually redirect your Web requests to sites advertising products or services, often with pop-ups for these products that repeatedly pop up on your screen.

6. **Rootkits**- Malware that entwines itself in the boot sector of your hardrive, often outside the partition table in the Master Boot Record, traditional cleaners cannot even detect its presence since it does not reside in the OS or file system.

7. **Ransomware**- Locks you out of your computer or data, it demands that you send money to unlock your system or unencrypt your data. Variants that encrypt your data are impossible to decrypt without the key, and your only chance it retrieving the data is from backups made before your system got infected.

Cleaning an infected system

Many of these variants entwine themselves in the operating system and files, making it so that an end user cannot remove it themselves without professional assistance. A professional cleaning by a company like Madison Computer Works means making an image of your hard drive (a snapshot backup of your OS, applications, and data, then scanning your system with as many as 5 different cleaners, and can take anywhere from 1-2 hours of labor to get it cleaned off properly. Often the removal of malware can destabilize the operating system, requiring a repair install of the OS, or it can require affected programs and applications to be reinstalled. These days, cleaning off an infection properly is best done by professionals since current malware is so invasive and pernicious.

Prevention and Protection

Traditionally, the most common way to protect against a virus infection was by installing an antivirus (AV) program on your computer, and making sure that the virus definition files (VDF) were kept up-to-date. With an average of 33 million variants of malware a month, these traditional anti-malware definition files have become so large that they need to be updated daily, and slow computers down, sometimes to a crawl. Thankfully, new cloud-based technology has evolved to more efficiently combat this onslaught. Not all AV products are equal in their ability to detect new and undiagnosed viruses, but we have put much time and energy into finding the best possible protection available. Webroot's SecureAnywhere uses the latest scans for malware in the cloud before data even reaches your computer. Because the definition files run on large servers up in the cloud (rather than on your computer), SecureAnywhere won't consume your computer's resources (RAM, processor, etc.). Utilizing this technology, your computer runs much faster, without the need for pesky definition updates nor slow boot up speeds, due to the loading of those massive definition files. We have found Secure Anywhere to be the best anti-malware product on the market today.

The best way to prevent new infections is a two-pronged approach, using both SecureAnywhere and an ad blocker, as well as keeping your OS and browsers up to date. Definition-based protection alone is no longer able to protect your system from the overwhelming number of poisonous variants injected into legitimate websites an ads, every day. The majority of recent infections have been coming through the web browser, but it is still important to protect yourself from infections that can, and do, come through traditional vectors such as email or USB flash drives. Infections are more than just a nuisance; they can compromise sensitive and personal information, and infect friends and family. Don't just live with these parasites.