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

Cyber Crime Alert Notice

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"

2CAN 0001-12-CID361-9H **3 May 2012**

"PERSONAL COMPUTER DOOMSDAY?"

OVERVIEW:

The purpose of this Cyber Crime Alert Notice (2CAN) is to inform all service members and Department of the Army civilians of a method used to alter DNS (Domain Name System) Servers also known as DNS hijacking or DNS redirection. In this latest scam, the cyber crooks use malware to change the PC user's domain name server settings to replace the Internet Service Provider's legitimate DNS servers with nefarious DNS servers, often referred to as a rogue DNS server, which are operated by the criminal. CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

DNS Background:

DNS is an Internet service that converts user-friendly domain names into the numerical Internet protocol (IP) addresses that computers use to talk to each other. When you enter a domain name, such as www.fbi.gov, in your web browser address bar, your computer contacts DNS servers to determine the IP address for the website. Your computer then uses this IP address to locate and connect to the website. DNS servers are operated by your Internet service provider (ISP) and are included in your computer's network configuration. DNS and DNS Servers are a critical component of your computer's operating environment—without them, you would not be able to access websites, send e-mail, or use any other Internet services.

FBI Alert:

According to an FBI alert, malware causes a computer to use rogue DNS servers in one of two ways. First, it changes the computer's DNS server settings to replace the ISP's good DNS servers with rogue DNS servers operated by the criminal. Second, it attempts to access devices on the victim's network that runs a router or home gateway. The malware attempts to access these devices using common default usernames and passwords and, if successful, changes the DNS servers these devices use from the ISP's good DNS servers to rogue DNS servers operated by the criminals.

What the Experts are Saying:

Experts recommend testing computers for infection of the DNSChanger malware, and those testing positive will need to be cleaned of the malware in order to maintain continued internet connectivity beyond July 9, 2012.

After July 9, 2012, if your PC is infected you will get a screen stating Address Not Valid or Security Issues Detected.

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. Other users, we recommend that you visit the CCIU website to review previous 2CANs.

JULY 9, 2012:

Computers testing positive for infection of DNSChanger malware will need to be cleaned of the malware in order to maintain continued internet connectivity beyond July 9, 2012. If users don't rid themselves of DNS Changer before then, they'll have to load anti-virus software on their computers by disc or USB drive.

PROTECTING YOUR HOME COMPUTER:

The Army Computer Emergency Response Team (ACERT) 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: To go to the ACERT website click here.

ADDITIONAL REPORTING AND INFORMATION:

DNS Changer Working Group
http://www.dcwg.org/

U.S. CERT
http://www.us-cert.gov/current/archive/2012/04/30/archive.html

Security World
http://www.net-security.org/malware_news.php?id=1983

FBI
http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

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.