MONTHLY
Cyber Security
Newsletter

Security Tips

Mississippi Department of Information Technology Services

Security Services Division

October 2016

Beware of Malware

From the desk of Thomas F. Duffy, Chair, MS-ISAC

The criminals who sell the fake antivirus have professional-looking websites, call centers where you can ask for help, and even different payment levels. After you buy and install the fake antivirus, it will infect your computer with malware instead of cleaning it and the malicious actors have your money!

Happy Cyber Security Awareness Month! October is not only National Cyber Security Awareness Month, it is also a time celebrate Halloween. Just like the disguises the trick'r'treaters wear, malware can use "costumes" to disguise what it is, and tricks you into installing it. These disguises come in many forms, but if you know what to look for, you can avoid the tricks.

Trojan Horses

Trojan Horses are a type of malware that misrepresent themselves to look legitimate, much like the Trojan Horse the Greek army used to enter Troy. Trojan Horses may be apps in smartphone stores, freeware and shareware, or even attachments to emails. The last is a very common spam technique and is often used with spam email campaigns that say you have a voicemail, fax, or shipping notification. When you click the attached document to hear the voicemail, or see the fax, or who has shipped you a package, the file opens to show you what you expect to see or hear, but in the background malware is downloading on to your computer.

Drive-by Downloads and Malvertising

Drive-by downloads occur when a program is downloaded onto your device without your permission. One way this happens is through malicious advertising or *malvertising*. You know the advertisements that appear on the edge of many webpages? When malicious actors purchase advertising space there, they can install malware in the advertisement. That means that if you see that malicious advertisement, which looks like any legitimate advertisement, the malware hidden in the advertisement will automatically try to download onto your device.

Social Engineering – Malicious Links

Social engineering relies on tricking you into taking an action, such as clicking on a link or opening an attachment. When the webpage or attachment opens, malware is installed on your device. Some types of social engineering use *link baiting* or other techniques to get you to click on the malicious link. Link baiting (which is not necessarily malicious) is when content providers use a teaser, such as "5 Things Preventing You From Being Rich" or "When I found about this trick, it blew my mind!", to get you to click on a link.

Social Engineering - Scareware

Scareware, such as ransomware and fake antivirus software, frequently use social engineering by making popup boxes look like messages from your computer. These messages look official and say things "System Warning!" and "Threats Found!" or "Your computer is infected. Click OK to remove the virus." They hope you'll click on the message, which allows the malware to be downloaded on to your computer. Often clicking anywhere on the message allows the malware to be downloaded, so instead hit the back button or on a Windows computer, use the Task Manager to close the popup window.

As if scareware wasn't bad enough, some versions of scareware use the scary warning messages to convince you to buy the malware. *Fake antivirus* malware most commonly uses this technique. Fake antivirus is malware that pretends to be real antivirus software. The criminals who sell the fake antivirus have professional-looking websites, call centers where you can ask for help, and even different payment levels. After you buy and install the fake antivirus, it will infect your computer with malware instead of cleaning it and the malicious actors have your money!

Minimize Your Risk

Avoid the tricks by being aware of the tactics:

- Only open an email attachment or click on a link if you're expecting it and know what it contains. Do not open email attachments or click on the links from unknown or untrusted sources.
- If something looks suspicious in an email from a trusted source, call and verify the email is legitimate.
- Use up-to-date antivirus protection and apply recommended patches/updates to your device.
- Only install third-party applications and software that you really need. Make sure it is from the vendor or the Android, Apple or Windows Store. Since the app stores allow third-parties to post and sell apps, make sure the app is from a trustworthy source.
- Use discretion when posting personal information on social media. This information is a treasure-trove to scammers who will use it to feign trustworthiness.

Provided By

MS-ISAC MULTI-STATE Information Sharing & Analysis Center

STOP | THINK CONNECT