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

Cyber Crime Alert Notice

2CAN 0027-07-CID221-9H 24 April 2007

Turning Tragedy into Cyber Crime

Overview:

Unscrupulous cyber criminals have again shown that they will use practically any means to further their illicit schemes: Computer security experts are warning users to beware of phishing Web sites, spam e-mails, and malware attacks that have emerged following the recent tragedy at Virginia Tech. The Asian Tsunami (2004) and Hurricane Katrina (2005) both spawned a rash of fraudulent donation Web sites and spam e-mails, and it appears cyber criminals are attempting to exploit the notoriety of this latest tragedy and the charitable nature of the Army community.

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

The Phishing Threat:

A wealth of information resources are available to inform computer users about the threat posed by phishing, and AKO users can visit On Cyber Patrol to view an awareness briefing from the Joint Task Force for Global Network Operations and previous 2CANs covering vishing and keylogging.

Within the past week, the SANS Internet Storm Center noted approximately 450 new domain names for Web sites that their researchers believe might be tied to fraudulent schemes designed to capitalize on the Virginia Tech shootings. *SC Magazine* also reported on the recent phenomenon of phishing schemes following highly visible tragedies and current events.

Additionally, computer users should be suspicious of unsolicited spam e-mails ostensibly from charitable organizations or fund raising initiatives acting on behalf of Virginia Tech. The Virginia Tech Web site has a list of legitimate charities and scholarship funds, and Army community members should only donate to charities that have been properly vetted.

The Federal Trade Commission offers the following guidance to avoid falling victim to charity fraud:

- Donate to recognized charities you have given to before.
- Give directly to the charity, not the solicitors for the charity.
- Do not give out personal or financial information; do not donate cash.
- Check out any charities before you donate.

The United States Computer Emergency Readiness Team (US-CERT) offers the following general guidance to avoid falling victim to phishing schemes:

- Do not follow unsolicited Web links received in e-mails.
- Contact your financial institution immediately if you believe your account and/or financial information has been compromised.
- Verify the legitimacy of the e-mail by contacting the company directly through a trusted contact number.
- Visit the Anti-Phishing Working Group for more information on known phishing attacks.

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"

Cyber Crime Alert Notice

THE MALWARE THREAT:

Malware includes a wide spectrum of programs that are designed to harm a computer, and when paired with social engineering tactics, malware can be an especially dangerous threat. The IT security and control firm Sophos reported a recent wave of spam e-mails containing a hyperlink purporting to show camera phone footage of the Virginia Tech shootings. But curious computer users who click on the hyperlink will get an unpleasant surprise: The hyperlink directs users to a screen saver file called TERROR_EM_VIRGINIA.scr, which is actually a Trojan capable of stealing user names, passwords, and account numbers.

The Joint Task Force for Global Network Operations and the Army Computer Emergency Response Team offer free antivirus software and firewalls for Department of Defense personnel to use on their home computers. These safeguards are generally effective for detecting and eliminating malware, in addition to other computer security threats. You must access the following links from a .mil computer system and authenticate with your CAC and PIN: https://www.jtfgno.mil/antivirus/home_use.htm or https://www.acert.1stiocmd.army.mil/Antivirus/updates.htm. The software files can be saved to removable media and then installed on home computers.

ADDITIONAL CHARITY FRAUD, PHISHING, AND MALWARE RESOURCES:

Federal Trade Commission on Charity Fraud:
http://www.ftc.gov/bcp/conline/edcams/charityfraud/coninfo.html

Better Business Bureau's Phishing Phacts:
http://www.bbbonline.org/idtheft/phishing.asp

National Consumers League's Phishing Awareness:
http://phishinginfo.org

SGT Firewall On Cyber Patrol (AKO only):
https://www.us.army.mil/suite/page/190357

SANS Institute's Malware FAQ:
http://www.sans.org/resources/malwarefaq/index.php

White Paper on Malware from US-CERT (Caution - high geek factor):
http://www.uscert.gov/reading_room/malware-threats-mitigation.pdf

In Memoriam

CYBER CRIMINAL INTELLIGENCE PROGRAM
CUSTOMER SURVEY

Dear Customer:

Please take a moment and complete this survey to help evaluate the quality and value of CCIU Cyber Criminal Intelligence products. Your response will help us to serve you more effectively and efficiently in the future. Thank you for your assistance.

Product Title: 2CAN 0027-07 - Turning Tragedy into Cyber Crime

Customer's Organization (optional): _____

Marking instructions: Indicate the appropriate response accordingly.

1	Strongly Disagree
2	Disagree
3	Neither Agree nor Disagree
4	Agree
5	Strongly Agree
NA	Not Applicable

QUALITY

1	2	3	4	5	NA	
○	○	○	○	○	○	The product was timely and relevant to contemporary Internet safety issues.
○	○	○	○	○	○	The product was clear and logical in the presentation of information with supported judgments and conclusions.
○	○	○	○	○	○	The product is reliable (i.e., sources are well-documented and reputable).

VALUE

1	2	3	4	5	NA	
○	○	○	○	○	○	The product contributed to your knowledge of previously unknown Internet safety subjects.
○	○	○	○	○	○	The product caused you to pay more attention to Internet safety subjects relevant to your or your family.
○	○	○	○	○	○	The product increased your familiarity with CID Cyber Lookout's Internet safety initiatives.
○	○	○	○	○	○	The product caused you to research Internet safety subjects in greater depth, using the additional resources listed in the product.

ADDITIONAL COMMENTS

If you have the free Acrobat Reader, please click below to print your completed survey and mail or fax it to CCIU (address/fax information on front page).

PRINT

If you have Acrobat Professional, please click below to extract this page, save a copy of the completed survey, and e-mail it to: cybercrimintel.cciu@us.army.mil

EXTRACT