The Monthly Security Awareness Newsletter for Everyone

Stop That Malware

Overview

You probably have heard of terms such as virus, Trojan, ransomware, or rootkit when people talk about cyber security. These are different types of malicious programs, called malware, that cyber criminals use to infect computers and devices. Once installed, they can do whatever they want. Learn what malware is, what danger it poses, and most importantly, what you can do to protect yourself from it.

What Is Malware?

Simply put, malware is software--a computer program--used to perform malicious actions. This term is a combination of the words malicious and software. Cyber criminals install malware on your computers or devices to gain control over them. Once installed, malware can enable criminals to spy on your online activities, steal your passwords or files, or use your system to attack others. Malware can even take control of your own files, demanding that you pay a ransom to get them back. Many people believe that malware is a problem only for Windows computers. Unfortunately, malware can infect any device, from Mac computers and smartphones to DVRs and security cameras. The more computers and devices cyber criminals infect, the more money they can make. Therefore, everyone is a target, including you.

Protect Yourself - Stop Malware

You may think that all you have to do is install a security program like anti-virus software and you are safe from getting infected. Unfortunately, anti-virus cannot stop all malware. Cyber criminals are constantly developing new and more sophisticated malware that can evade detection. In turn, anti-virus vendors are constantly updating their products with new capabilities to detect malware. In many ways it has become an arms race, and the bad guys are usually one step ahead. Since you cannot rely on anti-virus alone, here are additional steps you should take to protect yourself:

Cyber criminals often infect computers or devices by exploiting vulnerabilities in your software. The more current your software is, the fewer vulnerabilities your systems have and the harder it is for cyber criminals to infect them. Make sure your operating systems, applications, browser and browser plugins, and devices are always updated and current. The easiest way to ensure this is to enable automatic updating whenever possible.

A common way cyber criminals infect computers or mobile devices is by creating fake computer programs or mobile apps, posting them on the Internet, and then tricking you into downloading and installing one. Only download and install programs or apps from trusted online stores. Also, stay away from mobile apps that are brand new, have few positive reviews, are rarely updated, or have been downloaded by a small number of people. No longer using a computer program or mobile app? Delete it.

Cyber criminals often trick people into installing malware for them. For instance, they might send you an email that looks legitimate and contains an attachment or a link. Perhaps the email appears to come from your bank or a friend. However, if you were to open the attached file or click on the link, you would activate malicious code that installs malware on your system. If a message creates a strong sense of urgency or seems too good to be true, it could be an attack. Be suspicious, common sense is often your best defense.

Regularly back up your system and files to Cloud-based services, or store your backups offline, such as on disconnected external drives. This protects your backups in case malware attempts to encrypt or erase them. Backups are critical. They are often the only way you can recover from a malware infection.

Ultimately, the best way to defend against malware is to keep all your software and devices up-to-date, install trusted anti-virus software when possible, and be alert for anyone attempting to trick you into infecting your own system. When all else fails, regular backups are often the only way you can recover.

Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Lenny Zeltser *combats malware by creating endpoint security products at Minerva Labs and teaching at the SANS Institute. Lenny is active on Twitter as @lennyzeltser and writes a security blog at zeltser.com.*

Resources

Ransomware:	https://www.sans.org/u/EdI
Backups:	https://www.sans.org/u/EdN
Stop That Phish:	https://www.sans.org/u/EdS