

Member Obligations for Sharing FBI Information

The purpose of disseminating FBI intelligence products is to obtain information which can be useful to the FBI's intelligence gathering on the subject matter, or to aid a pending criminal investigation. Guidance on whom and how to contact the FBI if there is positive information is provided in the body of the intelligence product. The owner of the information in this intelligence product has approved dissemination. The disclosure of the information in this intelligence product could jeopardize law enforcement efforts and, therefore, it is restricted information.

The following guidance on receipt of restricted information is provided:

In disseminating intelligence products, the FBI is seeking information from the recipient of the information;

It is recognized that the information the FBI is seeking maybe available from the personnel who work at the recipient's place of business;

The recipient should exercise due care in discussing information learned from an intelligence product, providing only what is sufficient to determine whether a non recipient may substantially provide useful details and to obtain such information;

The recipient may disclose sufficient information to his/her own personnel which would allow for the protection of their computer or administrative systems, but may not disclose the intelligence product itself or discuss the source of the information; and,

The recipient agrees to maintain a list of names of persons in receipt of any intelligence product information, providing it to the FBI upon request.



Office of Intelligence and Analysis

**Homeland
Security**

Homeland Security Assessment

(U) Increasing Threat of Keyloggers to Computer Security

14 May 2007

(U//FOUO) Prepared by the Critical Infrastructure Threat Analysis Division.

(U) Key Findings

(U//FOUO) Keyloggers and associated spyware have evolved into one of the most prevalent and potentially harmful threats to U.S. information infrastructure. Users of these intrusive software programs and hardware devices have targeted personally identifiable information, corporate intellectual property, government classified information, and critical infrastructure data repositories.

(U//FOUO) Online banking, commercial, and financial institutions appear to be among targets criminals favor in keylogging attacks.

(U//FOUO) Instead of simply attacking network operations to damage them, cyber attackers use keyloggers to acquire passwords and other sensitive information. Such access can allow data to be taken without user knowledge, facilitating blackmail, extortion, and identity theft.

(U//FOUO) Keylogger tools are flexible, portable, and versatile, and they provide an extraordinary opportunity for trusted insiders to compromise an organization's sensitive data.

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official. State and local Homeland security officials may share this document with authorized security personnel without further approval from DHS.

(U) This product contains U.S. Person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label ^{USPER} and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other USPER information has been minimized. Should you require the minimized USPER information please contact the DHS/I&A Production Management Division at IA.PM@ha.dhs.gov.

(U) Keyloggers Threat

(U//FOUO) Keystroke loggers—also known as keyloggers—were intended originally as legitimate computer surveillance and monitoring tools to troubleshoot sources of computer system errors or to record keyboard activities for analysis and program debugging. Keyloggers also can be used, however, to compromise privacy and steal data from computers. As a result, keyloggers are becoming a primary choice for cyber criminals to commit identity theft and online fraud.

(U//FOUO) As the number of keylogger hosting websites grows and the number of malicious variants increases, the threat to information security will rise.

- (U//FOUO) The Anti-Phishing Working Group (APWG)^{USPER}, an industry association focused on eliminating identity theft and fraud, said that the number of malicious keylogger variants it tracked grew from 184 in January 2006 to 345 in January 2007. During the same period, the number of websites offering keyloggers grew from 1,100 to 1,750. In addition, the APWG collected evidence that hackers in different countries share methods, techniques, and toolkits to exploit keyloggers.
- (U//FOUO) The growth in malicious keylogger variants and hosting websites coincides with a worldwide increase in the number of malicious keylogger attacks on computers. According to the SANS Institute^{USPER}—a group that trains and certifies security professionals—more than 9.9 million computers in the United States were infected with one or more malicious keylogger variants as of late 2006.

(U//FOUO) Some keylogger attacks have targeted nuclear and government entities.

- (U//FOUO) The FBI in October 2006 reported the compromise—apparently through keylogger-type software—of a server supporting a nuclear reactor research facility in Pennsylvania. No classified data were compromised.
- (U//FOUO) The FBI in September 2006 reported cyber intruders loaded keylogger software on three endpoint computers of the European Organization for Nuclear Research. The intruders captured log-in credentials that permitted them full access to a U.S. Government-operated computer system and to local networks and trusted systems in Western Europe.

(U) Hardware Keyloggers

(U//FOUO) Keylogger technology which is versatile in its application, can be engineered into both hardware devices and software programs. A hardware keylogger records keystrokes in the device's built-in, non-volatile memory. The device does not rely on the targeted system's resources to operate and is not identifiable by anti-malware software.

- (U//FOUO) A generic hardware keylogger resembles a AA battery in size and blends in with the surrounding wire harness, obscuring its presence to most users. It can capture, encrypt, and store up to two million keystrokes, starting immediately after the affected computer's power is turned on.

(U//FOUO) Installation of a hardware keylogger requires physical access to the targeted system, making trusted insiders the primary threat for surreptitious deployment of such a device.



(U//FOUO) Pre-installation: standard cable connects the keyboard to the PS/2 processor port.



(U//FOUO) Post-installation: hardware keystroke logger inserted between keyboard and PS/2 processor port.

(U//FOUO) Representation of Hardware Keylogger: Hardware keystroke loggers are available commercially in three models: a cable between the keyboard and processor port, an implanted device in the keyboard, and a keyboard with logging functionality built-in. The last type is the most difficult to identify. It is ideal for capturing passwords.

©www.keyghost.com

(U) Features of Keylogger Hardware Devices

- *(U) Direct physical access required to install.*
- *(U) Easier to install than software versions.*
- *(U) Password or invasive log-on access to target system not required.*
- *(U) Information recorded on one system can be decoded on another computer.*
- *(U) Functionality independent of operating system it is monitoring.*
- *(U) Captures verbatim keystroke activities immediately after system power-on.*

(U) Software Keyloggers

(U//FOUO) A software keylogger targets a computer or system through e-mail attachments, Internet relay chat channels, peer-to-peer networks, or downloadable infected applications. Downloadable software such as games, music and video clips, screen savers, and utilities could carry keylogging software. Hackers often embed keyloggers within a virus or Trojan horse program. Hackers also can install software keyloggers from a disk or external storage device such as a USB memory stick or flash drive.

- (U//FOUO) Although insiders with access and opportunity can easily install software or hardware keyloggers on network and stand-alone platforms, remote installation by hackers constitutes the most compelling threat to vulnerable systems.
- (U//FOUO) An attack on the Los Alamos National Laboratory in June 2003 used the Bugbear.B worm fitted with a keylogger payload and a trigger for deployment.

(U//FOUO) Current generation keyloggers are virtually undetectable and extremely difficult to eradicate with most antivirus or anti-spyware tools. The software leaves no evidence of its presence in the operating system registry, process list, system tray, task manager, or add/remove program queues where legitimate applications are visible. Moreover, when in operation keylogging software uses little memory and few central processing unit cycles and, as a result, likely would go unnoticed.

(U) Features of Keylogger Software Programs

- (U) *Quick remote installation.*
- (U) *Concealed collection technique.*
- (U) *Continuous execution in stealth.*
- (U) *Covert channel used to transfer data from compromised computer.*
- (U) *Can spread to other computers when included in a Trojan.*
- (U) *Can monitor target's keystrokes from any location.*
- (U) *Observes target's activities in real-time.*

(U) Criminal Use of Keyloggers

(U//FOUO) Criminal enterprises use keyloggers to capture personally identifiable information such as social security numbers and authentication credentials to access bank accounts, credit cards, and debit cards of consumers and e-commerce services. Once

hackers penetrate a computer system with keylogger software or hardware, they can harvest critical information to use for immediate gain or for identity theft.

- (U//FOUO) Hackers compromised the website of the 2007 Super Bowl venue with Trojan and keylogger software to collect information on game patrons' bank accounts and credit cards.
- (U//FOUO) In October 2005 criminals impersonating the cleaning staff of a major Japanese bank in the United Kingdom implanted hardware keyloggers on computers handling wire transfers. Bank security foiled an attempted heist of \$440 million.
- (U//FOUO) Hackers in September 2003 inserted keylogger software in the network of a videogame software company and captured log-in access credentials of key employees. They were able to steal the source code of a popular videogame that could be altered to run simulators for combat-related training support.

(U) Outlook

(U//FOUO) Keylogging poses a growing threat to the security of many computer systems, especially those of financial websites, e-commerce sites, and web-based mail sites. Although no nexus to terrorist use of keyloggers has been established, malicious code writers have advertised on the Internet their willingness to sell keylogging software to clients for use in criminal enterprises. Terrorists could mimic the practices of cyber criminals to fund their activities through cyber fraud.

(U//FOUO) Improved computer operating systems, application programs, and anti-virus software—as well as programs for patching vulnerable systems—can help mitigate attacks. Network and endpoint system administrators should establish system baseline parameters and closely monitor them for changes, install manufacturers' prescribed patched software in a timely manner, properly configure computer systems with online access, keep anti-virus software current, and perform periodic vulnerability tests.

(U//FOUO) For more information on how to protect computers or mitigate attacks, contact the U.S. Computer Emergency Readiness Team (US-CERT) through the Internet at www.us-cert.gov/reading_room/ or call the US-CERT hotline at 1-888-282-0870.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Reporting Notice:

(U) DHS encourages recipients of this document to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force and the National Operation Center (NOC). The FBI regional phone numbers can be found online at <http://www.fbi.gov/contact/fo/fo.htm>, and the NOC can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at 202-282-9201 or by unclassified e-mail at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) For comments or questions related to the content or dissemination of this document please contact the DHS I&A Production Management staff at IA.PM@hq.dhs.gov.

(U) Tracked by: CYBER-040000-01-05, CYBER-020700-01-05, CYBER-020200-01-05