OUCH! | March 2016

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- What Is Malware?
- Who Creates Malware?
- Protecting Yourself

# What Is Malware?

## Overview

You may have heard of terms such as virus, trojan, ransomware, or rootkit when people discuss cyber security. All of these words describe the same thing, types of programs used by criminals to infect computers and devices. A common term used to describe all these different programs is the word malware. In this newsletter, we will explain what malware is, who creates it and why, and most importantly, 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 **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. Cyber criminals install malware on your computers or devices to gain control over them or gain access to what they contain. Once installed, these attackers can use malware to spy on your online activities, steal your passwords and files, or use your system to attack others. Malware can even deny access to your own files, demanding that you pay the attacker a ransom to regain control of them.

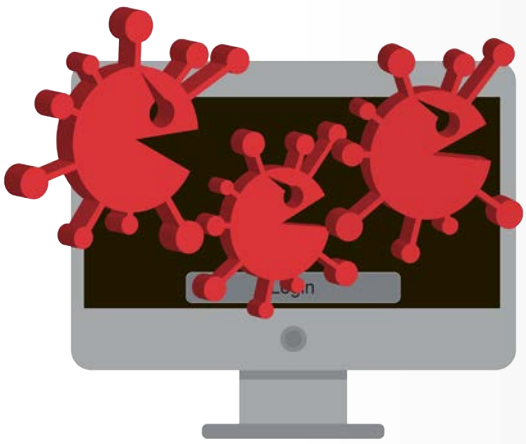
Many people have the misconception that malware is a problem only for Windows computers. While Windows is widely used (and thus a big target), malware can infect any device, including Mac computers, smartphones, and tablets. The more computers and devices cyber criminals infect, the more money they can make. Therefore, everyone is a target, including you.

## Who Creates Malware?

Malware is no longer created by just curious hobbyists or amateur hackers, but by sophisticated cyber criminals. Their goal is to make money from your infected computer or device, perhaps by selling the data they've stolen from

## What Is Malware?

you, sending spam emails, launching denial of service attacks, or performing extortion. The people who create, distribute, and benefit from malware can range from individuals acting on their own to well-organized criminal groups or even government organizations. People who are creating today's sophisticated malware are often dedicated to that purpose, developing malware as their full-time job. In addition, once they develop their malware, they often sell it to other individuals or organizations, even supplying their "customers" with regular updates and support.



*Protect yourself from malware by being skeptical of suspicious messages, keeping your devices updated, and have current anti-virus installed when possible.*

### Protecting Yourself

A common step to protecting yourself is to install anti-virus software from trusted vendors. Such tools, sometimes called anti-malware software, are designed to detect and stop malware. However, anti-virus cannot block or remove all malicious programs. Cyber criminals are constantly innovating, 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, with both sides attempting to outwit the other. Unfortunately, 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 their software. The more current your software is, the fewer vulnerabilities your systems have and the harder it is for cyber criminals to infect them. Therefore, make sure your operating systems, applications, and devices are enabled to automatically install updates.
- A common way cyber criminals infect mobile devices is by creating a fake mobile app, posting it on the Internet, and then tricking people into downloading and installing it. As such, only download and install apps from trusted online stores. In addition, only install mobile apps that have been posted online for a long time, downloaded by a large number of people, and have numerous positive reviews.

## What Is Malware?

- On computers, use a standard account that has limited privileges rather than privileged accounts such as "Administrator" or "root." This provides an additional protection by preventing many types of malware from being able to install themselves.
- 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, is confusing, 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 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 system.

## Secure Development Life Cycle: Agile Development

Be sure to check out our free resources, including our blog and Video of the Month. This month, we're covering Software Development Life Cycle: Agile Development. View the video at: https://www.securingthehuman.org/u/8x9.

## Resources

| | |
|---|---|
| Phishing: | https://securingthehuman.sans.org/ouch/2015#december2015 |
| Social Engineering: | https://securingthehuman.sans.org/ouch/2014#november2014 |
| Securely Using Mobile Apps: | https://securingthehuman.sans.org/ouch/2015#january2015 |
| Securing Your New Tablet: | https://securingthehuman.sans.org/ouch/2016#january2016 |
| Backups: | https://securingthehuman.sans.org/ouch/2015#august2015 |

## License