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

Cyber Crime Alert Notice

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

"DO WHAT HAS TO BE DONE"

2CAN 0005-08-CID221-9H **13 February 2008**

VALENTINE MESSAGE COULD LEAVE YOU WITH A BROKEN HEART (OR HARD DRIVE)

OVERVIEW:

Social engineering has emerged as a popular strategy for cyber criminals to obtain personal information from unsuspecting victims or trick them into installing malicious software (malware). Their strategy involves exploiting human curiosity and a desire for reward by manipulating unsuspecting users into performing actions that they would not normally take. The Storm Worm has spread across the Internet with the help of social engineering attacks that combine tempting e-mail messages with malware.

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

ONLINE ROMANTICS BEWARE:

With Valentine's Day approaching, computer users should be on the lookout for spam e-mails that are spreading malware associated with the Storm Worm.

The Storm Worm has capitalized on various holidays in the last year by sending millions of e-mails advertising an e-card link within the text of the spam e-mail. Valentine's Day has been identified as the next target.

According to an FBI news release, "The e-mail directs recipients to click on a link to retrieve an electronic greeting card, or some of these messages contain a header like 'Looking for that perfect Valentine's Day gift?' or 'Make Valentine's Day Night a memorable one.' Once the user clicks on the link, malware is downloaded to the user's computer, causing it to become infected and become part of the Storm Ware botnet."

A robot network or "botnet" is a network of compromised computers under the remote control of a single hacker. Botnets can be used to facilitate criminal activity such as sending spam e-mail, identity theft, denial of service attacks and spreading malware to other computers.

Experts recommend that computer users never open any unsolicited e-mail or click on any links provided in them.

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

- Do NOT trust unsolicited email.
- Treat all email attachments with caution.
- Do NOT click links in unsolicited e-mail messages.
- Install antivirus software, and keep its virus signature files up-to-date.
- Turn off the option to automatically download attachments.
- Block executable and unknown file types at the e-mail gateway.
- Configure your e-mail client for security.
- 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:

Websense Security Labs alert:
http://www.websense.com/securitylabs/alerts/alert.php?AlertID=838

Internet Crime Complaint Center press release:
http://www.ic3.gov/media/2008/080211.htm

vnunet.com news item:
http://www.vnunet.com/vnunet/news/2209198/valentines-day-spamming-storm

Security Fix blog in *The Washington Post*:
http://blog.washingtonpost.com/securityfix/2008/02/the_storm_worms_family_tree_1.html

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.***