June 2023

SecurityAwarenessNews

the security awareness newsletter for security aware people

Avoiding Malware Infections

Malware Motives

How Malicious Infections Spread

Browsing for Malware

Malware Motives

Malware is the umbrella term covering any form of malicious software or code that alters the functionality of computers and smart devices. There are many types that serve a variety of purposes for cybercriminals.

Avoiding malware infections is a fundamental security objective. It's also important to gain an understanding of the motives behind malicious infections. Here are a few of the most common malware use cases.

Data Theft

Confidential information carries a lot of value. Trade secrets, intellectual property, personal information (full names, addresses, national ID numbers), and passwords are all examples of data that malware is designed to steal.

Espionage

Spyware is a type of infection that provides attackers access to webcams and microphones. It can also be used to monitor email communications or other messaging platforms.

Account Takeover

When an attacker is able to gain control of online accounts, they can cause a lot of irreversible damage. Email, for example, could be used by cybercriminals to impersonate you and scam your contacts.

Financial Gain

Stealing money is the main goal behind ransomware, which locks systems and data until a ransom is paid. It's one of the most common attacks targeting people and organizations around the world.

Service Disruption

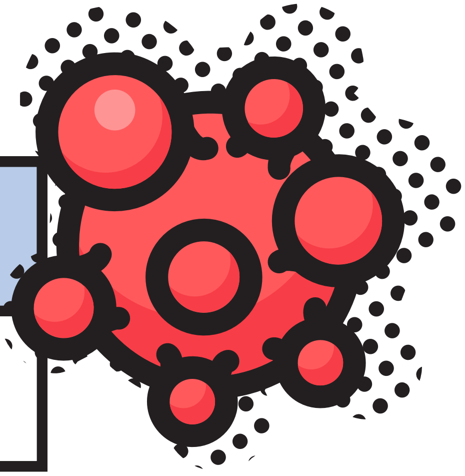
In the case of DDoS (distributed denial-of-service), attackers cause internet and network outages by flooding servers with more information than they can handle.

Website Defacement

A form of digital vandalism, website defacement occurs when cybercriminals make visual alterations to an organization's site, usually for political reasons.

As you can see, malware is used for many reasons, some of which are more dangerous than others. No matter the case, everyone should remain motivated to keep their machines and devices healthy. You can do that by prioritizing security awareness at work, at home, and everywhere in between.

How Malicious Infections Spread



ATTACK METHOD: PHISHING

Phishing is a common scam that uses email and other forms of communication to mislead people into clicking malicious links or downloading infected attachments. It's the top attack method in the cybercriminal's playbook.

PREVENTION TECHNIQUE: You can spot phishing scams by looking for common warning signs such as threatening or urgent messages, misspellings, and unexpected attachments.

ATTACK METHOD: USB DRIVES AND CABLES

One of the simplest ways to spread malware is by planting infected USB flash drives and cables in public areas. This tactic preys on human curiosity. Many people feel tempted to plug in a USB device when they find one.

PREVENTION TECHNIQUE: Only use the USB devices you own. If you find a random drive or cable, don't plug it in. Instead, report them immediately.

ATTACK METHOD: MOBILE APPS

The main smartphone app stores have robust vetting processes designed to prevent cybercriminals from uploading malicious apps. Unfortunately, some still get through. Malicious apps can steal data or give attackers access to bank accounts.

PREVENTION TECHNIQUE: Do a little bit of research and only download apps from legitimate developers. Never install anything on work-issued devices without approval.

ATTACK METHOD: SOFTWARE VULNERABILITIES

Cybercriminals are constantly scanning for software vulnerabilities that allow them to bypass security controls. It's one of the main reasons developers issue ongoing updates. Failure to install those updates could allow attackers to hack into systems without detection.

PREVENTION TECHNIQUE: Be sure to keep your personal devices updated at all times. At work, follow policy regarding software and device management.

Browsing for Malware

The most likely way malware spreads is by typical phishing attacks that contain malicious links or attachments. In some cases, however, the attackers wait for people to come to them when browsing the internet. Here's how:

Compromised Websites

It's possible for legitimate websites to host malicious code that can install malware on a visitor's computer. This happens when a site is improperly configured or when various components are left outdated. The code will scan the visitor's device for vulnerabilities that allow it to automatically install the malware.

Watering Hole Attacks

These attacks occur when cybercriminals research and track which sites employees visit the most. They will then attempt to compromise those sites by injecting malicious code into them, which can then infect a visitor's computer. The name of the attack refers to how hunters often sit and wait at a natural resource their targeted prey is likely to visit (such as a pond or river).

Malvertising

Short for malicious advertising, malvertising uses pop-up advertisements that cause infections when clicked. Just like in typical phishing attacks, the advertisements are designed to be intriguing and encourage internet users to click without giving it much thought.

Malicious Push Notifications

Browser push notifications are customized messages that deliver information to users. While they can serve useful purposes, they're also abused by malicious hackers. Security researchers have identified that push notifications can be used to deliver malicious advertisements or prompt users to install software.

While it can be difficult to know if you're visiting a compromised website, there are a number of ways to stay safe while browsing.

Here at work, always follow policies and never bypass any security controls. Those simple actions help protect data, systems, and everyone associated with our organization.

In your personal life, follow these guidelines:

- Keep your browser updated. Remember: Developers often issue updates to fix crucial security flaws. An outdated browser makes for an easy target.
- Utilize security plugins. Many browsers offer free plugins that can help keep you safe, such as ad blockers, which eliminate annoying (and dangerous) pop ups.
- Think before you click. Avoid clicking on pop ups and never install anything when randomly prompted to do so by a website.

SAC the security awareness™ COMPANY
a KnowBe4 company