HOW TO PREVENT MALWARE

Malicious Software, also known as Malware, takes many forms. Insidious and potentially catastrophic, viruses, trojans, worms, and the like constantly threaten businesses. The good news? There are ways to prevent becoming a victim of Malware. Let's look at what Malware is, what forms it takes, and the best ways to block or mitigate an attack.

WHAT IS MALWARE?

Companies need to understand Malware to understand how it can hurt their business. Malware is programming or software that installs itself on a system. The coding in the software is designed to cause extensive damage to data and systems or to gain unauthorized access to a network. Malware can spread throughout your organization's computers. Most strains are disseminated via a link or executable file sent through an email.

MALWARE EXAMPLES

Malware is an unfortunate and all too common tactic employed by hackers. Computer Viruses, Keyloggers, Spyware, Trojan Horses, and other examples of Malware are issues that halt the effectiveness of operating your business and threaten sensitive data. Let's take a look at some of the most common types.

COMPUTER VIRUS

A Computer Virus, much like the biological type, spreads quickly and causes damage to data and software. Viruses are aimed at disrupting systems and causing major operational issues - resulting in data loss and leakage. Originating when the infected file is opened, the Virus spreads from the original document or software it is attached to via networks, drives, file sharing programs, or the infected email attachment.

KEYLOGGER

A Keylogger is a Malware that falls under the category of Spyware. When a keylogger is installed on a system, it records every keystroke. The intent of Keylogging is to gain fraudulent access to passwords and other confidential information. Not all Keyloggers are illegal. There are legitimate applications. For example, keyloggers are frequently used by IT departments to troubleshoot issues.

SPYWARE

On a broader scope, Spyware is designed to “spy” on the user of the infected computer. This type of Malware obtains sensitive data and transmits it from the user’s hard drive to a third party without your consent. Spyware can also affect network and device performance causing a slow down in daily user activities.

TROJAN HORSE

A Trojan Horse is Malware that pretends to be legitimate software. It is typically hidden as an attachment or a free-to-download file in an email. Once the recipient clicks on the attachment or link, the malicious code is transferred onto the user’s device. It will then execute a task such as gaining backdoor access to corporate systems, spying on users’ online activity, or stealing sensitive data.

HOW TO PREVENT MALWARE

Now that you know what Malware is, how do you protect your systems from attack? There are two sides to prevention: protective tools and user vigilance.

PROTECTIVE TOOLS

Taking steps to implement the protective tools necessary to prevent a malware attack is relatively simple. They include:

1. **Install Antivirus software**
2. **Regularly update all software on your systems**
3. **Only buy apps from trustworthy sources**
4. **Install a Firewall**
5. **Backup data regularly**

USER VIGILANCE

Employee education is key to prevention. Arming employees with knowledge will ensure they know the risks and the procedures to prevent an attack. Phishing is the easiest way for a hacker to dupe an employee into installing Malware on a device. When in doubt, don't click that link!

HOW TO STOP A MALWARE ATTACK

What does your organization do if you have been infected with Malware? There are immediate steps that you must take to mitigate the extent of damage caused:

1. **Promptly disconnect infected hardware, computers, laptops, and tablets, from the network, whether hardwired or Wi-FI enabled.**
2. **Disable any access the virus/malware may have to any core areas. That may include physically disconnecting from the core network connections, including switches.**
3. **Reset all passwords, especially for administrator and other system accounts. Be sure to verify you are not locking yourself out of systems needed for recovery!**
4. **Safely wipe any infected devices and reinstall the Operating System.**
5. **Reconnect devices to a clean network.**
6. **Download, install, and update the Operating System.**
7. **Install, update, and run Antivirus software.**
8. **Verify that your backup and devices are free from Malware, then restore data from the backup.**
9. **Monitor Antivirus Scans to identify if any infection remains.**

FUSE3 OFFERS BEST-IN-CLASS SOLUTIONS

We offer methods to ensure that your sensitive data is not breached. FUSE3 uses comprehensive detection technology with unparalleled threat awareness to detect suspicious user-installed apps or data theft. With our online reporting, your entire network, including The Cloud, email, and personal files, will be monitored for any suspicious activity. In addition, we offer Security Awareness Training.

Don't paint a target on your systems!

CONTACT US TODAY

916-484-1780

FUSETHREE.COM | FUSE3