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

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

"DO WHAT HAS TO BE DONE"

2CAN 0050-07-CID221-9H **7 September 2007**

"MONSTER PHISH" LURE ONLINE JOB SEEKERS

OVERVIEW:

The U.S. Office of Personnel Management warned in a recent security alert that hackers have stolen the names, e-mail addresses, and telephone numbers of about 146,000 subscribers to USAJOBS.gov, the U.S. Government's official job listing Web site. The hackers accessed the information from the résumé database run by Monster.com, which provides the technology for USAJOBS.gov. No Social Security numbers were compromised.

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

ONLINE JOB SEEKERS BEWARE:

Current and former job seekers could find themselves targeted by so-called "phishing" e-mails, possibly disguised as Monster.com or USAJOBS.gov messages. Officials at Monster.com confirmed that they had identified and shut down the server accessing contact information through the unauthorized use of compromised legitimate employer/client log-in credentials. "Monster is in the process of reaching out to its entire employer population to mitigate any ongoing issues," officials at the job hunting site said. "In addition, Monster is placing a security alert on the Monster.com site."

Military job seekers may be among the 1.3 million people at risk after Internet criminals hacked into the résumé database at Monster.com. The Defense Department's transition assistance Web site TurboTAP.org is operated under a contract with Military Advantage, which is also a part of Monster.com. Monster.com believes the thieves intend to send e-mail purportedly originating from Monster.com or USAJOBS, in order to gain the job seekers' trust, and then attempt to engage in financial transactions or lure them into downloading malicious software.

Monster.com officials say the company is in the process of contacting those who might have been affected, with information on precautionary steps to take. Officials said they have identified and shut down the source of the malicious software. They also are working with regulatory agencies and law enforcement authorities.

If you have received an e-mail that claims to be from Monster.com and clicked on the embedded link in the e-mail, Monster.com advises running an anti-virus application to remove anything that might have been maliciously installed in your computer. Users are encouraged to contact a Monster.com representative to have your Monster account password changed. Should you receive an e-mail purportedly from Monster instructing you to download a tool or update your account or access agreement, please contact Monster.com to verify its legitimacy. If you receive a suspicious email regarding your USAJOBS search, email it, with the full "header" information intact, to mayday@fedjobs.gov. Instructions on obtaining header information can be found at: http://www.spamcop.com/help_with_headers/.

These types of occurrences are not exclusive to the United States: Our friends in Australia have also encountered similar problems. Australia's iTnews reported that "Security researchers have unearthed the single largest cache of stolen identities, thanks in part to a Trojan stealing the data that has been hidden in a fraudulent advertisement on online job sites like Monster.com."

For more information about key logging or phishing, we encourage Army Knowledge Online users to visit the On Cyber Patrol Web site at https://www.us.army.mil/suite/page/190357 and review previous 2CANs and other relevant information products.

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:

The Washington Post (registration required):
http://blog.washingtonpost.com/securityfix/2007/08/would_you_like_a_job_with_that_1.html

Symantec:
http://www.symantec.com/enterprise/security_response/weblog/2007/08/a_monster_trojan.html

SANS Institute:
http://isc.sans.org/diary.html?storyid=3295

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

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.