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 0016-12-CID361-9H **4 September 2012**

"HELD FOR RANSOM"

OVERVIEW:

The purpose of this Cyber Crime Alert Notice (2CAN) is to inform Department of the Army personnel of illegal "ransomware" that masquerades as an alert from U.S. Cyber Command (USCYBERCOM) and/or other government agencies. In this latest scam, cybercriminals are using a computer virus named Reveton, which holds your computer ransom, thus giving it the name ransomware. The ransomware lures the victim to a drive-by download website, at which time the ransomware is installed on the user's computer. Once installed, the computer freezes and a screen is displayed warning the user they have violated a federal law. To unlock the computer, the user is instructed to pay a fine to USCYBERCOM using a prepaid money card service. The geographic location of the user's IP address determines what payment services are offered. The ransomware has predominately been using the Federal Bureau of Investigation (FBI) name and logo to trick individuals; however, recently the virus creators have started using the USCYBERCOM name and logo. The ransomware continues to operate on the compromised computer and can be used to commit online banking and credit card fraud. The use of the USCYBERCOM name and logo can be an attempt to extort money from Department of Army and other Department of Defense (DoD) personnel. CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

Background:

Unlike trying to trick users into opening malicious email attachments, the virus exploits known vulnerabilities when the user visits a compromised website. Malware distributors use various techniques to attempt to direct Internet users to Websites that have been compromised or are intentionally hosting malicious code. Users can be secretly infected with malware simply by visiting a website, even without attempting to download anything themselves, thus giving it the name "drive-by download."

Recommended Actions:

1. **Do not pay the money**.

2. **Remediate the malware.** The average user will not be able to easily remove the malware. If you become a victim of the Reveton virus:

   - Immediately disconnect the computer from the network and seek the assistance from a computer expert in removing the virus.
   - Be aware that even if you are able to unfreeze your computer on your own, the virus may still operate in the background. Certain types of viruses and malware have been known to capture personal information such as user names, passwords, and credit card numbers.
   - File a complaint on the FBI Internet Crime Complaint Center (IC3) website (http://www.ic3.gov)
   - For any incident involving a U.S. Army computer, immediately notify your information assurance and security officers.

For more information about computer security and other computer related scams, we encourage Army Knowledge Online users to visit the On Cyber Patrol Website and review previous 2CANs and other relevant information products. Other users, we recommend that you visit the CCIU website to review previous 2CANs.

PROTECTING YOUR HOME COMPUTER:

The U.S. Army Cyber Command (ARCYBER) 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 ARCYBER website click here.

ADDITIONAL REPORTING AND INFORMATION:

INTERNET CRIME COMPLAINT CENTER (IC3)
http://www.ic3.gov/media/2012/120809.aspx

SYMANTEC
http://www.symantec.com/connect/search/apachesolr_search/RANSOMWARE?filters=tid%3A2261%20type%3Ablog

ONLINE SAFETY 411 INFORMATION
http://www.onlinesafety411.com/index.php?s=RANSOMWARE

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.***