



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

CID Cyber Lookout
On Point for the Army

DISTRIBUTION:

This document is authorized for wide release with no restrictions.

2CAN 0003-07-CID221-9H

THRIFT SAVINGS PLAN SECURITY NOTICE

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 steal funds from their Thrift Savings Plan (TSP) accounts and to encourage personnel to safeguard online personally identifiable information (PII). Because approximately 49% of TSP participants access their accounts using a home computer, the potential exists for future thefts and fraudulent activities (Survey data from *Thrift Savings Plan Participant Survey Results 2006*). CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

TSP ALERT:

The following alert was recently posted on the TSP Web site (www.tsp.gov/account/login_security-news-ab.html):

To illustrate the importance of participant vigilance, in late December the computers of several TSP participants were infected with keylogging software. This software allowed criminals to record all key strokes made by the participant without the participant's knowledge and to learn the participant's TSP PIN and other account information. We were able to identify approximately two dozen participants who had relatively small amounts withdrawn from their accounts and electronically forwarded to fraudulent accounts. Although we are working with the financial companies involved for the return of the funds, the total amount of loss involved is approximately \$35,000. All affected participants have been notified.

We emphasize that the account information for these participants was not improperly obtained from the TSP record keeping system. External penetration testing has demonstrated that our system has not been breached. There is no evidence of any successful attacks against the system to identify a PIN and thus obtain access.

We have concluded that the personal information was compromised when keyloggers monitored each keystroke made by these participants while they entered their TSP information into their own computer. We are working with the U.S. Secret Service, which has found that such personal information is increasingly available on keylogger lists that are for sale through criminal networks.

The cases identified all involve electronic funds transfers. Criminals prefer this "paperless" way to steal money. As an added security measure, we have discontinued making these electronic payments for on-line transactions.

While anyone can be a victim of keylogging, individuals whose computers are not protected with updated security software (that includes firewalls, anti-virus and spyware detection) are most vulnerable. We strongly urge all participants to ensure the adequacy of security on their computers by installing keylogger protection and promptly closing their browser after each visit to their TSP account information on the Web site. These steps will reduce your exposure.



This practice should be followed for all on-line access to any financial account. (To close your browser, click the X at the top of your internet screen – logging off a Web site does not clear your browser's memory.)

Participants using the TSP Web site (or any Web site involving PII) must be vigilant and protect their computers. Although the TSP cannot be responsible for participants' negligence or poor security practices, the TSP will ensure that their Web page security is current and that the risk of fraudulent activity is reduced to the greatest extent possible. The TSP will be implementing additional online security measures in the near future.

ADDITIONAL INFORMATION FROM TSP ABOUT SECURELY ACCESSING THEIR WEB SITE:

www.tsp.gov/faq/faq3a.html

ADDITIONAL INFORMATION ABOUT KEYSTROKE LOGGING:

Keystroke logging (often called keylogging) is a diagnostic used in software development that captures the user's keystrokes. It can be useful to determine sources of error in computer systems and is sometimes used to measure employee productivity on certain clerical tasks. Such systems are also used by computer hackers, providing a means to obtain passwords or encryption keys and thus bypassing other security measures.

Keystroke logging can be achieved by both hardware and software means. Hardware key loggers are commercially available devices which come in three types: inline devices that are attached to the keyboard cable, devices which can be installed inside standard keyboards, and actual replacement keyboards that contain the key logger already built-in. The inline devices have the advantage of being able to be installed instantly. However, while they may go unnoticed for quite some time, they are easily detected visually upon closer inspection. Of the three devices available, the most difficult to install is also the most difficult to detect. The device that installs inside a keyboard (presumably the keyboard the target has been using all along) requires soldering skill and extended access to the keyboard to be modified. However, once in place, this type of device is virtually undetectable.

PROTECTING YOUR HOME COMPUTER:

The Joint Task Force for Global Network Operations offers free antivirus software for Department of Defense 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.jtfgno.mil/antivirus/home_use.htm

Disclaimer: The appearance of hyperlinks in this 2CAN, along with the views and opinions of authors, products or services contained therein does not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations. Such links are provided consistent with the stated purpose of this 2CAN.



CCIU's "Toucan Lan" keeps an eye on cyber crime issues of interest to the Army community.

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: _____

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 your mission, programs, priorities, or initiatives.
						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 satisfying intelligence gaps or predicated cases, especially in previously unknown areas.
						The product resulted in a shift to address previously overlooked investigative areas.
						The product resulted in more informed decisions concerning investigative initiatives and/or resource allocation.
						The product identified new information associated with pending matters or offered insights into information that could change the working premise in a program or initiative.

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).

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