



September 2010

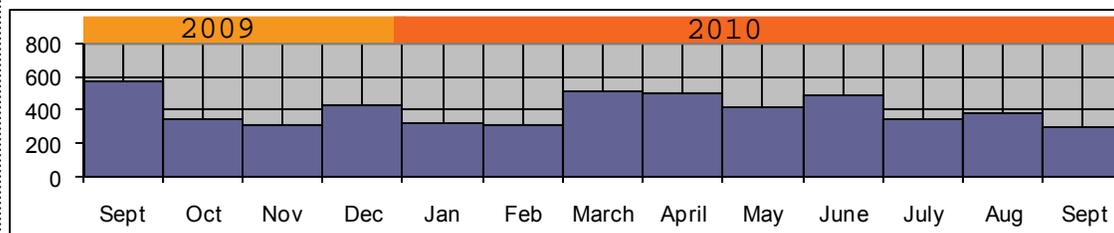
### IN THIS REPORT

- 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

[The Register](#) reported that a Web site run by the conservative Tea Party movement was overrun by the denizens of 4chan September 21. Web site vulnerabilities on the official teaparty.org Web site allowed pranksters to divert surfers landing on the photo section of the site to smut and shock sites. According to [IDG News Service](#), a hacker who claims he was behind a fast-spreading e-mail worm that crippled corporate networks recently, said that the worm was designed, in part, as a propaganda tool. The hacker, known as Iraq Resistance, responded to inquiries sent to an e-mail address associated with the "Here you have" worm, which during a brief period early September 9 accounted for about 10 percent of the spam on the Internet. [The Register](#) also reported privacy activists were upset about the use of flash cookies to respawn traditional Web site cookies. But an even more persistent type of cookie that is almost impossible to kill off may lie just around the corner. So-called invulnerable evercookies use eight different techniques and locations to hide on tagged systems. [The H Security](#) stated that Microsoft, in a security advisory, has confirmed the vulnerability in the process used by ASP.NET applications to encrypt cookies and other session information. In the announcement for the security advisory, Microsoft said it was not, so far, aware of any attacks. In other news:

- [The Register](#) reported that Vodafone, a global telecommunications company headquartered in England, has been caught taking liberties with customers' e-mail accounts, and it seems at least some of the customers are not happy about the practice.
- [DarkReading](#) reported that a federal court judge recommended that Microsoft be allowed to acquire the 276 Internet domains that formerly drove the Waledac botnet, which plagued users and enterprises for more than 1 year.



September 2010

**Programmable Logic Controllers:** PLCs are computer-based solid-state devices that control industrial equipment and processes. While PLCs are control system components used throughout SCADA and DCS systems, they are often the primary components in smaller control system configurations used to provide operational control of discrete processes such as automobile assembly lines and power plant soot blower controls. PLCs are used extensively in almost all industrial processes. ([Arclight](#))

### **\*Special Coverage\***

On September 14, Microsoft has credited security partners at Kaspersky Lab and Symantec for helping to [close a critical Windows vulnerability](#) that was being exploited by a sophisticated worm that has attacked industrial plants around the world. The bug in the Windows Print Spooler, which was one of at least 11 vulnerabilities Microsoft patched September 14, was under active attack by the Stuxnet worm, a sophisticated piece of malware that penetrated factories and other industrial plants. Meanwhile, Siemens [reported](#) that industrial plants in Germany have also been hit by the Stuxnet worm. According to a spokesperson for Siemens, about one third of the 15 infections discovered at industrial plants worldwide have been found at sites in the German process industry sector. Siemens' own plants are said not to be affected. Analyses by Siemens have confirmed that Stuxnet can, in theory, manipulate **Programmable Logic Controllers**.

Shortly after the Siemens report, speculation began as to the target of Stuxnet. The [emerging consensus](#) of security experts who have examined the Stuxnet worm is that it was built to destroy operations at one target: possibly Iran's Bushehr nuclear reactor. In recent weeks, they have broken the cryptographic code behind the software and taken a look at how the worm operates in test environments. Researchers agree that Stuxnet was built by a very sophisticated and capable attacker — possibly a nation-state — and it was designed to destroy something big. Stuxnet also reminded the Energy community that power companies and organizations that run supervisory control and data acquisition (SCADA) and process control systems face challenges securing this traditionally proprietary technology. Many of these products have been known to carry vulnerabilities for years, and typical security tools cannot drill down into this often-closed software. The [CSO of NetWitness](#) believes that the SCADA and power industry will have to follow what retail did with its old POS systems when PCI hit and they needed security.

Finally, Stuxnet may have taken an [Indian satellite offline](#). On July 7, 2010, a power glitch in the solar panels of India's INSAT-4B satellite resulted in 12 of its 24 transponders shutting down. As a result, an estimated 70 percent of India's Direct-To-Home (DTH) companies' customers were without service. India's DTH operators include Sun TV and state-run Doordarshan and data services of Tata VSNL. Once it became apparent that INSAT-4B was effectively dead, SunDirect ordered its servicemen to redirect customer satellite dishes to point to ASIAT-5, a Chinese satellite owned and operated by Asia Satellite Telecommunications Co., Ltd. India's Space Research Organization is a Siemens customer. According to the resumes of two former engineers who worked at the ISRO's Liquid Propulsion Systems Center, the Siemens software in use is Siemens S7-400 PLC and SIMATIC WinCC, both of which will activate the Stuxnet worm.

### **Cyber Attacks**

#### **4chan invades Tea Party Website**

*September 22 – (Commercial)*

A Web site run by the conservative Tea Party movement was overrun by the denizens of 4chan September 21. Web site vulnerabilities on the official teaparty.org Web site allowed pranksters to divert surfers landing on the photo section of the site to smut and shock sites. It is unclear what Web site security shortcomings were exploited in that attack and whether these are now closed. The assault coincides with ongoing DDoS attacks by members of 4chan against entertainment industry Web sites in protest against legal actions against Tor-

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



September 2010

rent tracker Web site The Pirate Bay. The Oregon Tea Party made the mistake of using the “We Are Legion” slogan of Anonymous, the anti-Scientology movement that spawned in 4chan, in its official materials this summer. In response, Anonymous hacked the Tea Party’s Facebook page, posting flames and image macros, before the local branch of the dissident conservative movement promised to stop using the slogan.

**The Register:** [4chan invades Tea Party Website](#)

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

#### **Newly discovered World Cup database breach exposed 250,000 attendees’ details**

*September 10 – (Banking)*

Hundreds of thousands of attendees at the 2006 World Cup international soccer tournament in Germany were put at risk of identity theft, though the major breach of a Federation Internationale de Football Association (FIFA) database was only recently uncovered. Initially reported by Norwegian newspaper Dagbladet, the breach came to light when an employee of the firm in charge of World Cup 2010 ticketing, circulated an e-mail peddling more than 250,000 2006 World Cup customer details, including such personal information as birth dates and passport information. According to the director of security strategy at database monitoring firm Imperva, the customer data in question came from the German event 4 years ago and not the South African World Cup. He said the event is indicative of a number of failures, including carelessness with older databases and unused data, a failure to think beyond the conclusion of the event, and a failure to have a full data security protection and destruction strategy. The firm in charge of ticketing and ticketing data at the South African World Cup, Match, a subsidiary of U.K.-based Byrom, was not in charge of ticketing for Germany’s World Cup. It did confirm that it was its own employee who appeared to be responsible for the data’s dissemination. However, it categorically denied the data came from its own database.

**DarkReading:** [Newly discovered World Cup database breach exposed 250,000 attendees’ details](#)

#### **Fake ‘universal’ iPhone jailbreaking exploit contains Trojan**

*September 20 – (IT)*

Even though a hacker announced he was working on an exploit that will change this and will allow users to jailbreak any existing or future iPhone or iPad (regardless of the iOS version), this exploit has yet to see the light of day. Aware that the jailbreaking community is eagerly waiting for the solution, miscreants have tried to push malware. According to a Kaspersky Lab expert, the awaited exploit will be called “Greenpois0n,” so they named the .rar archive that contains the information-stealing Trojan greenpois0n\_By p0sixninja and made it available for download on popular Torrent sites. Web sites selling fake tools that can supposedly jailbreak any iPhone with any iOS have also appeared. Selling these tools for a price that goes up to \$40, they are also trying to capitalize on the users’ lack of patience.

**Help Net Security:** [Fake ‘universal’ iPhone jailbreaking exploit contains Trojan](#)

#### **Vodafone shares subscriber info with world**

*September 22 – (Communications)*

Vodafone, a global telecommunications company headquartered in England, has been

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



September 2010

caught taking liberties with customers' e-mail accounts, and it seems at least some of the customers are not happy about the practice. The problem is with the password reminder feature on the "My account" section of the carrier's Web site. All one has to do is enter the phone number of a person. If they have an online account, Vodafone gladly gives up their e-mail address. The Register was able to test the feature and it worked as described. "There is nothing to stop a determined spammer from entering thousands of numbers and getting a long list of email addresses," a Vodafone subscriber wrote. "Nothing to stop a fraudster from sending you an email to an address you only use with Vodafone."

**The Register:** [Vodafone shares subscriber info with world](#)

### Accounts raided in global bank hack

#### *October 1 – (International)*

More than 100 people have been charged in an alleged global scheme to use computer viruses to steal at least \$3 million from U.S. bank accounts. The U.S. investigation is related to the arrest of 19 people in London September 28, in a probe into an international cybercrime group that allegedly stole at least \$9.5 million from U.K. banks, a person familiar with the investigation said September 30. According to U.S. court documents, computer hackers in Eastern Europe used the Zeus Trojan to access bank accounts of small- and mid-size businesses and municipal entities in the United States. The charges in New York include conspiracies to commit bank fraud, possess false identification documents, commit wire fraud, commit money laundering, and make false use of a passport. Persons named in criminal complaints in federal court in Manhattan include citizens of Russia and Moldova. Nine people have been arrested in the New York area, while one person has been taken into custody elsewhere in the United States, the FBI's New York office confirmed September 30. Many of those arrested in the New York area are money mules who are used to funnel money to the cybercrime group.

**Wall Street Journal:** [More than 60 charged in cyber scheme](#)

See also; **Wall Street Journal:** [U.K. arrests 19 for bank cyberfraud](#)

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

- *September 1 – (IT) Help Net Security:* [Corporate espionage for dummies: HP scanners](#). HP has for some time, embedded remote scanning capabilities into network aware scanners, a functionality referred to as Webscan. Webscan allows one to not only remotely trigger the scanning functionality, but also retrieve the scanned image, all via Web browser. The feature is generally turned on by default with no security.
- *September 8 – (Banking; Government) AnnArbor.com:* [Eastern Michigan University investigating computer security breach, employee banking information may be compromised](#). An Eastern Michigan University computer server was hacked into September 3, potentially exposing employees' direct deposit banking information, some university passwords, and personal identification numbers, according to an e-mail sent to the EMU community September 3.
- *September 9 – (Banking) Computerworld:* [Hotel operator warns of data breach](#). HEI Hospitality, owner and operator of upscale hotels operating under the Marriott, Sheraton, Westin, and other monikers, has sent letters informing some 3,400 customers that their credit card data may have been compromised.
- *September 10 – (Health) Computerworld:* [Hospital appeals \\$250,000 fine for late breach disclosure](#). The Lucile Packard Children's Hospital at Stanford University in



September 2010

Palo Alto, California is appealing a \$250,000 fine imposed by the California Department of Public Health for its alleged delay in reporting a January 2010 data breach that exposed confidential patient data.

- *September 22 – (IT) **Help Net Security:** [Trojan stealing private key certificates.](#) Symantec warned about Infostealer.Nimkey, a Trojan that is designed to collect private key certificates, keystrokes, and clipboard data and send it to a Web site where the authors can collect them.*
- *September 29 – (IT) **Network World:** [Many Android apps leak user privacy data.](#) A recent test of prototype security code for Android phones found that 15 of 30 free Android Market applications sent users' private information to remote advertising servers, without the users being aware of what was being sent or to whom.*

### Threats and Vulnerabilities

#### IPv6 transition poses new security threats

*September 2 – (Communications; IT)*

IPv6 has been in the works for over a decade now, but with the exhaustion of the IPv4 address space expected anywhere from spring to June of 2011, the long transition to the new IP may finally be on the radar screen for some organizations. Unlike its predecessor, the “new” protocol was built with security in mind: it comes with IPSec encryption, for instance, and its massive address space could help prevent worms from propagating, security experts said. But its adoption also poses new security issues, everything from distributed denial-of-service (DDoS) attacks to new vulnerabilities in IPv6 to misconfigurations that expose security holes. Some experts expect implementing DNSSEC in an IPv6 network to be simpler than in existing IPv4 networks.

**DarkReading:** [IPv6 transition poses new security threats](#)

#### Anti-US hacker takes credit for ‘Here you have’ worm

*September 12 – (All Sectors)*

A hacker who claims he was behind a fast-spreading e-mail worm that crippled corporate networks said that the worm was designed, in part, as a propaganda tool. The hacker, known as Iraq Resistance, responded to inquiries sent to an e-mail address associated with the “Here you have” worm, which during a brief period early September 9 accounted for about 10 percent of the spam on the Internet. Security experts agree that the worm could have caused more damage. However, it did include some very malicious components, such as password logging software and a backdoor program that could have been used to allow its creator to control infected machines. But because the software was not terribly sophisticated, it was quickly shut down as Web servers that it used to infect machines and issue new commands were taken offline.

**IDG News Service:** [Anti-US hacker takes credit for ‘Here you have’ worm](#)

#### Airborne laser test failure blamed on software error

*September 13 – (DIB)*

The recent test failure of the experimental U.S. Airborne Laser system was caused by a communications software glitch that led the weapon to prematurely stop firing its beam at a target missile, the Defense Department’s Missile Defense Agency said September 10. The September 1 test of the system installed on a converted Boeing 747 was intended to build off the success of a February firing by demonstrating the effectiveness of the chemical laser

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



September 2010

system at ranges greater than 100 miles. The system was able to identify and follow the liquid-fuel, short-range ballistic missile in its liftoff phase, according to an agency press release. “However, the experiment terminated early when corrupted beam control software steered the high energy laser slightly off center,” it stated. “Preliminary indications are that a communication software error within the system that controls the laser beam caused misalignment of the beam. The [Airborne Laser Test Bed] safety system detected this shift and immediately shut down the high energy laser.” The agency intends to relaunch flight tests starting with assessments September 13 of fixes to the ABL software.

**Global Security Newswire:** [Airborne laser test failure blamed on software error](#)

### **Unofficial fix brings temporary relief for critical Adobe vuln**

*September 15 – (IT)*

Security researchers have released what they say is an unofficial fix for the critical Adobe Reader vulnerability that is being actively exploited to install malware on machines running Microsoft Windows. The download replaces a buggy strcat call in a font-rendering DLL module with a more secure function, according to researchers at penetration-testing firm RamzAfzar. Protecting oneself from the underlying stack overflow flaw is as easy as overwriting the existing CoolType.dll located in the Acrobat Reader folder with the revised one. “We’ve decided to modify this strcat call and convert it to strncat,” they wrote. “Why? Because strncat at least receives the buffer size and how much bytes you want to copy from src to dest.” The CSO of Rapid7 and chief architect of the Metasploit project said he has not had a chance to test whether the update truly patches the gaping hole left by Adobe developers. But he said the approach seemed to make sense. Adobe has said it would not release an update for Reader until October 4.

**The Register:** [Unofficial fix brings temporary relief for critical Adobe vuln](#)

### **SpyEye botnet’s bogus billing feature**

*September 17 – (Banking)*

SpyEye is a software package that promises to make running a botnet a point-and-click exercise. A unique component of SpyEye is a feature called “billinghammer,” which automates the purchase of worthless or copycat software using credit card data stolen from victims of the botnet. The SpyEye author explained this feature in detail on several hacking forums where his kit is sold, even including a video that walks customers through the process of setting it up. Basically, the scam works like this: The botmaster acquires some free-ware utility or legitimate program, renames it, claims it as his own and places it up for sale at one of many pre-selected software sales and distribution platforms, including ClickBank, FastSpring, eSellerate, SetSystems, or Shareit. The botmaster then logs in to his SpyEye control panel, feeds it a list of credit card numbers and corresponding cardholder data, after which SpyEye opens an Internet Explorer Window and — at user-defined intervals — starts auto-filling the proper fields at the botmaster’s online store and making purchases.

**Krebs on Security:** [SpyEye botnet’s bogus billing feature](#)

### **Workaround for ASP.NET server’s encryption vulnerability**

*September 20 – (IT)*

In a security advisory, Microsoft has confirmed a vulnerability in the process used by ASP.NET applications to encrypt cookies and other session information. In the announcement for the security advisory, Microsoft said it was not, so far, aware of any attacks. How-



September 2010

**Cross Site Scripting:** an attack that takes advantage of a Web site vulnerability in which the site displays content that includes un-sanitized user-provided data. For example, an attacker might place a hyperlink with an embedded malicious script into an online discussion forum. That purpose of the malicious script is to attack other forum users who happen to select the hyperlink. For example it could copy user cookies and then send those cookies to the attacker. ([Imperva](#))

ever, the security group encouraged users to “review the advisory for mitigations and workarounds.” A blog entry describes how to implement the workarounds and offers a script to help administrators determine whether their ASP.NET applications are vulnerable. The cause of the problem was highlighted by two security researchers who established that there was an issue with how the ASP.NET framework encrypted data. Usually, this uses the Advanced Encryption Standard (AES) in Cipher Block Chaining mode (CBC), but this mode is vulnerable to what are called Padding Oracle Attacks PDF, which can allow encrypted data, such as cookies, to be decrypted without the key.

**The H Security:** [Workaround for ASP.NET server’s encryption vulnerability](#)

### Twitter hack: Made in Japan?

*September 23 – (IT)*

The recent Twitter attack that caused a widespread headache for the micro-blogging service appears to have been triggered by a Japanese computer hacker who said he was only trying to help. The attack, which emerged and was shut down within hours September 21, involved a **cross-site scripting** flaw that allowed users to run JavaScript programs on other computers. The originator is believed to be someone who uses the name “Masato Kinugawa” in cyberspace and acknowledges creating the Twitter account “RainbowTwtr” that demonstrated the vulnerability. Through his Twitter account and personal blog, Kinugawa regularly tracks down possible computer security loopholes and notifies companies of their existence. Kinugawa said he contacted Twitter about the weakness August 14. “Twitter had not fixed this critical issue long after it had been notified,” Kinugawa tweeted. “Twitter left this vulnerability exposed, and its recognition of this problem was low. Rather than have someone maliciously abuse this under the radar, I decided it would be better to urgently expose this as a serious problem and have it be addressed.”

**Associated Press:** [Twitter hack: Made in Japan?](#)

### Uber-zombie cookies give us the fear

*September 23 – (IT)*

So-called invulnerable evercookies use eight different techniques and locations to hide on tagged systems, including Web history, HTML5 session storage and even the “RGB values of auto-generated, force-cached PNGs using HTML5 Canvas tag to read pixels (cookies) back out” as well as in flash or regular cookies. Providing just one copy of the cookie remains, the other locations are rebuilt. A developer explains the point of his idea:

“Evercookie is designed to make persistent data just that, persistent. By storing the same data in several locations that a client can access, if any of the data is ever lost (for example, by clearing cookies), the data can be recovered and then reset and reused. Simply think of it as cookies that just won’t go away.” The developer reckons using Private Browsing in Safari will stop all evercookie methods following a browser restart. He has not tested whether this approach work with other browsers.

**The Register:** [Uber-zombie cookies give us the fear](#)

### Other Threats and Vulnerabilities articles:

- *September 1 – (All Sectors) ZDNet:* [Malware hosted on Google Code project site](#). Malicious hackers are using the Google Code repository to host Trojans horses, backdoors and password stealing keyloggers, according to researchers at Zscaler.



September 2010

- *September 6 – (IT) **Sophos: [TechCrunch Europe serves up malware attack](#)***. The European Website of TechCrunch (eu.techcrunch.com), one of the world’s most popular blogs, appears to have fallen victim to hackers, who have planted a malicious script on their site, designed to infect unsuspecting visitors.
- *September 6 – (IT) **The H Security: [Flash Player as a spy system](#)***. If a forged certificate is accepted when accessing the Flash Player’s Settings Manager, which is available exclusively online, attackers can potentially manipulate the player’s Website privacy settings. This allows a Web page to access a computer’s Web cams and microphones and remotely turn the computer into a covert listening device or surveillance camera.
- *September 9 – (IT) **Help Net Security: [Android SMS Trojan delivered via SEO techniques](#)***. During the course of researching the origin for the first SMS Trojan for Android devices, Help Net Security found a new Android package masquerading as a porn media player, but which instead sends SMS messages to premium rate numbers.
- *September 9 – (IT) **Help Net Security: [Multiple vulnerabilities in Cisco Wireless LAN Controllers](#)***. The Cisco WLC family of devices has been found to be affected by two denial of service vulnerabilities, three privilege escalation vulnerabilities, and two access control list bypass vulnerabilities.
- *September 9 – (Communications; IT) **Computerworld: [Mass injections and malware infections at Media Temple](#)***. Since at least the spring of 2010, a swarm of infections have been found in Media Temple Web hosted sites. Google Safe Browsing diagnostics states that of the 66,060 Media Temple sites tested in the last 90 days, 12,423 had malicious content.
- *September 14 – (All Sectors) **Help Net Security: [Global botnet offering DDoS services](#)***. Damballa discovered a botnet that offers pay-for-delivery DDoS attacks. The IMDDOS botnet, named after the commercial name on the botnet Web site, has grown to one of the largest active global botnets in less than 4 months from initial testing. The IMDDOS botnet offers a commercial service for delivering DDoS attacks against any desired target.
- *September 18 – (Communications; IT) **Softpedia: [Sites hosted at Go Daddy hit by mass injection attack again](#)***. Researchers from Sucuri Security, a company running a Web integrity monitoring service, warn that a number of Web sites hosted at Go Daddy have had malicious code injected into their pages. All infected sites had base64-encoded JavaScript added to all of their PHP files.

### Policy, Legislation and Governance

#### Microsoft gets legal approval to acquire former Waledac domains.

*September 8 – (Communications, IT)*

A federal judge recommended that Microsoft be allowed to acquire the 276 Internet domains that formerly drove the Waledac botnet, which plagued users and enterprises for more than 1 year. According to a USA Today report, the U.S. District Court of Eastern Virginia has granted a motion that, in effect, gives Microsoft permanent ownership of the Web domains once used by the Waledac cybergang to send instructions to hundreds of thousands of “bot” PCs. The idea is to put the botnet permanently out of business by taking its component parts out of the cybercriminals’ hands, Microsoft said in a blog. “Our legal action to permanently shut down the botnet has been successful, and we have begun working with Internet service providers and CERTs to help customers remove the Waledac infection from their computers.” The number of unique IP addresses infected by Waledac, which was taken

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



September 2010

down earlier this year, is steadily declining. “As of August 30th, there were just more than 58,000 unique IP addresses infected with Waledac malware,” the company said. “That’s down from nearly 64,000 addresses during the week of July 23rd.”

**DarkReading:** [Microsoft gets legal approval to acquire former Waledac domains](#)

### **NSA product accreditations lag behind IT security advances**

*September 15 – (IT)*

The National Security Agency (NSA) held its first conference related to its views on trusted computing the week of September 13. The NSA Trusted Computing Conference and Exposition in Orlando, Florida drew about 500 attendees and 39 exhibiting companies. The NSA chief of the network solutions office noted in his keynote that since May of this year, the national-security strategy has been “COTS [commercial off the shelf] first, not GOTS [government].” The chief of network solutions said the NSA wants to influence how commercial technologies are developed, and hopes “richer collaboration could further harden national-security systems” and give commercial systems some “government-like security.”

**Network World:** [NSA product accreditations lag behind IT security advances](#)

### **IETF approves e-crime reporting format**

*September 20 – (Banking; IT)*

An Internet standards group has approved an electronic crimes reporting format, which may eventually give security researchers a cohesive, broad set of data to gauge online crime. The Internet Engineering Task Force (IETF) approved a customized version of the XML-based Instant Object Description Exchange Format (IODEF). Extensions have been added that are appropriate for creating standard e-crime reports. The format allows for unambiguous time stamps, support for different languages and a feature to attach samples of malicious code. It solves the problem of inconsistent reports, which make it harder to spot trends and react faster. The goal is for groups hit by Internet crime, such as banks, to be able to mine a centralized databases. If a bank is experiencing an attack, it could query the database to find out ranges of IP (Internet Protocol) addresses that have been used for offenses such as phishing attacks. Further queries could determine if other banks have been hit by attacks and analyze spam messages to see if there are common patterns in the grammar, or if the attacks originate from a certain area. All of the information could then be used to contact ISPs to take steps to stop the abuse. The Anti-Phishing Working Group, which has been instrumental in developing the reporting format, plans to run a trial to see how organizations can share the data in the format.

**IDG News Service:** [IETF approves e-crime reporting format](#)

### **The soft underbelly of combat networks**

*September 21 – (Government)*

The steps to defend military networks are often the same as those needed to protect systems at other federal government agencies and commercial enterprises, said the chief information security officer at Unisys. The official, whose information security career began three decades ago in the Air Force and continued as CISO at the Transportation Security Administration before she moved to Unisys, said DOD and many government organizations have network-level security pinned down fairly well. The application level is where most breaches, data thefts and other vulnerabilities lurk, she said. The federal government has become “really good at the perimeter security. I think the area that needs to be more focused in on is

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



September 2010

secure code and application development,” she said. Network perimeter security has improved with better firewalls and encryption. But the trend toward cloud computing poses potential problems that might negate advances. She said many organizations’ perimeters are becoming cloudy with the increase of wireless devices and applications.

**Defense Systems:** [The soft underbelly of combat networks](#)

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

- *September 2* – (Government) ***The New New Internet:*** [Bids open for new cyber-insider threat program](#). The week of August 30, the Defense Advanced Research Projects Agency opened bids for a new Cyber Insider Threat program. The CINDER program arises from the military being targeted by a number of high-profile security breaches over the past few years.
- *September 3* – (Energy) ***Government Computer News:*** [NIST guidelines tackle the security issues that accompany smart grid](#). A final set of guidelines for a smart-grid security architecture has been released by the National Institute of Standards and Technology, outlining how security requirements will be incorporated into the design of the nation’s next-generation power distribution system.
- *September 7* – (Government) ***Computerworld:*** [Ohio bans offshoring as it gives tax relief to outsourcing firm](#). Ohio’s governor is delivering one of the strongest attacks yet on offshore outsourcing, calling it not only a threat to jobs but an IT security risk. The governor’s criticism of offshore outsourcing was part of a recent order to state agencies prohibiting them from hiring any firm that sends work offshore.
- *September 9* – (Communications) ***Government Computer News:*** [A new domain signs on with DNSSEC](#). The .info top-level domain, the Internet’s seventh largest TLD with more than 6.5 million registered domains within it, was digitally signed September 1 to enable use of the DNS Security Extensions. The delegation signer records have been published in the DNS Root to enable validation of signatures on Domain Name Service query responses.
- *September 20* – (Government) ***Government Computer News:*** [Agencies slowly making progress on continuous monitoring](#). Continuous monitoring for vulnerabilities and configuration errors in IT systems is an accepted best practice. The good news is that more than half — 57 percent — of the respondents said they are monitoring networks continuously for vulnerabilities, and another 13 percent are scanning at least weekly. But only 39 percent are doing continuous scans for compliance with configuration requirements such as the Federal Desktop Core Configuration.
- *September 28* – (Energy) ***Homeland Security Newswire:*** [DOE awards \\$30 million to bolster smart grid cybersecurity](#). Speaking at the first GridWise Global Forum, the U.S. Energy Secretary recently announced the investment of more than \$30 million for 10 projects that will address cybersecurity issues facing the U.S. electric grid.

### **Reports and Publications**

**SC Magazine UK:** [SQL injections dominated malware in 2010, as Gumblar botnet named as ‘the most significant malware development in years’](#). The number of IPS SQL injections increased substantially in the second quarter of 2010 following a downturn. Cisco’s global [threat report](#) for the second quarter revealed IPS SQL injection signature firings increased substantially in the period to coincide with outbreaks of SQL injection-compromised Web sites. It also claimed Asprox SQL injection attacks made a reappearance

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



September 2010

in June of 2010, after nearly 6 months of inactivity.

**Next Gov: [CBP failed to follow basic security practices to protect financial systems.](#)**

The Customs and Border Patrol (CBP) failed to properly set computer controls that allow only authorized users to view financial data, and to certify networks complied with security standards, according to an [audit](#) released September 1 by the Homeland Security Department's inspector general. A number of problems the inspector general found in 2008 still were not fixed in fiscal 2009, according to the audit, which analyzed CBP's financial systems and was conducted by the accounting firm KPMG.

**Help Net Security: [Every week 57,000 fake Web addresses try to infect users.](#)** Every week, hackers are creating 57,000 new Web addresses which they position and index on leading search engines in the hope that unwary users will click them by mistake. eBay, Western Union and Visa top the rankings of the most frequently used keywords; followed by Amazon, Bank of America, Paypal and the United States internal revenue service. These are the conclusions of a study carried out by PandaLabs, which has monitored and analyzed the major [blackhat SEO](#) attacks of the last 3 months.

**TrendLab Malware Blog: [Cybercriminals hone in on critical systems.](#)** In the 2010 threat forecast, "[The Future of Threats and Threat Technologies](#)," Trend Micro researchers mentioned that new attack vectors will arise for virtual/cloud environments. To add to this, critical infrastructures such as a SCADA network will become another serious potential target for cybercriminals.

**Federal Computer Week: [DHS audit finds serious vulnerabilities in US-CERT security.](#)** A scan of IT systems at US-CERT, the Homeland Security Department's primary operational cybersecurity agency, found hundreds of vulnerabilities that could allow someone to compromise data, according to a recent inspector general's [report](#). Although DHS has policies in place to mitigate and correct problems, the lack of an automated system for patching vulnerabilities has left a large number of unpatched and possibly serious flaws in the agency's mission operating environment, the IG found.

**Washington Technology: [Federal Acquisition Regulation needs to toughen safeguards against unauthorized disclosure of sensitive information.](#)** Three major federal departments that work closely with sensitive information lack strong safeguards to protect that information, which contractors are accessing while working, according to a report released September 10. The Defense, Homeland Security, and Health and Human Services departments have supplemented the Federal Acquisition Regulation (FAR) with provisions to protect information. However, the additional provisions in DOD's and HHS' rules don't go far enough to protect sensitive data, according to the [Government Accountability Office](#).

**Help Net Security: [80% of network attacks target Web-based systems.](#)** A new [report](#) by HP TippingPoint DVLabs, SANS Institute and Qualys Research Labs, provides data and analysis — including real-world examples of attacks and recommended ways to mitigate risk — to fully inform companies about the latest security threats. It includes updated vulnerability trends, an in-depth analysis of a PDF-based exploit, discussion of client versus server side attacks, and information on growing tendencies, including botnets and malicious



September 2010

JavaScript.

**DarkReading:** [Number of malware-infected Websites tops 1 million mark](#). According to a new [report](#) published in a blog September 15 by researchers at security firm Dasient, the number of Web sites infected by malware in the second quarter of 2010 spiked to more than 1.3 million — the first time that figure has ever topped 1 million. “That’s a jump of almost two times the number that we saw in the previous quarter,” said Dasient’s co-founder.

**Information Week:** [Consolidating federal data centers could take 10 years](#). The federal government’s plan to consolidate data centers as a cost-saving, security, and efficiency measure could take as long as 10 years to complete, according to a new [report](#). A report from government analysis firm INPUT that assessed progress on the Federal Data Center Consolidation (FDCC) initiative also found that there are some significant challenges to achieving the plan.

**SC Magazine UK:** [Symantec warns of a new virus threat, as remote workers most likely to breach rules](#). With Stuxnet and the “Here you have” worm both highlighting the threat of a virus, there has been a further detection of what has been called the Sality.AE virus. According to Symantec’s [September 2010 MessageLabs Intelligence Report](#), the Sality.AE virus was the most prevalent blocked piece of malware in the month.

**V3.co.uk:** [Software vulnerabilities reaching ‘unacceptable’ levels](#). Developers are failing to meet industry security standards when creating new software, according to testing firm [Veracode](#). Data collected on 2,900 applications by the company’s security verification service suggests that more than half of tested applications contain “unacceptable” levels of vulnerabilities. More than 80 percent of submitted Web applications contained errors listed in the [Open Web Application Security Project’s](#) Top 10 risk list.

**Help Net Security:** [Breakdown of security weaknesses by industry and organization size](#). WhiteHat Security released the tenth installment of its [Security Website Security Statistics Report](#), providing a first-time breakdown of the state of Web site security by industry and company size. Compiled using data from more than 2,000 production Web sites across 350 organizations, this latest issue shines a spotlight on the need for organizations to focus on improving responsiveness in remediating vulnerabilities in order to reduce risk and improve the effectiveness of the systems development life cycle over time.

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](#).*

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