2020

Protecting Against Malicious Code

DHS Security Tip (ST18-004)

INCEPTUS | CAPE CORAL, FLORIDA 33904

Contents

What is malicious code?

Malicious code is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include viruses, worms, and Trojan horses.

- **Viruses** have the ability to damage or destroy files on a computer system and are spread by sharing an already infected removable media, opening malicious email attachments, and visiting malicious web pages.
- **Worms** are a type of virus that self-propagates from computer to computer. Its functionality is to use all of your computer's resources, which can cause your computer to stop responding.
- **Trojan Horses** are computer programs that are hiding a virus or a potentially damaging program. It is not uncommon that free software contains a Trojan horse making a user think they are using legitimate software, instead the program is performing malicious actions on your computer.
- **Malicious data files** are non-executable files—such as a Microsoft Word document, an Adobe PDF, a ZIP file, or an image file—that exploits weaknesses in the software program used to open it. Attackers frequently use malicious data files to install malware on a victim's system, commonly distributing the files via email, social media, and websites.

How can you protect yourself against malicious code?

Following these security practices can help you reduce the risks associated with malicious code:

- **Install and maintain antivirus software.** Antivirus software recognizes malware and protects your computer against it. Installing antivirus software from a reputable vendor is an important step in preventing and detecting infections. Always visit vendor sites directly rather than clicking on advertisements or email links. Because attackers are continually creating new viruses and other forms of malicious code, it is important to keep your antivirus software up to date.
- **Use caution with links and attachments.** Take appropriate precautions when using email and web browsers to reduce the risk of an infection. Be wary of unsolicited email attachments and use caution when clicking on email links, even if they seem to come from people you know.
- **Block pop-up advertisements.** Pop-up blockers disable windows that could potentially contain malicious code. Most browsers have a free feature that can be enabled to block pop-up advertisements.
- **Use an account with limited permissions.** When navigating the web, it's a good security practice to use an account with limited permissions. If you do become infected, restricted permissions keep the malicious code from spreading and escalating to an administrative account.

- **Disable external media AutoRun and AutoPlay features.** Disabling AutoRun and AutoPlay features prevents external media infected with malicious code from automatically running on your computer.
- **Change your passwords.** If you believe your computer is infected, change your passwords. This includes any passwords for websites that may have been cached in your web browser. Create and use strong passwords, making them difficult for attackers to guess.
- **Keep software updated.** Install software patches on your computer so attackers do not take advantage of known vulnerabilities. Consider enabling automatic updates, when available.
- **Back up data.** Regularly back up your documents, photos, and important email messages to the cloud or to an external hard drive. In the event of an infection, your information will not be lost.
- **Install or enable a firewall.** Firewalls can prevent some types of infection by blocking malicious traffic before it enters your computer. Some operating systems include a firewall; if the operating system you are using includes one, enable it.
- **Use anti-spyware tools.** Spyware is a common virus source, but you can minimize infections by using a program that identifies and removes spyware. Most antivirus software includes an anti-spyware option; ensure you enable it.
- **Monitor accounts.** Look for any unauthorized use of, or unusual activity on, your accounts—especially banking accounts. If you identify unauthorized or unusual activity, contact your account provider immediately.
- **Avoid using public Wi-Fi.** Unsecured public Wi-Fi may allow an attacker to intercept your device's network traffic and gain access to your personal information.

What do you need to know about antivirus software?

Antivirus software scans computer files and memory for patterns that indicate the possible presence of malicious code. You can perform antivirus scans automatically or manually.

- **Automatic scans** – Most antivirus software can scan specific files or directories automatically. New virus information is added frequently, so it is a good idea to take advantage of this option.
- **Manual scans** – If your antivirus software does not automatically scan new files, you should manually scan files and media you receive from an outside source before opening them, including email attachments, web downloads, CDs, DVDs, and USBs.

Although anti-virus software can be a powerful tool in helping protect your computer, it can sometimes induce problems by interfering with the performance of your computer. Too much antivirus software can affect your computer's performance and the software's effectiveness.

- **Investigate your options in advance.** Research available antivirus and anti-spyware software to determine the best choice for you. Consider the amount of malicious code the software recognizes and how frequently the virus definitions are updated. Also, check for known compatibility issues with other software you may be running on your computer.

- **Limit the number of programs you install.** Packages that incorporate both antivirus and anti-spyware capabilities together are now available. If you decide to choose separate programs, you only need one antivirus program and one anti-spyware program. Installing more programs increases your risk for problems.

There are many antivirus software program vendors and deciding which one to choose can be confusing. Antivirus software programs all typically perform the same type of functions, so your decision may be based on recommendations, features, availability, or price. Regardless of which package you choose, installing any antivirus software will increase your level of protection and ultimately lower risk.

How do you recover if you become a victim of malicious code?

Using antivirus software is the best way to defend your computer against malicious code. If you think your computer is infected, run your antivirus software program. Ideally, your antivirus program will identify any malicious code on your computer and quarantine them, so they no longer affect your system. You should also consider these additional steps:

- **Minimize the damage.** If you are at work and have access to an information technology (IT) department, contact them immediately. The sooner they can investigate and “clean” your computer, the less likely it is to cause additional damage to your computer—and other computers on the network. If you are on a home computer or laptop, disconnect your computer from the internet; this will prevent the attacker from accessing your system.
- **Remove the malicious code.** If you have antivirus software installed on your computer, update the software and perform a manual scan of your entire system. If you do not have antivirus software, you can purchase it online or in a computer store. If the software cannot locate and remove the infection, you may need to reinstall your operating system, usually with a system restore disk. Note that reinstalling or restoring the operating system typically erases all your files and any additional software that you have installed on your computer. After reinstalling the operating system and any other software, install all the appropriate patches to fix known vulnerabilities.

Threats to your computer will continue to evolve. Although you cannot eliminate every hazard, by using caution, installing and using antivirus software, and following other simple security practices, you can significantly reduce your risk and strengthen your protection against malicious code.

How can Inceptus help?

With the ever-changing threat landscape, it is difficult to keep up with the changes and threats that evolve daily. That is why you need a dedicated team that is dedicated to keeping you safe, secure and protected while doing business on the Internet. Inceptus Protection

Plans are tailored security programs designed to address the gaps in your current ecosystems cyber security stance and provide the ultimate protection against hackers, malware/ransomware and downtime, all while protecting your brand & reputation.

- No matter where you have already made investments in you cyber posture Inceptus will assess your organization to identify gaps to your cyber defenses.
- A customized plan is designed to fill the gaps with plug-in cyber solutions and services to ensure that there are layers of defenses at each stage the cyber kill chain to stop even the most determined adversaries.
- Our comprehensive defense in depth strategies protect you against hackers by providing competing controls and processes between hackers and your data.
- All services are installed, hardened, managed, supported and monitored 24/7/365 by Inceptus' highly skilled analysts that follow tried and tested incident response processes and harden your ecosystem keeping you and your data stays safe.

Contact Inceptus

Inceptus
4825 Coronado Pkwy., Suite 1
Cape Coral, FL 33904
(239) 673-8130

General Questions:
info@inceptussecure.com
Support Questions:
soc@inceptussecure.com