Computer Crime Investigative Unit
U.S. Army Criminal Investigation Command

Cyber Crime Prevention Flyer

CPF 0004-13-CID361-9H 16 January 2013

"REMOTE HOSTILE TAKEOVER"

OVERVIEW:

The purpose of this Cyber Crime Flyer is to inform all service members and Department of the Army civilians of the latest scam wherein cybercriminals are using readily available malware to compromise mobile devices, specifically ones running the Android operating system (OS). Criminals are using different variants of malware to lure the victims. Some variants purport to promise a work-at-home opportunity that guarantees profits; while others provide links which appear to be legitimate sites. The malware is able to completely take over the mobile device allowing the criminal unfettered remote access to it. The attack vector for this mobile malware is often a text message masquerading as a system update, or a link to a specific website.

Background:

Unlike traditional attack vectors such as exploiting email attachments, this malware exploits text messages tricking the victim into believing they need to update their mobile device. The text message contains a link which takes the user to a site that automatically downloads the malware allowing the cyber criminal the ability to make calls, send texts, download new apps and install malicious software.

Likewise, the Federal Communications Commission, partnering with many public and private-sector mobile security experts, has released the Smartphone Security Checker. You tell it what OS you have (Android, Apple iOS, BlackBerry, Windows Mobile), and the site will return a 10-step checklist specific to that OS of things you need to do to help protect your device.

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"

Safety Tips to Protect Your Mobile Device:

- Obtain malware protection for your mobile device. Look for applications that specialize in antivirus or file integrity that helps protect your device from rogue applications and malware.
- Be aware of applications that enable geo-location. The application will track the user's location anywhere. This application can be used for marketing, but can also be used by malicious actors, raising concerns of assisting a possible stalker and/or burglaries.
- Jailbreak or rooting is used to remove certain restrictions imposed by the device manufacturer or cell phone carrier. This allows the user nearly unregulated control over what programs can be installed and how the device can be used. However, this procedure often involves exploiting significant security vulnerabilities and increases the attack surface of the device. Anytime an application or service runs in "unrestricted" or "system" level within an operation system, it allows any compromise to take full control of the device.
- Avoid clicking on or otherwise downloading software or links from unknown sources.
- Review and understand the permissions you are giving when you download applications.
- Utilize the FCC Smartphone Security Checker.

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 Cyber Crime Alert Notices (2CAN) and other relevant information products. Other users, we recommend that you visit the CCIU website to review previous 2CANs.

Additional Information/Sources:

Internet Crime Complaint Center (IC3)
http://www.fbi.gov/scams-safety/e-scams

Symantec
http://www.symantec.com/connect/blogs/fbi-issue-warnings-over-rogue-malware-attacks

Federal Communications Commission
http://www.fcc.gov/

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.

Disclaimer: The appearance of hyperlinks in this Cyber Crime Prevention Flyer (CCPF), along with the views and opinions of authors, products or services contained therein does not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations. Such links are provided consistent with the stated purpose of this CCPF.

CCIU's "Toucan Lan" keeps an eye on cyber crime
issues of interest to the Army community.