Monitor

(U) Cyber Security

Volume I Number 10

IA-0009-09

(U) Cyber Security

Volume I, Number 10

September 2008

(U) The Cyber Security Monitor is published by the DHS/Office of Intelligence and Analysis (I&A)/Critical Infrastructure Threat Analysis Division (CITA), with input from the U.S. Computer Emergency Readiness Team (US–CERT) at the National Cyber Security Division. CITA is the threat analysis component of the Homeland Infrastructure Threat and Risk Analysis Center.

(U//FOUO) This non-technical publication is intended for analysts and managers at Federal agencies, State and local Fusion Centers, and private sector partner organizations. DHS/I&A/CITA compiles the articles from intelligence reporting, government agency publications, and open sources.

(U//FOUO) Incidents involving cyber-related activity or breaches, including loss of personally identifiable information, should be reported to US–CERT at https://forms.us-cert.gov/report/ or e-mailed to soc@us-cert.gov.

Table of Contents

(U) Researchers Identify Emerging Malicious Hardware Threat

(U) A team of researchers in the United States has concluded that hackers could install malicious circuits in a computer's processor that would take control of other computers with which the circuits subsequently come into contact.

(U) The researchers created malicious circuits that could be used in advanced electronics such as computers. The circuits can bypass a computer's security controls, remain undetected by anti-virus software, and gain access to passwords and other sensitive information on other computers connected to the compromised computer.

— (U) According to the researchers, a user whose computer has been compromised by the malicious hardware most likely would remain unaware that his or her information was in jeopardy since the malicious hardware would not be detected even by antivirus software.

(U) Installing malicious hardware on a computer is considerably more difficult than installing malicious software. An attacker would have to gain access to the relevant chip at some point during its manufacture or, as the researchers have suggested, at a later juncture during maintenance.

(U) Prominent Phishing Group Tries New Tactics

(U) A prominent phishing group has added a new element to its traditional attacks. Its latest attack includes a "drive-by" download of malicious software and potentially places an increased number of users at risk.

— (U) The objective of the attack is to download the Zeus Trojan onto vulnerable computers. The Zeus program collects data from forms, takes screen shots, and steals passwords that hackers can use to remotely control infected computers.

— (U) According to security experts, the phishing group writes its own code, launches its own attacks, and is responsible for 50 percent of all current phishing scams.

— (U) The group's skills are evident in a recent version of Zeus that creates a new binary file for every phishing kit it sells. Anti-virus programs that use signature analysis techniques may not detect such files.

(U) **Drive-by download:** A download of malware, spyware, or a computer virus that takes place without a user's knowledge or intervention. A user's system can be infected simply by visiting a website, viewing an e-mail message, or clicking on a deceptive popup window.

(U) Drive-by downloads can infect computers without user awareness, but individuals still can minimize the risk of falling prey to phishing attacks by following safe computer practices. Users should keep anti-virus software up to date, never download or install unfamiliar software, and never click on links or attachments in unsolicited e-mails.

(U) Criminals Renting Botnets to Unskilled Hackers

(U) Hackers who lack the programming skills to create their own botnets can now rent an all-in-one hosting server that enables them to carry out attacks. For a fee, hackers gain access to a server with a built-in Trojan, infection tools, and software support and maintenance. The server typically is located in a country with lax cyber crime laws.

(U) The new botnet service allows unskilled hackers to begin collecting compromised data immediately without taking the usual preliminary steps of compromising a server or setting up their own back-end server and installing virus administration tools.

— (U) According to security experts, unskilled hackers simply pay a fee to gain access to a version of the Zeus Trojan stored on the hosting server and create infection points where compromised data can be collected.

— (U) The Zeus Trojan performs advanced keylogging when infected users visit certain Web pages. The compromised information then is encrypted and sent to a collection point controlled by the hacker.

— (U) Groups hosting these servers reportedly provide software support to customers similar to that offered by traditional software companies.

(U) Criminals are likely to continue refining their operations, as they did in this case, by adopting a software-as-a-service model to maximize their profits and potentially place more computer users at risk. Users can decrease their vulnerability to these risks by following safe computer practices such as keeping anti-virus software up to date, never downloading or installing unfamiliar software, and never clicking on links or attachments in unsolicited e-mails.

(U) **Software-as-a-Service:** A software delivery method that allows users to access software on a remote server for a fee.

(U) Universal Serial Bus Hacksaw Tool Evolving to Attack Networks

(U) An old but evolving cyber exploit allows hackers to exfiltrate data from thumb drives and e-mails to a remote, hacker-controlled location. First introduced in October 2006, Universal Serial Bus (USB) Hacksaw enables a hacker to locate and upload

documents from the USB drive on a victim's computer. A new capability allows this tool to attack other computers connected to the same network as the victim's computer.

— (U) In April 2008, a security expert announced research results that showed USB Hacksaw had been modified to allow it to target not just the USB drive on a specific computer to which a hacker gains physical access, but also to allow the program to scan the victim's computer network for documents to send back to the hacker's e-mail account.

— (U) In earlier versions of the program, an attacker would plug a USB thumb drive containing the USB Hacksaw program into a computer, automatically infecting it and causing it to covertly retrieve files from any USB drives subsequently plugged into the computer. The program would then send the files to a prearranged e-mail address. A hacker needs only seconds of physical access to the targeted computer to plug in a thumb drive that instantly installs the USB Hacksaw program.

(U) Any computer infected with the USB Hacksaw is able to send the contents of a USB thumb drive—and in the latest version, the contents of network drives—clandestinely to a hacker. Users therefore should exercise caution when saving information on thumb drives that might be plugged into a computer whose overall security has not been ascertained. Users should also pay attention to the physical security of the computers they use and limit potential physical access that hackers could exploit to install USB Hacksaw.

(U) **Reporting Notice:**

(U) DHS encourages recipients of this document to report information concerning suspicious or criminal activity to DHS and the FBI. The DHS National Operations Center (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. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov. The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm. 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) Incidents involving cyber related activity or breaches, including loss of Personally Identifiable Information, should be reported to US–CERT at https://forms.us-cert.gov/report or emailed to soc@us-cert.gov. For additional information on cyber related topics or to sign up to receive cyber alerts from the US–CERT National Cyber Alert System, visit www.us-cert.gov.

(U) For comments or questions related to the content or dissemination of this document please contact the DHS/I&A Production Branch at IA.PM@hq.dhs.gov, IA.PM@dhs.sgov.gov, and IA.PM@dhs.ic.gov.

(U) **Tracked by:** CYBR-010000-02-06, CYBR-020000-02-06, CYBR-040000-02-06, HSEC-030000-01-05