



July 2010

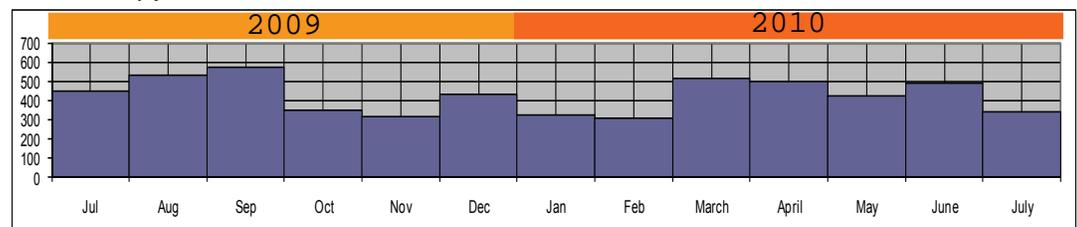
### IN THIS REPORT

- Executive Summary  
\*Special Coverage\*
- Cyber Attacks
- Data Breach/  
Information Gathering
- Threats and  
Vulnerabilities
- Policy, Legislation  
and Governance
- Reports and  
Publications

## CIKR Monthly Open Source Cyber Digest (OSCD)

### About this Report

The Monthly Open Source Cyber Digest (OSCD) is a tailored summary of domestic and international cyber events with specific relevance to the operations of the Critical Sectors community. The OSCD is primarily a compilation and reorganization of reporting drawn from the Daily Open Source Infrastructure Report (OSIR). The OSCD may also contain additional unclassified reporting found using open source research methodologies and may include imagery; local, national, and international media reports; academia and industry sources; multimedia and blogs; and other relevant, publicly-available sources. The OSCD does not provide analysis or projection; the content found within the OSCD is strictly for situational awareness.



Number of [software vulnerabilities](#) per month according to the National Institute of Standards and Technology's (NIST) National Vulnerabilities Database.

### Executive Summary

[CTV News](#) reports that several European NATO members have expressed concern that the fallout from a massive online leak of confidential U.S. documents on the Afghan war could extend well beyond the Internet and even affect the war itself. The U.S. records cover six years of the war in Afghanistan, including previously unknown accounts of civilian deaths and targeted attacks on Taliban members. NATO has declined to comment, but representatives from NATO member countries said they hope the leaks do not pose problems for the war effort. [V3.co.uk](#) reported that experts have uncovered a sophisticated malware operation targeting defense contractors. Researchers at Symantec Hosted Services said the operation involved compromising the site of one firm, and then using the hacked site to host a malware attack on another contractor by directing employees to the compromised site with a series of fraudulent phishing e-mails. The attempt is to exploit a new vulnerability in the Windows Help component. [Homeland Security News-wire](#) says a group of nations including the United States, China, and Russia have for the first time signaled a willingness to engage in reducing the threat of attacks on each others' computer networks. Although the agreement provides [recommendations](#) only, a cyberwarfare expert with the Council on Foreign Relations said it represents a "significant change in U.S posture." In other news:

- [Fox News](#) reports that researchers have uncovered new ways that criminals can spy on Internet users even if they are using secure connections to banks, online retailers or other sensitive Web sites.
- [Associated Press](#) announced that WellPoint Inc. has notified 470,000 of its insurance customers that medical records, credit card numbers and other sensitive information may have been exposed in the latest security breach of the health insurer's records.



July 2010

**Worm:** A self-propagating program that can automatically distribute itself from one computer to another.

### \*Special Coverage\*

For the past month, Microsoft has been closely [tracking](#) a new family of threats called [Stuxnet](#). Instead of using AutoPlay, the malware takes advantage of specially-crafted shortcut files, such as Windows Explorer, also known as .lnk files, placed on USB drives to automatically execute malware as soon as the .lnk file is read by the operating system. Stuxnet has been classified as a **worm**.

Modules of the malware were first [detected](#) by VirusBlokAda specialists June 17, and were added to the anti-virus bases as Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2. [VirusBlokAda](#) said it has seen numerous incidents of the Trojan spy payloads dropped by the malware since adding detection for the malign code in June. The attack features root-kit components designed to hide the presence of the information-stealing payload on compromised systems. The digital certificate, assigned to legitimate firm Realtek Semiconductor, used to sign the root-kit components in the malware was revoked by VeriSign following discovery of the attack. All versions of Windows, including the just-released beta of Windows 7 Service Pack 1 (SP1), as well as the recently retired Windows XP SP2 and Windows 2000, are vulnerable to attack.

According [to IDG News Service](#), the highly sophisticated Stuxnet targets systems running Siemens industrial-control, system-management software. The worm steals SCADA (supervisory control and data acquisition) project files from Siemens' computer systems. It has been [suggested](#) that Stuxnet looked like "it was made for espionage." The malicious software may have been in circulation since January, said a senior technical director with Symantec Security Response. Siemens confirmed July 21 that one of its customers has been hit by worm. The unidentified victim, which does not own the type of SCADA systems targeted by the worm, "told us their workstations serially rebooted without any reason," the head of the department said July 20. VirusBlokAda soon received reports of the malware from "all over the Middle East," he added. Computers in Iran have been hardest hit by the worm. According to data from Symantec, nearly 60 percent of all systems infected by the worm are located in Iran. Indonesia and India have also been hard-hit by the malicious software. According to [InfoWorld](#), Symantec is now logging about 9,000 infection attempts per day.

Microsoft released July 21 a stopgap fix to help Windows users protect themselves. Microsoft initially said customers could disable the vulnerable component by editing the Windows registry. However, such editing carries a high risk of causing system-wide problems. In an updated advisory posted July 20, Microsoft added instructions for using a much simpler, point-and-click "FixIt" tool to disable the flawed Windows features. The tool allows Windows users to nix the vulnerable component by clicking the "FixIt" icon, following the prompts, and then rebooting the system. However, it removes the graphical representation of icons on the Task bar and Start menu bar and replaces them with plain, white icons. But, G Data, a German security company, [released](#) a tool July 27 that blocks attacks using Microsoft's shortcut vulnerability while also preserving shortcut icons. The tool, called the G Data LNK Checker, is a small piece of software that is independent of other security software. It monitors the creation of shortcuts and will block the execution of code when a shortcut icon is displayed. G Data said its software will display a red warning signal if a shortcut tries to execute something that appears to be malicious.

Researchers at [Eset](#) have discovered a second variant of Stuxnet, called "jmidibs.sys." Like the original worm, the second variant is signed with a certificate. The

[\[Return to top\]](#)



July 2010

certificate was bought from VeriSign by JMicon Technology Corp., a company based in Taiwan. “We rarely see such professional operations,” the senior researcher wrote. “They either stole the certificates from at least two companies or purchased them from someone who stole them. At this point, it is not clear whether the attackers are changing their certificate because the first one was exposed or if they are using different certificates in different attacks, but this shows that they have significant resources.” The SANS Institute’s Internet Storm Centre has responded to the heightened threat by moving onto yellow alert status for the first time in years.

### Cyber Attacks

#### **Maine’s online database of legislative activity gets hacked**

*June 29 – (Government Facilities)*

An unknown hacker broke into Maine’s online database of legislative activity and attempted to manipulate the code of the Web site June 24, according to The Portland Press Herald. The legislature’s IT staff shut down the Web site’s bill-status function, which allows users to follow legislation such as roll calls, committee votes, amendments and fiscal notes. The manipulated code inserted the addresses of extraneous Web sites that could have exposed users’ computers to harm if they clicked on the links, said the director of IT for the legislature. “It’s not really a hugely harmful thing, if you get the Web site down,” he said. As soon as IT staff became aware of the problem, they took down the Web site. The bill-status section of [www.mainelegislature.org](http://www.mainelegislature.org) is run by a vendor, International Roll-Call. It is unclear whether the hacking impacted the Web sites of other state legislatures operated by the company, but the IT director said there have been talks with vendor officials who said they plan to increase security.

**The New New Internet:** [Maine’s online database of legislative activity gets hacked](#)

#### **Google confirms attack on YouTube**

*July 5 – (Information Technology)*

Malicious hackers attacked Google’s YouTube July 4, exploiting a cross-site scripting (XSS) vulnerability on the ultra-popular video sharing site, primarily hitting sections where users post comments. The attack potentially put at risk YouTube cookies of users who visited a compromised page, but it could not be used to access their Google account. The attackers apparently targeted a teen singing sensation, incorporating code into YouTube pages devoted to him so that visitors saw tasteless messages pop up about the teen star, and were redirected to external sites with adult content. An industry source familiar with the situation said that while the attack itself did not involve malware infections, such a risk is inherent whenever users visit any Web page, such as the ones attackers redirected users to. It is not clear if those landing pages contained malware, but most up-to-date anti-virus software is designed to protect against those threats.

**IDG News Service:** [Google confirms attack on YouTube](#)

#### **South Korean government web sites, banks hit by suspected cyber attack**

*July 8 – (Banking; Government Facilities)*

Suspected cyber attacks paralyzed Web sites of major South Korean government agencies, banks and Internet sites in a barrage that appeared linked to similar attacks in the United States, South Korean officials said July 6. The sites of the presidential Blue House, the Defense Ministry, the National Assembly, Shinhan Bank, Korea Exchange Bank and top Inter-

[\[Return to top\]](#)



July 2010

net portal Naver went down or had access problems, said a spokeswoman at Korea Information Security Agency. The alleged attacks appeared to be linked to the knockout of service of websites of several government agencies in the United States. The U.S. sites were hit by a widespread and unusually resilient computer attack that began July 4. In the United States, the Treasury Department, Secret Service, Federal Trade Commission and Transportation Department Web sites were all down at varying points, according to officials inside and outside the government. Some of the sites were still experiencing problems late July 6. Some of the South Korea sites remained unstable or inaccessible July 7. The South Korean spokeswoman said there have been no immediate reports of financial damage or leaking of confidential national information from the alleged cyber attack, which appeared aimed only at paralyzing Web sites.

**Associated Press:** [South Korean government websites, banks hit by suspected cyber attack](#)

### ***Other Cyber Attacks articles:***

- *July 22* – (Communications) **Reuters:** [Baidu may press claims over hackers: U.S. judge](#). China's leading search engine, Baidu Inc, can sue its U.S.-based domain name service provider, Register.com Inc, for breach of contract, gross negligence and recklessness related to an attack by hackers, a U.S. judge ruled July 22. A January 11 attack prevented Internet users around the world from gaining access to Baidu for 5 hours and disrupted its operations for 2 days, according to the lawsuit. Baidu holds the greatest share of the Chinese online search market.
- *July 26* – (International) **The Register:** [EU climate exchange website hit by green-hat hacker](#). An EU Climate Exchange Web site was hacked as part of a political protest against carbon credits by a green-hat defacement crew. The front page of the ECX.eu Web site was sprayed with digital graffiti lampooning the concept of applying a market-based approach to tackling carbon emissions. An anonymous group of hacktivists called Decocidio claimed responsibility for the attack, which took place late July 22.
- *July 28* – (International) **DarkReading:** [Panda Security, Defence Intelligence help bring down butterfly botnet author](#). Spain's Panda Security and Canada's Defense Intelligence provided key information to the FBI and international authorities that led to catching 23 year-old, "Iserdo," the confirmed author of the Butterfly botnet kit. With their partners in the Mariposa Working Group, the two security firms identified Iserdo by analyzing the software behind the Mariposa botnet that compromised millions of systems worldwide. Iserdo was arrested in Maribor, Slovenia.

### **Data Breach/Information Gathering**

#### **Security glitch exposes WellPoint data again**

**June 29 – (Health)**

WellPoint Inc. has notified 470,000 individual insurance customers that medical records, credit card numbers and other sensitive information may have been exposed in the latest security breach of the health insurer's records. The Indianapolis company said the problem stemmed from an online program customers can use to track the progress of their application for coverage. It was fixed in March. A spokeswoman said an outside vendor had upgraded the insurer's application tracker last October, and told the insurer all security measures were back in place. But a California customer discovered that she could call up confidential information of other customers by manipulating Web addresses used in the program. Customers use a Web site and password to track their applications. WellPoint learned about

[\[Return to top\]](#)



July 2010

the problem when the customer filed a lawsuit in March.

Associated Press: [Security glitch exposes WellPoint data again](#)

### **White hat uses Foursquare privacy hole to capture 875K check-ins**

*June 29 – (Information Technology)*

A coder figured out that Foursquare had a privacy leak because of how it published user check-ins on Web pages for each location. On pages like the one for San Francisco's Ferry Building, Foursquare shows a random grid of 50 pictures of users who most recently checked in, no matter what their privacy settings. When a new check-in occurs, the site includes that person's photo somewhere in the grid. So the coder built a custom scraper that loaded the Foursquare Web page for each location in San Francisco, looked for the differences, and logged changes. Even though he was using an old computer running through the slow but anonymous Tor network, he estimates he logged 70 percent of all check-ins over three weeks. That amounts to 875,000 check-ins. The coder reported the privacy breach to Foursquare June 20, and the company admitted the bug existed. They asked for time to fix the bug, and then, according to an e-mail sent to the coder, the company modified its privacy settings to let users opt out of being listed on location's Web pages. The site previously allowed users to opt out of being listed in the "Who's here now" function, but until June 29, that button did not apply to listing "Who's checked in there."

Wired.com: [White hat uses Foursquare privacy hole to capture 875K check-ins](#)

### **Fake femme fatale shows social network risks**

*July 22 – (Government Facilities; Defense Industrial Base; Information Technology)*

Hundreds of people in the information security, military and intelligence fields recently found themselves with egg on their faces after sharing personal information with a fictitious Navy cyberthreat analyst named "Robin Sage." Robin's profile on prominent social networking sites was created by a security researcher to illustrate the risks of social networking. In a conversation with Computerworld, the co-founder of Provide Security said he used a few photos to portray the fictional Sage on Facebook, LinkedIn and Twitter as an attractive, somewhat flirty cybergeek, with degrees from MIT and a prestigious prep school in New Hampshire. Then he established connections with 300 men and women from the U.S. military, intelligence agencies, information-security companies and government contractors. The goal was to determine how effective social networking sites can be in conducting covert intelligence-gathering. Despite some patently obvious red flags, such as noting that the 25-year-old Sage had worked professionally for 10 years, the scheme worked. The connections to Sage, who was depicted as a real-life Abby Scuito, a fictional character in CBS's NCIS television series, were established in less than a month. Many friends freely shared personal information and photos, invited Sage to conferences and asked her to review documents. Some "friends" at major companies, including Google and Lockheed Martin, even expressed interest in hiring her, he noted. Had Sage really been a foreign agent, she would have had access to a lot of useful information, the researcher said.

Computerworld: [Fake femme fatale shows social network risks](#)

### **Couple charged over hybrid car industrial espionage plot**

*July 23 – (Critical Manufacturing)*

A Troy, Michigan couple faces charges of stealing industrial secrets on hybrid cars from GM before attempting to sell the data to a Chinese auto manufacturer. A former GM worker

[\[Return to top\]](#)



July 2010

and her husband have been charged with four offenses, including unauthorized possession of trade secrets and wire fraud under an indictment unsealed July 22. GM reportedly places a value of \$40 million on the stolen documents. The former GM worker allegedly copied thousands of sensitive documents onto a hard disk after she was offered a severance agreement in January 2005. This hard drive was used by Millennium Technology International, a firm run by the two defendants, which months later allegedly offered hybrid-vehicle technology to Chery Automobile in China. The circumstances of the case raise serious questions about the security controls applied by GM to safeguard its research around the time of the alleged data theft. In May 2006, the couple's home was raided, leading to the recovery of computers containing industrial secrets, according to prosecutors.

**The Register:** [Couple charged over hybrid car industrial espionage plot](#)

### **NATO allies fear fallout of leaked Afghan war docs**

*July 26 – (Government Facilities)*

Several European NATO members have expressed concern that the fallout from a massive online leak of confidential U.S. documents on the Afghan war could extend well beyond the Internet — and could even affect the war itself. The U.S. records cover six years of the war in Afghanistan, including previously unknown accounts of civilian deaths and targeted attacks on Taliban members. “A lot of it is mundane, but a lot of it is also very serious, on-the-ground, battlefield reports about the situation in the war, and right now it doesn't seem like it is matching the narrative that is coming out of the Pentagon,” a freelance journalist told CTV's Canada AM during a July 26 interview. NATO declined to comment, but representatives from NATO member countries said they hope the leaks do not pose problems for the war effort. The German foreign minister warned that “backlashes” could result from the 91,000 records posted online by the WikiLeaks organization July 25.

**CTV News; Associated Press; Canadian Press:** [NATO allies fear fallout of leaked Afghan war docs](#)

### **Russian gang uses botnets to automate check counterfeiting**

*July 28 – (Banking)*

The director of SecureWorks has uncovered a sophisticated check-counterfeiting ring that uses compromised computers to steal and print millions of dollars worth of bogus invoices, and then recruit money mules to cash them. The highly automated scheme starts by infiltrating online check archiving and verification services that store huge numbers of previously cashed checks. It then scrapes online job sites for e-mail addresses of people looking for work, and sends personalized messages offering jobs performing financial transactions for an international company. The scammers then use stolen credit-card data to ship near exact replicas of checks to those who respond. The director was able to track the operation by infecting a lab computer and observing its interactions with command and control channels. A database file the criminals carelessly exposed showed 3,285 checks had been printed since June of 2009, and 2,884 job seekers had responded to the employment offer. Assuming each check was written in amounts of \$2,800, a threshold sum that brings increased scrutiny to transactions, the director estimates the checks were valued at about \$9 million.

**The Register:** [Russian gang uses botnets to automate check counterfeiting](#)

### **Other Data Breach/Information Gathering articles:**

- *June 30 – (Health) The Register:* [Medical diagnoses for 130,000 people vanish into](#)



July 2010

- [thin air](#). New York-based Lincoln Medical and Mental Health Center has become one of the latest medical providers to expose highly sensitive patient data after CDs containing unencrypted data sent by FedEx never made it to their destination. The breach exposed medical and psychological diagnoses, and procedures for 130,495 patients.
- *July 1* – (Banking) *Associated Press*: [NY ex-bank computer tech admits ID theft, \\$1M scam](#). Prosecutors said a computer technician admitted to using a three-month stint at a New York bank to steal 2,000 other employees' identities, and then use them for years to loot about \$1 million from charities.
  - *July 7* – (Banking; Government Facilities) *Honolulu Star-Advertiser*: [UH breach affects 53,000](#). University of Hawaii officials said July 6 that a hacker breached the security of a parking office computer server that contained personal information of 53,000 people. There were 40,870 Social Security numbers and 200 credit cards that were possibly compromised.
  - *July 19* – (Government Facilities) *SC Magazine*: [Personal details of 93,000 staff and students at university could be exposed after database compromise](#). The personal details of 93,000 people have been exposed, following the compromise of a database at a college in Storm Lake, Iowa. The social security numbers, addresses, and driver's license information of students and staff at Buena Vista University dating back to 1987 could be vulnerable.
  - *July 20* – (Health) *Healthcare IT News*: [Mass. hospital investigating the potential loss of back-up data for 800,000 individuals](#). South Shore Hospital in Weymouth, Massachusetts, reported July 14 that back-up computer files containing personal, health and financial information for approximately 800,000 individuals may have been lost by a data-management company that was hired to destroy them.
  - *July 20* – (Banking) *Krebs on Security*: [Skimmers siphoning card data at the pump](#). Thieves recently attached bank card skimmers to gas pumps at more than 30 service stations along several major highways in and around Denver, Colorado. Similar attacks have hit other parts of the country. Police in Arizona also are dealing with a spike in reports about skimmers showing up at gas pumps, prompting the governor to urge the Arizona Department of Weights and Measures to increase inspections.
  - *July 27* – (Banking) *Gainesville Sun*: [Area credit card skimmers may be part of statewide theft ring](#). Law enforcement officials said a dozen credit-card skimming devices have been found this month at Gainesville, Florida area gas stations along with other devices found at St. Johns and Flagler County stations, in what appears to be a statewide theft ring.

### Threats and Vulnerabilities

#### Malware takes aim at defense contractors

*July 1 – (Defense Industrial Base)*

A sophisticated malware operation targeting defense contractors has been uncovered, according to experts. Researchers at Symantec Hosted Services said the operation involved compromising the site of one firm, and then using the hacked site to host a malware attack on another contractor. The attack began when the first company's site was compromised and embedded with a landing page and obfuscated exploit code. The attackers then sent a series of e-mails to employees of a second firm, claiming the company's chief executive had been arrested by U.S. authorities. When the targeted users clicked on an included link, they were directed to the compromised site of the first company, which then attempted to exploit a

[\[Return to top\]](#)



July 2010

new vulnerability in the Windows Help component, and infect users with an assortment of malicious software.

V3.co.uk: <http://www.v3.co.uk/v3/news/2265825/malware-takes-aim-defence>

### **Symbian malware creating mobile botnet**

*July 7 – (Information Technology)*

Mobile security firm NetQin claims to have found malware spreading via Symbian Series 60 handsets, which is being used to build a mobile botnet. The company has identified three pieces of malware masquerading as mobile games or special offers, which infect versions three and five of the Series 60 Symbian platform. NetQin estimates that 100,000 handsets have been infected and could be used to form a mobile botnet. "... These botnets do one of two things: send messages to all the contacts of the address book directly, or send messages to random phone numbers by connecting to a server. The viruses will delete the sent messages from the user's outbox and SMS log. All messages contain URLs linked to malicious sites that users won't be able to see until after they've fallen into the virus trap," NetQin reported. However, a Symbian Foundation representative told V3.co.uk that there is no evidence that the malware is using handsets in a botnet, and that it had already rescinded the software's certification. The spokesman also said that NetQin had not contacted the Symbian Foundation about the malware, which he described as "very minor."

V3.co.uk: <http://www.v3.co.uk/v3/news/2266108/symbian-malware-creating-mobile>

### **Bizarre phone ransom Trojan found by researchers**

*July 13 – (Information Technology)*

Researchers have discovered a bizarre piece of Trojan ransomware which disables programs on infected PCs before demanding victims to make a small payment to a Ukrainian mobile phone network in return for an unlock code. According to Webroot, the Krotten ransom Trojan eschews complex encryption taken by a range of ransomware programs in the past and simply sets out to interfere with the host PC in as many ways as possible. It starts out by changing 40 registry keys for a number of Windows settings, adding expletive text in Russian to the Internet Explorer title bar, disabling features such as the Windows Start bar, and blocking the ability to print or open files. Rebooting the system will display the following text box in Russian, which Webroot translates in its blog on Krotten. "In order to restore normal functionality of your computer without losing all the information! and saving money, send me an e-mail to xxxx@xxx.xxx, with the code for replenishing a Kyivstar account with 30 Grivna. In response within 24 hours you will get an e-mail with a file to remove this program from your computer." Grivna is the currency of the Ukraine and 30 Grivna is the equivalent of less than \$4. The Trojan was, the researchers reckon, also written using a DIY malware kit called Sign Of Misery (SOM).

PC Advisor UK: <http://www.networkworld.com/news/2010/071310-bizarre-phone-ransom-trojan-found.html?hpg1=bn>

### **Deepwater Horizon alarm had been 'inhibited,' technician testifies**

*July 23 – (Energy)*

An alarm system on the Deepwater Horizon had been "inhibited" for about a year before the April 20 explosion in the Gulf of Mexico that killed 11 workers and started the worst oil disaster in the nation's history, the platform's chief electronics technician testified to a federal panel July 23. An inhibited mode means sensors for toxic or combustible gases or fire



July 2010

are active and will alert the platform's computer system, but the computer does not trigger an audible or visual alarm, a technician told the six-member panel. Supervisors on the Transocean rig were aware that the alarm system had been inhibited. "When I discovered about a year ago it was inhibited, I inquired as to why it was inhibited, and the explanation I got is that ... they did not want people woke up at 3 o'clock in the morning due to false alarms," the technician said. The rig's general alarm system also has normal and override settings, the technician testified. Under an override setting, the computer will not recognize the sensor information for any purpose, he said. The alarm system's visual alerts were on light towers throughout the rig, he said. A red light signified fire, a yellow light meant toxic gas, and a blue light indicated combustible gases.

CNN: [Deepwater Horizon alarm had been 'inhibited,' technician testifies](#)

### **Black Hat conference demonstration reveals ATM security risk**

*July 29 – (Banking)*

At the Black Hat conference in Las Vegas, IOActive's director of security research gave a demonstration of how he learned to crack the security of various stand alone ATMs after coming across several errors and security weaknesses in their [software] coding, allowing him to gain full access to the machines' safes. He wrote multiple programs to exploit some of the machines' weaknesses including one that allows him to gain remote entry without the need of a password, which he calls Dillinger, and a second program, Scrooge, that relies on a back-door entry with the ability to conceal itself from the machine's main operating system. In the case of Triton ATMs, the researcher found the motherboard of the machine was lacking in physical security, and once he had gained access to it, he was easily able to use a similar back-door technique then simply trick the machine into thinking that the hack was actually a legitimate update. So far, the researcher has attempted to hack four different ATMs and, as he demonstrated at the conference, he found that the same "game over vulnerability" enabled him to crack every one of them.

Daniweb: [Black Hat conference demonstration reveals ATM security risk](#)

### **Even with SSL/TLS, browsers still are susceptible to attack**

*July 29 – (Information Technology/Banking)*

Two researchers publicized 24 methods attackers can use to take over users' accounts or assume control of a website without the need for any exploits, due to the way browsers implement "HTTPS." For any of the two dozen attacks to work, however, a criminal would have to have assumed control of a user's computer via a man-in-the-middle (MITM) exploit, by which an attacker intercepts communications between two systems. But the researchers wanted to show that HTTPS protection alone will not stop bad things from happening. For example, the pair detailed an attack known as "session fixation" that takes advantage of the fact that banks using HTTPS do not change a user's cookie after they login; they simply mark it as valid. As a result, an attacker with MITM control could visit the bank site ahead of the user and set the cookie, essentially logging in the crook as the legitimate user. Another scenario, known as "delayed pop-up," involves a user who visits a website, such as a bank, and clicks on a link to go the SSL-protected version of the site. This opens a second tab, but if the attacker has control of the first tab, he is able to change the other HTTPS tab to redirect users to malicious executables or authentication forms. However, the researchers said the reliance on MITM makes the scenarios the researchers demonstrated is unlikely to happen on a widespread scale.



July 2010

SC Magazine: [Even with SSL/TLS, browsers still are susceptible to attack](#)

**Other Threats and Vulnerabilities articles:**

- *June 30* – (Information Technology) **IDG News Service:** [Sony says 535,000 laptops at risk of overheating](#). More than half a million Sony laptops sold this year contain a software bug that could lead them to overheat, the company said June 30. Sony has recorded 39 cases of overheating among Vaio F and C series laptops that have been on sale since January.
- *June 30* – (Information Technology) **Help Net Security:** [Virus production from Russia increases again](#). Virus production from Russia is on the upswing after a temporary decline last month when Russian hosting service PROXIEZ-NET was taken down in early May. Russia is now responsible for 7.4 percent of the world's malware, and is back to being in the top four virus-producing countries.
- *July 1* – (Emergency Services Sector) **Rochester Post-Bulletin:** [Month of glitches preceded siren failure on night of tornado](#). A corrupted computer-activation code is responsible for several northwest Rochester, Minnesota weather sirens failing to sound during a June 17 storm that included damaging winds and one or more tornadoes.
- *July 7* – (Information Technology) **The Register:** [Trojan skewers security software with Windows](#). Security watchers have discovered a Trojan that uses built-in Windows functionality to overwrite security software and compromise systems by disguising itself as an antivirus update package.
- *July 13* – (Information Technology) **IDG News Service:** [With fix now out, Microsoft sees jump in XP attacks](#). Microsoft urged Windows users to update their software July 13, saying it has now seen more than 25,000 attacks leveraging one of the critical bugs fixed in July's monthly security patches.
- *July 13* – (Banking) **The Register:** [Zeus baddies unleash nasty new bank Trojan](#). Hackers have created a new version of the Zeus crimeware toolkit that is designed to swipe bank log-in details of Spanish, German, U.K. and U.S. banks. The malware payload is far more selective in the banks it targets.
- *July 14* – (Information Technology) **The H Security:** [Scareware: Now with live support](#). A researcher of Kaspersky has discovered that scareware distributors now offer live support, convince victims in fluent English that their software is genuine, and get them to install the bogus full product. Users installing fake anti-virus software Security Master AV and clicking on the "Online Support" button are directed to a chat window in which they can put questions directly to the scareware "vendor."
- *July 14* – (Banking) **Network World:** [ZeuS Trojan attempts to exploit MasterCard, Visa security programs](#). The notorious ZeuS banking Trojan is popping up on infected computers with a fake enrollment screen for the "Verified By Visa" or "MasterCard SecureCode Security" programs, luring victims into a fraudulent online enrollment action that would end up giving criminals sensitive financial data.
- *July 15* – (Information Technology) **IDG News Service:** [Researchers: Password crack could affect millions](#). Two security experts said they have discovered a basic security flaw that affects dozens of open-source software libraries, including those used by software that implements the OAuth and OpenID standards, which are used to check passwords and user names when people log into Web sites, such as Twitter and Digg.
- *July 16* – (All Sectors) **Tech Herald:** [Criminals pushing Rogue anti-Virus disguised as scanned documents](#). E-Mail messages claiming to be scanned documents are the

[\[Return to top\]](#)



July 2010

latest attempt by criminals to push rogue anti-virus malware to the masses. The messages, which claim to come from a Xerox WorkCentre Pro, come with a Zip file that will immediately infect the system if accessed.

- *July 22* – (All Sectors) **Help Net Security**: [1.2 million infected by Eleonore exploits toolkit](#). AVG's Web security research team has discovered a network of 1.2 million malware-infected computers controlled by cybercriminals who were using the Eleonore exploit toolkit -- commercial-attack software enabling cybercriminals to infect and monitor compromised PCs.
- *July 23* – (Information Technology) **The Register**: [Dell blames staff for malware infection](#). Dell said human error was to blame for mistakes which led it to ship a number of replacement server motherboards to customers pre-loaded with spyware. The company declined to say whether it was running anti-virus software at its factory but said it had taken steps to improve processes.
- *July 23* – (Information Technology) **IDG News Service**: [Researcher finds Safari reveals personal information](#). Apple's Safari's AutoFill feature could be abused by hackers to harvest personal information, according to a security researcher.
- *July 23* – (Information Technology) **The New New Internet**: [Hacker enlists other unwitting hackers in scam](#). A new freeware phishing kit being offered in hacker forums offers a way to set up fake Web sites and spam e-mails to capture users' legitimate log-in credentials. However, the malware writers are able to siphon off a significant portion of entered log-in credentials, leaving only a few for the cyber criminals employing the phishing kit.
- *July 27* – (Banking) **eWeek**: [Citi, Apple disclose iPhone app security flaw](#). Citigroup and Apple are encouraging users who downloaded Citi's banking application for the iPhone to upgrade to a new version after a security flaw was discovered.
- *July 28* – (Energy) **The Register**: [Smart meters pose hacker kill-switch risk, warn boffins](#). A professor in security engineering at the University of Cambridge Computer Laboratory warns that the move to smart metering introduces a "strategic vulnerability" that hackers might conceivably exploit to remotely switch off elements on the gas or electricity supply grid.

### Policy, Legislation and Governance

#### HHS proposes new privacy, security rules

*July 8 – (Health)*

The Department of Health and Human Services (HHS) secretary announced July 8 new proposed privacy and security rules and resources. The secretary said they would strengthen the privacy of health information, and help all Americans understand their rights and the resources available to safeguard their personal health data. The rules are part of an effort led by the Office of the National Coordinator for Health Information Technology and the HHS Office for Civil Rights to ensure Americans trust personal health data exchange. The proposed rules come as part of the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to ensure broader individual rights and stronger protections when third parties handle individually identifiable health information.

**Healthcare IT News:** [HHS proposes new privacy, security rules](#)



July 2010

### **NYSE sets new trading collars**

*July 15 – (Banking)*

The New York Stock Exchange’s electronic exchange will introduce new limits designed to prevent erroneous trades that have triggered trading halts installed after the market’s “flash crash” in May. The rules will prevent the buying or selling of stocks at a price outside of set limits, the exchange said. “This would help prevent the erroneous trades from taking place to begin with,” said a spokesman for NYSE Euronext, owner of the Big Board. Since the exchanges established a market-wide, circuit-breaker pilot program last month in response to the May 6 “flash crash,” trading halts have been triggered in three stocks following erroneous trades. The circuit breakers, established for all individual stocks in the Standard & Poor’s 500-stock index, halt trading in a stock for 5-minutes if its price moves 10 percent up or down within 5-minutes. The spokesman said the circuit breakers will remain in place, but likely will occur less frequently with the new system.

**Wall Street Journal:** [NYSE sets new trading collars](#)

### **A first: 15 nations agree to start working together on cyber arms control**

*July 19 – (All Sectors)*

A group of nations including the United States, China, and Russia have for the first time signaled a willingness to engage in reducing the threat of attacks on each others’ computer networks. Although the agreement, reached at the UN, provides [recommendations](#) only, a cyberwarfare expert with the Council on Foreign Relations said it represents a “significant change in U.S posture” and is part of the White House administration’s strategy of diplomatic engagement. A Washington Post reporter [writes](#) that among other steps, the group recommended that the UN create norms of accepted behavior in cyberspace, exchange information on national legislation and cybersecurity strategies, and strengthen the capacity of less-developed countries to protect their computer systems.

**Homeland Security News:** [A first: 15 nations agree to start working together on cyber arms control](#)

### **Other Policy, Legislation and Governance articles:**

- *July 1 – (Government Facilities) Government Computer News:* [Security guidance needed before government moves to the cloud, GAO says](#). Cloud computing offers the promise of greater efficiency, flexibility and even security, but federal agencies will not adopt the technology on a large scale until issues of securing cloud infrastructure and services are addressed systematically, the Government Accountability Office (GAO) said in a report.
- *July 8 – (All Sectors) ComputerWorld:* [GAO slams White House for failing to lead on cybersecurity](#). The GAO said in a report released the United States risks falling behind other countries on cybersecurity matters. The report highlighted the United States being unable to adequately protect its interests in cyberspace, and that the White House Office of Science and Technology Policy has so far failed to live up to its responsibility to coordinate a national cybersecurity R&D agenda.
- *July 8 – (Defense Industrial Base) Nextgov:* [U.S. nuke agency announces new data, physical security controls](#). The National Nuclear Security Administration, which oversees the nation’s nuclear weapons stockpile, announced on July 8 the rollout of new information and physical security controls aimed at balancing efficiency and safety. But officials said the implementation of information-security improvements is about a year



July 2010

- behind the progress the agency has made on physical protection.
- *July 8* – (All Sectors) *Nextgov*: [Official calls securing critical infrastructure against cyberattack impractical](#). Securing the nation’s power grid and other computer systems that operate the nation’s critical infrastructure against cyberattack is unrealistic, because companies cannot afford to check if suppliers have provided trustworthy products, an intelligence official from the Energy Department said July 8.
  - *July 13* – (Information Technology) *The Register*: [Facebook for hackers shut down in Pakistan](#). Five alleged hackers have been arrested by Pakistani authorities in raids that led to the closure the Pakbugs hacking and carding forum. Pakbugs is blamed for running amok across thousands of Web sites belonging to various governmental and non-governmental organizations in Pakistan and elsewhere.
  - *July 15* – (All Sectors) *DarkReading*: [White House issues progress report on cyber-security](#). The U.S. President and his cybersecurity czar both offered optimistic progress reports and encouraged more activity in the private sector. The White House said it is putting cybersecurity into its agenda as a “key management priority.” The Administration also pointed to changes in FISMA guidance.
  - *July 15* – (Banking) *Computerworld*: [Visa moves to reduce payment card data in retail systems](#). A new payment-card, security initiative launched by Visa July 14 could eliminate the need for retailers and other organizations to store full, 16-digit, credit- and debit-card numbers on their systems.

### Reports and Publications

**DarkReading:** [More than 80 percent of U.S. enterprises hit by advanced attacks](#). The [Ponemon Institute’s](#) new “Growing Risks of Advanced Threats” report has found that 83 percent of U.S. enterprises have been victimized by so-called advanced threats, attacks that use zero-day exploits, social engineering, or other sophisticated methods of getting past security measures.

**SC Magazine:** [United States lacking adequate cyber workforce](#). The United States is lacking an adequate number of individuals within the federal government and private sector with the technical skills necessary to secure cyberspace, concludes a [report](#) released by the Center for Strategic and International Studies (CSIS).

**Help Net Security:** [Spam now a vehicle for heavy malware distribution](#). AppRiver released a detailed [summary and analysis](#) of spam and malware trends traced between January and June 2010. During this timeframe, they quarantined more than 26 billion spam messages to protect its customer base of 45,000 corporations and six million mailboxes.

**The H Security:** [Windows exploit protection mostly unused](#). According to an [analysis](#) by security firm Secunia, very few applications use the Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) features of Windows which can render attacks on vulnerabilities ineffective.

**Homeland Security NewsWire:** [Secureworks World Cup of cyber security finds India the safest nation, U.S. the least safe](#). The United States is the least cyber-secure country in the world, according to [SecureWorks](#), an information security service provider.



July 2010

**CNET News:** [Report: Adobe Reader, IE top vulnerability list](#). The most exploited vulnerabilities tend to be Adobe Reader and Internet Explorer, but a rising target for exploits is Java, according to a [report](#) released July 14 by M86 Security Labs.

**Homeland Security NewsWire:** [New report: Apple software has the most vulnerabilities](#). A new [report](#) from security software provider Secunia, finds that the latest data shows Apple has surpassed Oracle and even Microsoft in accounting for the most software vulnerabilities, though the No. 1 ranking is related only to the number of vulnerabilities.

**DarkReading:** [Third-party content could threaten websites, study says](#). A [report](#) by Dasient, a security start-up company, found that third-party content can be compromised to gain access to a corporate Web site, but most companies do not do much to secure it.

**BankInfoSecurity.com:** [Most breaches caused by crime gangs](#). The [2010 Verizon Data Breach Investigations Report](#) found that organized crime was responsible for 85 percent of all stolen data in 2009. And stolen credentials were the most common way to gain unauthorized access into organizations.

**IDG News Service:** [Verizon: Data breaches often caused by configuration errors](#). Hackers appear to be increasingly counting on configuration problems and programming errors rather than software vulnerabilities in order to steal information from computer systems, according to a new [study](#) from Verizon.

**DarkReading:** [White paper: Corporate ignorance of phishing may prove catastrophic](#). Red Condor's [white paper](#) suggests that companies and their executives have ignored the phishing problem, or even scoffed at the notion that phishing poses threats on par with traditional methods of corporate espionage.

**DarkReading:** [One Breach = \\$1 Million To \\$53 Million In Damages Per Year, Report Says](#). Organizations are getting hit by at least one successful attack per week, and the annualized cost to their bottom lines, ranged from \$1 million to \$53 million. The independent Ponemon Institute's [The First Annual Cost of Cyber Crime Study](#) showed a median cost of \$3.8 million attack per year, a price tag that includes everything from detection, investigation, containment, and recovery any post-response operations.

Your comments and suggestions are highly valued. Please send us feedback at:  
[cikr.productfeedback@hq.dhs.gov](mailto:cikr.productfeedback@hq.dhs.gov)

This report is posted regularly to the [Homeland Security Information Network Critical Sectors](#) portal. If you would like to become a HSIN-CS member, please contact:  
[CIKRISAccess@DHS.gov](mailto:CIKRISAccess@DHS.gov)

*Unless otherwise noted, all definitions of cyber terms provided in this report are provided by the SANS [Glossary of Terms Used in Security and Intrusion Detection](#).*