Cyber Crime Prevention Flier

Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4485
Fax: 571.305.4189
E-mail:
cybercrimintel.cciu@us.army.mil

CCIU Web Page:
www.cid.army.mil/cciu.htm

CID Cyber Lookout
On Point for the Army

DISTRIBUTION:
This document is authorized for wide release with no restrictions.

"DO WHAT HAS TO BE DONE"

CPF 0023-12-CID361-9H **18 October 2012**

"MOBILE DEVICE MALWARE"

OVERVIEW:

The purpose of this Cyber Crime Prevention Flier is to inform all service members and Department of the Army civilians of the latest scam wherein cybercriminals are using malware to access mobile devices. As mobile devices increasingly take on the roles usually reserved for desktop and laptop computers, such as banking, emails, and storage of personal information, cyber criminals are taking note and targeting mobile platforms. Though mobile malware has been seen for virtually all mobile operating systems, the past several years has seen a surge in malware developed for Google's Android operating system. Whether used simply to show advertisements or to take full control of a user's device, mobile malware is a growing threat that can generally be avoided with just a few simple steps. CID elements are encouraged to brief supported installations and units on the contents of this Flier.

Background:

Mobile device malware can be used for a host of illegal purposes, including the display of advertisements, stealing user credentials or personal data, sending premium-rate SMS messages, downloading other threats, or allowing a remote cyber criminal unfettered access to the device. Many malicious applications combine several of these functionalities. The methods of delivery for mobile device malware vary as well. Some cyber criminals find vulnerabilities in mobile operating systems in order to force the installation of malware when visiting compromised websites. Yet others utilize social engineering by convincing a user that their device is infected by other malware and that the malicious application is a legitimate antivirus application. Most commonly, however, cyber criminals use icons and names of popular, legitimate applications to entice users into installing their malware. Some of these applications may even be available through the vendor's official application store (such as Google Play or the App Store) before they're detected and removed. Even more risky are third-party application stores, which may not offer the same level of vetting as the official versions.

TIPS TO AVOID BECOMING A VICTIM:

1. Download applications only from the official vendor application store (e.g. Apple App Store, Google Play, BlackBerry App World, Windows Phone Apps+Games Store, etc.)
2. Keep your device fully patched by applying all operating system updates when prompted.
3. Don't follow links sent via spam or other unsolicited email, or open their attachments.
4. If available for your operating system, consider installing a mobile antivirus program. Most platforms offer several free and low-cost applications from well-known antivirus vendors.
5. Don't "jailbreak," "root," or otherwise circumvent the security safeguards of your device. This makes it even easier for malicious applications to avoid the same security measures to get control of your device.
6. When purchasing applications, do some research. Make sure the author of the software matches the application. For popular applications, consider the number of downloads and/or reviews: a well-known game might have millions of downloads, whereas malware posing as it may only have a few hundred or thousand.
7. When installing applications, pay close attention to the permissions required for it. An alarm clock that needs to send SMS messages might warrant a closer look.

In short, good security practices are universal, no matter whether on a phone, tablet, computer, or other digital device. Be careful what you download and install, where it came from, what it wants to do, and consider dedicated software for detecting and removing mobile malicious threats.

For more information about computer security and other computer related scams, we encourage Army Knowledge Online users to visit the On Cyber Patrol Website and review previous 2CANs and other relevant information products. Other users, we recommend that you visit the CCIU website to review previous 2CANs.

Additional Information/Sources:

STAYSAFEONLINE.ORG
http://www.staysafeonline.org/stay-safe-online/mobile-and-on-the-go/mobile-devices

FBI
http://www.fbi.gov/scams-safety/e-scams?utm_campaign=email-Immediate&utm_content=145512

SOPHOS
http://nakedsecurity.sophos.com/2012/06/14/top-five-android-malware/

ICE ***CCIU is now using the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.***