Malware Basics: What You Need to Know

Devolutions

YOU CAN PROTECT YOUR DEVICES AND ORGANIZATION AGAINST MALWARE ATTACKS

Before you can protect your devices and organization against malware attacks, you need to know what you're fighting against – and I'm sorry to say, but it's really scary. It kind of makes the Night King from Game of Thrones seem like our cute and cuddly Waykee plush owl mascot.

To help you prepare for battle, below are 6 different types of malware, followed by 6 best practices for staying safe, and 2 malware myths to avoid.

Types of Malware

Virus: This type of malware attaches itself to a document or a legitimate program. It usually has the capacity to replicate itself repeatedly, in order to infect and corrupt other files without its victims' knowledge.

Trojan Horse: This type of malicious malware is usually hidden or embedded in an email attachment or in a useful or interesting program such as a computer game, in order to encourage a user to install it. One of the most insidious (and ironic) types of Trojan Horses is a program that claims to clear your computer of viruses, but instead delivers viruses to your computer.

Botnet: This type of malware is a network or collection of compromised computers and routers (IoT), which are linked to the Internet in a coordinated way for malicious purposes. Compromised machines are often turned into robot "zombies" and used to send spam, spread malware, and launch cyberattacks. A Botnet is also known as a zombie network.

Spyware: This type of malware is installed on a computer or device without the victim's awareness. Once activated, spyware collects and transmits information about a person or organization, such as passwords and credit card numbers.

Ransomware: This type of malware uses encryption to block access to a computer system or fines until a specific amount of money is paid — usually by cryptocurrency (e.g. Bitcoin), since the transaction cannot be traced or refunded. If the ransom is not paid, then the victim's files are destroyed.

Computer Worm: This type of malware is a self-replicating program that copies itself from computer to computer. Rather than infect files, its main purpose is to use resources such as computer memory and network bandwidth to inflict damage.

6 Best Practices to Prevent Malware

The bad news is that there is no 100% bulletproof way to eliminate malware. But the good news is that you significantly lower your chances of getting attacked and victimized by malware if you implement these best practices:

1. Install Anti-Virus and Anti-Malware Software

It goes without saying — but we'll say it anyway — that installing good anti-virus software and anti-malware software is a critical first step in keeping your computer and network safe. Make a habit of analyzing:

- Email attachments
- Files downloaded directly from the Internet
- USB sticks, memory cards and other portable storage devices before using them

Also, never disable or grant exceptions to your anti-virus or anti-malware software unless you really know what you're doing. It's kind of like leaving your house unlocked. If you're standing at the door for a few seconds, then it's OK. But if you're asleep, away, or in your geek cave playing games or streaming videos, then lock the door!

2. Only Visit Legitimate Sites

Only buy and download apps from legitimate sites, and never open or run a program from an unknown or doubtful source. You should also avoid browsing websites that deliver pirated material, as these are major malware sources (plus, downloading illegal content can expose you/your organization to serious legal penalties).

3. Think Before You Click

Always be careful if you receive a suspicious or unsolicited email — even if it seems to be from a colleague, family member or friend. Here are a few tips to keep in mind:

- Don't click on a link or a button in a message. Instead, hover over the link to see where it is taking you.
- Don't download or open email attachments from someone you don't know.
- When browsing websites, carefully read the content of a pop-up window before choosing an option or accepting an offer. You may be shocked at what you are being asked to agree to!

4. Read with a Sharp Eye

One of the principal methods used to spread malware is to scam users through social engineering. Pay close attention to the content of an email. Is the formatting strange and unfamiliar? Are there many grammar and spelling errors? When in doubt, contact the sender directly and confirm. Do this by calling them or sending a new email. Don't reply to the suspicious email.

5. Keep Everything Updated

Update your browsers, operating system and plugins. Updates are often released to patch any security liabilities. With updates, there is one rule to follow: the sooner the better.

6. Watch Out for the Warning Signs

If despite following these best practices you notice that your computer has slowed down or is repeatedly crashing, if there is excessive hard drive activity, if you're getting overrun by popups, or if there have been changes made to your browser's configuration (e.g. different home page), then immediately contact your technical support team. They'll either walk you through the scanning process, or if they're using a tool like Wayk Now, they can manage the process on their end while you wait (and hope for the best!).

Malware Myths

In closing, I'd like to highlight two persistent malware myths that keep getting people into a lot of trouble:

Myth 1 - If you install antivirus software on your computer, you can block all viruses.
FALSE! Antivirus software are not an absolute foolproof solution against malware. The effectiveness depends largely on how robust and up-to-date it is. Moreover, any antivirus needs to be supplemented by other tools such as antimalware software and antispyware software.

Myth 2 –If you use a secure connection like encrypted Wi-Fi, you're always protected against spyware.
FALSE! Using a secure connection won't protect you against spyware. It may not even protect you against hackers, which is why you should always use a good VPN when connecting over Wi-Fi.

The Bottom Line

The malware universe is getting worse, as cyber criminals keep creating new threats and variants of existing threats. Fortunately, if you know what you're up against and follow best practices and avoid myths, then you'll stay safe instead of becoming a victim. And you won't even need dragons or wildfire!