OUCH! | February 2014

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- What Is Malware
- Who and Why
- Protecting Yourself

What Is Malware

Overview

You may have heard of terms such as virus, worm, trojan or rootkit when people discuss cyber security. These terms describe types of programs used by cyber criminals to infect and take over computers and mobile devices. Today all of these different terms are now simply called malware. In this newsletter we will explain what malware is, who is developing it, why, and what you can to do protect yourself against it.

Guest Editor

Lenny Zeltser focuses on safeguarding customers' IT operations at NCR Corp and teaches malware combat at the SANS Institute. Lenny is active on Twitter as **@lennyzeltser** and writes a security blog at **blog.zeltser.com**.

What Is Malware

Simply put, malware is software, a computer program used to perform malicious actions. In fact, the term malware is a combination of the words malicious and software. The end goal of most cyber criminals is to install malware on your computers or mobile devices. Once installed, these attackers can potentially gain total control of them. Many people have the misconception that malware is a problem only for Windows computers. While Windows is widely used, and thus a big target, malware can infect any computing device, including smartphones and tablets. In fact, the prevalence of malicious software infecting mobile devices is steadily growing. In addition, remember that everyone is a target, including you. The more computers and mobile devices cyber criminals infect, the more money they can make. These criminals usually do not care whom they infect, just as long as they infect as many people as possible.

Who and Why

Malware is no longer created by just curious hobbyists or amateur hackers, but by sophisticated cyber criminals to help them achieve specific goals. These goals can include stealing confidential data, harvesting logins and passwords, sending spam emails, launching denial of service attacks, extortion or identity theft. For example, malware known as Cryptolocker is used by cyber criminals to infect and encrypt all of the files on your computer. Once infected and encrypted, these cyber criminals then demand a ransom in exchange for decrypting your files.

What Is Malware

The people who create, deploy and benefit from malware can range from individuals acting on their own to well-organized criminal groups or government organizations. In addition, the people that are creating today's sophisticated malware are often dedicated to that purpose; developing malware is their full-time job. In fact, once they develop their malware, they often sell it to other individuals or organizations and provide regular updates and support to their "customers." Once purchased, other criminals make money by installing the malware on millions of unsuspecting victims' systems, creating a botnet of infected systems. This botnet becomes a remotely controlled army, which the cyber criminal can then use for their own purposes, or sell the infected computers to other cyber criminals.

The best way to protect yourself against malware is to ensure your devices are updated, have current anti-virus if possible and, ultimately, be on the alert for attacks.

Protecting Yourself

A common step to protect your computers and mobile devices from malware is to install anti-virus software from trusted vendors. Anti-virus, sometimes called anti-malware, is security software designed to detect and stop malicious software. However, anti-virus cannot block or remove all malware. Cyber attackers are constantly innovating, developing new and more sophisticated attacks that can bypass anti-virus programs. In turn, anti-virus vendors are then constantly updating their products with new capabilities to detect new malware. In many ways it has become an arms race, with both sides attempting to outwit the other. Unfortunately, cyber criminals almost always have the upper hand. As such, remember that while anti-virus can detect and block a lot of malware, attackers are always creating new versions that will be missed. As a result, you cannot rely on just anti-virus to protect you. You have to take additional steps to protect yourself.

First, make sure your operating systems and applications are enabled to automatically install security updates. The more current your software is, the harder it is for cyber criminals to infect your computers or mobile devices.

Second, remember that you are one of the best defenses against malware. Malware infections often involve social engineering, which is nothing more than the attackers tricking or fooling you into installing the malware for them. One common example is phishing attacks. These are emails that appear legitimate but are really fakes designed to trick

What Is Malware

you into infecting your computer. For example, a cyber criminal may send you an email pretending to come from your bank asking you to click on a link. If you click on the link you are taken to a website that automatically attempts to hack into and infect your computer. Or perhaps they email you a notice that your package could not be delivered and ask you to open the attached tracking document, which will infect your computer when opened.

Social engineering attacks also happen over other technologies, such as your phone. For example, hackers may call you pretending to be Microsoft Technical Support and inform you that your computer is infected. Their story is a lie, however, and your computer is most likely fine. Their goal is to fool you into believing that you are infected and then trick you into either giving them remote access to your system or buying their security software, which is nothing more than malware. Use common sense. If a phone call or message seems odd, suspicious or too good to be true, it most likely is.

Ultimately, the best way to defend against malware is keep your software up-to-date, install trusted anti-virus software from well-known vendors and be alert for anyone attempting to fool or trick you into infecting your own computer.

Become A Security Professional - SANS 2014

If you haven't been to SANS 2014 training in Orlando, you can't miss this on April 5-14! One of our biggest events of the year, you will have countless opportunities to develop and expand your network of security experts and friends, and learn more than you can imagine from the top instructors in the cybersecurity industry. For more information, please visit http://www.sans.org/event/sans-2014/welcome.

Resources

OUCH Phishing:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

OUCH Securing Your Computer:
http://www.securingthehuman.org/resources/newsletters/ouch/2012#december2012

You Are the Target Poster:
http://www.securingthehuman.org/resources/posters

License