Contact Information:
Cyber Criminal Intelligence Program
9805 Lowen Road, Building 193
Fort Belvoir, Virginia 22060-5598

Phone: 703.805.3499 (DSN 655)
Fax: 703.805.2351 (DSN 655)
E-mail:
cybercrimintel.cciu@us.army.mil

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

CID Cyber Lookout
On Point for the Army

"DO WHAT HAS TO BE DONE"

2CAN 0007-10-CID361-9H **5 March 2010**

POP-UP COULD LEAVE YOUR PC MESSED UP

OVERVIEW:

Social Engineering has become the primary means used by attackers to obtain personal information from unsuspecting victims. Their strategy involves exploiting human curiosity and a desire for reward, by manipulating unsuspecting users into performing actions that they wouldn't normally take. The pop-up security message is the latest twist of a social engineering attack that preys on people's fears and concerns.

CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

THOSE PESKY POP-UPS:

According to an FBI news release, the FBI warned consumers about an ongoing threat involving pop-up security messages that appear while they are on the Internet. The pop-up messages may contain a virus that could harm your computer, cause costly repairs or, even worse, lead to identity theft. The messages contain scareware, fake or rogue anti-virus software that looks authentic.

The message may display what appears to be a real-time, anti-virus scan of your hard drive. The scareware will show a list of reputable software icons; however, you can't click a link to go to the real site to review or see recommendations.

Once the pop-up warning appears, it can't be easily closed by clicking the "close" or "X" buttons. If you click the pop-up to purchase the software, a form to collect payment information for the bogus product launches. In some instances, the scareware can install malicious code onto your computer, whether you click the warning or not. This is more likely to happen if the account logged into the computer has rights to install software.

Downloading the software could result in malicious programs being installed on your computer. Malicious programs can cause costly damages for individual users and financial institutions. The FBI estimates scareware has cost victims more than $150 million.

Cyber criminals use easy-to-remember names and associates them with known applications. Beware of pop-up warnings that are a variation of recognized security software. You should research the exact name of the software being offered. Take precautions to ensure operating systems are updated and security software is current. If you receive these anti-virus pop-ups, close the browser or shut down your computer system. You should run a full anti-virus scan when the computer is turned back on.

Cyber Crime Alert Notice

If you have experienced the anti-virus pop-ups or a similar scam, notify the Internet Crime Complaint Center (IC3) by filing a complaint at www.ic3.gov. Experts recommend computer users never open any unsolicited e-mail or click on any links provided in them.

By following these suggestions, you might prevent yourself from becoming the next victim:

- Do NOT trust unsolicited email.
- Treat all pop-ups with caution.
- Do NOT click links in unsolicited email messages.
- Install trusted anti-virus software, and keep its virus signature files up-to-date.
- Turn off the option to automatically download attachments.
- Employ the use of a spam filter.

Protecting Your Home Computer:

The Army Computer Emergency Response Team offers free antivirus software for Department of the Army personnel to use on home computers. You must access the following link from a .mil computer system and authenticate with your CAC and PIN:

https://www.acert.1stiocmd.army.mil/Antivirus/

Additional Reporting and Information:

http://www.websense.com/site/Docs/Reports/WSL_ThreatPredictions_2010.pdf

http://www.fbi.gov/cyberinvest/escams.htm

http://www.ic3.gov/media/2009/091211.aspx

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.