



August 2010

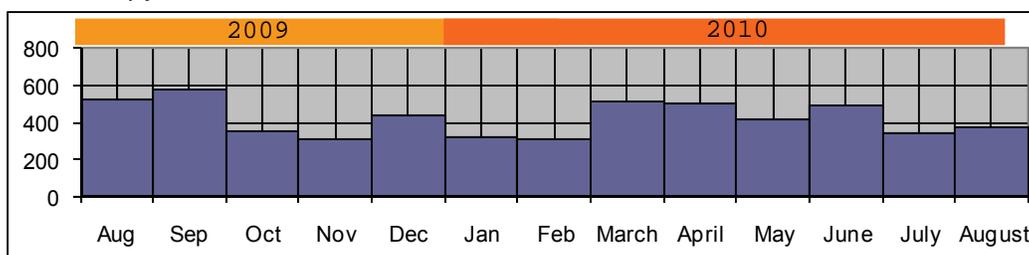
IN THIS REPORT

- 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

[SC Magazine](#) reported that a new family of bots, dubbed “YovoDDoS,” is responsible for nearly 200 distributed denial-of-service attacks targeting Web sites in China, the United States, South Korea and Germany, according to researchers at security firm Arbor Networks. Meanwhile, [Network World](#) reported Smartphones with malware could pose a significant military threat by sending location data to the enemy using mechanisms similar to those in recently discovered Android malware. Virginia’s IT operations arm has repaired the cause of a statewide IT system failure that affected online services and network operations of more than 20 of its agencies, including the Department of Motor Vehicles according to [Information Week](#). Finally, the [Associated Press](#) reported the United States for the first time is publicly warning about the Chinese military’s use of civilian computer experts in clandestine cyber attacks aimed at American companies and government agencies. In a move that is being seen as a pointed signal to Beijing, the Pentagon laid out its concerns in a carefully worded report explaining that the People’s Liberation Army is using “information warfare units” to develop viruses to attack enemy computer systems and networks. In other news:

- The [Washington Post](#) reported the most significant breach of U.S. military computers was caused by a flash drive inserted into a U.S. military laptop on a post in the Middle East in 2008. The Deputy Defense Secretary said malicious code placed on the drive by a foreign intelligence agency uploaded itself onto a network run by the U.S. military’s Central Command.
- The [New York Times](#) reported that A United States Navy drone, suffering a software problem, wandered into restricted airspace August 2 around Washington D.C. before operators could stop it.



August 2010

Special Coverage

On August 19, A critical flaw was discovered that one of [40 different Windows applications](#) could be used to hijack a computer or as an avenue to infect it with malware. The chief security officer at Rapid7 discovered the flaw while “researching the Windows shortcut vulnerability [.lnk vulnerability], a critical bug that Microsoft acknowledged in July and patched on August 2.” The affected programs will have to be patched individually.

It was later announced that the problem was much larger than originally assumed. The CEO of application security for Acros Security reported that about [200 Windows applications](#) were vulnerable to the flaw. He reiterated that each application would have to be individually patched. Acros warned Microsoft of the vulnerability in April. On August 23, a [Ph. D candidate](#) at the University of California, Davis, presented a paper that showed he informed Microsoft in “February that dozens of Windows applications, including many of its own, harbor bugs that hackers can exploit to seize control of computers. At least four of the bugs can be exploited remotely.” The security chief, the CEO, and Ph. D. candidate all agree the flaw can be used by “hackers who trick users into visiting malicious Web sites because of the way the software loads code libraries — dubbed ‘dynamic-link library,’ “ or files that have the .DLL extension for short. The Ph.D.’s [paper](#) claimed there were 28 programs that combined, contained 1,700 separate bugs that could be exploited by hackers.

[Microsoft](#) responded to the reports of the flaw August 23 by creating and publishing a tool in order to block the exploit, but declined to verify if any of its own applications were susceptible. Shortly before the announcement by Microsoft, the exploit code for the DLL vulnerability appeared on the Web site Metasploit. The [code](#) was released by the same chief security officer at Rapid7 who reported the issue August 19. The security officer also released an auditing tool that creates a record of applications that are vulnerable. On August 24, The Register reported that exploits for as many as [200 applications](#) including the Firefox browser, uTorrent BitTorrent client, and Microsoft Powerpoint, had been created and the attack code was posted to [Exploit Database](#). A similar vulnerability existed in Apple’s iTunes software for Windows, but was patched roughly 4 months before.

Cyber Attacks

Botnet conducts “Brute Force” attacks

August 13 – (IT)

A server-based botnet which attacks unsecure websites is currently launching a flood of attacks over the Internet, according to security researchers. The attacks are attempting to hack secure shells protecting Linux boxes, routers and other network devices by guessing the login credentials. The botnet hits websites which run an outdated version of phpMyAdmin, according to researchers. The vulnerability, which was patched back in April, is exploited by the botnet which installs a file which searches the Internet for devices using the SSH protocol for protection. “This bot then conducts brute force SSH attacks on random IP addresses specified by the bot herder,” one user wrote. A monitoring service run by the SANS Institute a six-times increase in sources participating in SSH scans in the past few weeks.

The New New Internet: [Botnet conducts “Brute Force” attacks](#)

DDoS botnet family discovered targeting scores of sites

August 24 – (IT)

A new family of bots is responsible for nearly 200 distributed denial-of-service attacks tar-

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



August 2010

getting Web sites in China, the United States, South Korea and Germany, according to researchers at security firm Arbor Networks. The bot family, which has been dubbed “YoyoDDoS” after the hostname of one of its initial command-and-control (C&C) servers, was first detected in March. To date, Arbor Networks has processed more than 70 variants from the family and identified at least 34 C&C servers, all but three located in China. Out of the 180 YoyoDDoS attacks that have been identified, 126 of them targeted IP addresses in China, while 32 targeted victims in the United States, 9 in South Korea, and 5 in Germany. Many online merchants have been targeted, including sites selling auto parts and cosmetics, a researcher said. Several gaming and gambling sites also were attacked, along with a Web site-hosting provider, a music forum and a personal blog. The attacks typically last from a few hours to 2 days, he added. Several sites have been attacked continuously for 24 to 48 hours.

SC Magazine: [DDoS botnet family discovered targeting scores of sites](#)

Other Cyber Attacks articles:

- *July 29* – (Health) **Bakersfield Californian:** [Kern Medical Center battling virus](#). Kern Medical Center (KMC) in Bakersfield, California, was hit by a computer virus that sent KMC operations back to the paper age for most of July 27 until the morning of July 29. Staff had to use paper and pen while billing systems, mobile device access, and administrative servers were offline.
- *August 9* – (IT/Communications) **The Register:** [DNS made easy rallies after punishing DDoS attack](#). DNS Made Easy has restored services following a vicious denial of service that peaked at 50Gbps August 7. The identity of the perpetrators and their motives remain unclear.
- *August 16* – (Gov Fac) **KOB 4 Albuquerque:** [Virus infects Sec. of State’s computer](#). Questions are being raised after some New Mexico state employees, including the office manager said they saw computer viruses display pornographic icons on the New Mexico secretary of state’s laptop computer. Answers have been hard to come by because the former IT director has left the country and both the deputy and the secretary herself insist the virus was not pornographic.
- *August 17* – (IT) **The Register:** [Apple.com hit in latest mass hack attack](#). A hack attack that can expose users to malware exploits has infected more than 1 million Web pages, at least two of which belong to Apple. The SQL injection attacks bombard the Web sites of legitimate companies with database commands that attempt to add hidden links that lead to malware exploits.
- *August 19* – (IT) **The New New Internet:** [Botnet conducts “Brute Force” attacks](#). A server-based botnet which attacks unsecure Web sites is launching a flood of attacks over the Internet, according to security researchers. The attacks are attempting to hack secure shells protecting Linux boxes, routers and other network devices by guessing the log-in credentials.

Data Breach/Information Gathering

Botnet with 60GB of stolen data cracked wide open

August 2 – (IT)

Researchers have cracked open a botnet that amassed more than 60GB of passwords and other stolen data, even as it cloaked itself using a state-of-the-art technique known as fast flux. When its command-and-control server was infiltrated, the Mumba botnet had snagged

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



August 2010

more than 55,000 PCs, according to the researchers from anti-virus provider AVG. The data-stealing operation is the work of the notorious Avalanche Group, a criminal operation that was responsible for two-thirds of all phishing attacks in the second half of 2009, according to a report earlier in 2009 from the Anti-Phishing Working Group. “These criminals are some of the most sophisticated on the Internet, and have perfected a mass-production system for deploying phishing sites and ‘crimeware,’” AVG wrote in a report issued August 2. “This means that mitigating the threat by going after the servers hosting the data using the ‘Mumba’ botnet is now much harder than before.” The botnet appears to have been spawned with an initial malware campaign that was launched in April. Its first week saw more than 35,000 infections. Several smaller campaigns were responsible for the remainder of the botnet’s 55,000 victims. The malware uses at least four variants of the latest Zeus crimeware kit, which allows well-financed criminals to deploy highly sophisticated botnets in a hurry. The stolen data includes log-in credentials for online bank, retail, and e-mail accounts, and social-networking sites.

The Register: [Botnet with 60GB of stolen data cracked wide open](#)

Six Florida colleges victims of widespread data breach

August 11 – (Gov Fac)

Six colleges in Florida had their students’ and employees’ personal data exposed and, in some cases, accessed and posted online by outsiders when a library-services firm serving the colleges inadvertently left the information in its database exposed for 5 days. Students, faculty, and employees at Broward College, Florida State College at Jacksonville, Northwest Florida State College, Pensacola State College, South Florida Community College, and Tallahassee Community College all are at risk of exposed personal data, according to The College Center for Library Automation (CCLA), which provides automated library services and electronic resources to Florida public colleges. As many as 126,000 individuals’ Social Security numbers and other personal data were accessed online by unauthorized people after a software upgrade at the organization resulted in the database being left exposed. The breach reportedly was discovered after a student found his own SSN via a Google search in late June. Although the CCLA did not specify how the data was there, it appears that whoever accessed it was likely posting it in an effort to sell or abuse it, security experts said.

DarkReading: [Six Florida colleges victims of widespread data breach](#)

Defense official discloses cyberattack

August 24 – (Gov Fac)

Now it is official: The most significant breach of U.S. military computers was caused by a flash drive inserted into a U.S. military laptop on a post in the Middle East in 2008. In an article to be published August 25 in Foreign Affairs discussing the Pentagon’s cyberstrategy, the Deputy Defense Secretary said malicious code placed on the drive by a foreign intelligence agency uploaded itself onto a network run by the U.S. military’s Central Command. “That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control,” he said in the article. “It was a network administrator’s worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary.” The Deputy Defense Secretary’s decision to declassify an incident that Defense officials had kept secret reflects the Pentagon’s desire to raise congressional and public concern over the threats facing U.S. computer systems, experts said.

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



August 2010

Washington Post: [Defense official discloses cyberattack](#)

Crime or espionage?

August 28 – (Gov Fac)

Recently, there have been a series of attacks using Zeus malware that appear to be less motivated by bank fraud and more focused on acquiring data from compromised computers. The themes in the e-mails — often sent out to .mil and .gov e-mail addresses — focus on intelligence and government issues. After the user receives such an e-mail, and downloads a file in the e-mail, his or her computer will likely (due to the low AV coverage) become compromised by Zeus malware and will begin communicating with a command and control server. It will then download an additional piece of malware, an “infostealer,” which will begin uploading documents from the compromised computer to a drop zone under the control of the attackers. What appears to be a one-off attack using Zeus, the author believes, is actually another round of a series of Zeus attacks. These attacks appear to be aimed at those interested in intelligence issues and those in the government and military, although the targeting appears to be general rather than targeted. Details of such an attack were recently posted on contagiodump.blogspot.com. The e-mail used in the attack appeared to be from “ifc@ifc.nato.int” with the subject “Intelligence Fusion Centre” and contained links to a report [EuropeanUnion_MilitaryOperations_EN.pdf](#) that exploits CVE-2010-1240 in order to drop a Zeus binary.

Information Warfare Monitor: [Crime or espionage?](#)

Other Data Breach/Information Gathering articles:

- *July 29 – (Health) Philadelphia Inquirer:* [Computer with patient data stolen from Jefferson](#). A laptop computer with health and personal information on 21,000 patients was stolen from an office at Thomas Jefferson University Hospital in Philadelphia in June and the patients whose information was on the laptop were notified July 23.
- *August 2 – (Banking) Krebs on Security:* [Texas firm blames bank for \\$50,000 cyber heist](#). A business telephone equipment company in Texas is trying to force its bank into a settlement over an attack by organized cyber thieves in 2009 that cost the company \$50,000.
- *August 5 – (Banking) IDG News Service:* [Hackers find a new target in payroll processing](#). Criminals hacked into a desktop computer belonging to Regeneron Pharmaceuticals and tried to steal money by redirecting funds using Regeneron’s account on a third-party payroll system, operated by Ceridian. The attack did not work, but it shows that criminals, who have been making millions by hacking into computers and initiating fraudulent bank transfers, may have found a new target.
- *August 6 – (IT) IDG News Service:* [Zeus malware used pilfered digital certificate](#). Researchers at Trend Micro have found that a widespread piece of malware used a digital certificate from a competing security company’s product in an attempt to look legitimate. The version of Zeus detected by Trend Micro had a digital certificate belonging to Kaspersky’s Zbot product, which is designed to remove Zeus. The certificate — which is verified during a software installation to ensure a program is what it purports to be — was expired, however.
- *August 11 – (Banking) The Register:* [Zeus botnet raid on UK bank accounts under the spotlight](#). More details have emerged of how security researchers tracked down a Zeus-based botnet that raided more than \$1 million from 3,000 compromised U.K. online

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



August 2010

- banking accounts. The vice president of technical strategy for M86 Security said hackers began the assault by loading compromised third-party sites with a battery of exploits designed to infect visiting PCs with variants of the Zeus banking Trojan.
- *August 15* – (Health) **InformationWeek**: [Analysis: Healthcare breach costs may reach \\$800 million](#). According to an analysis by the Health Information Trust Alliance (HITRUST), regulated health care organizations that have reported health information breaches of 500 or more people could cumulatively spend upwards of \$1 billion in related costs.
 - *August 17* – (All Sectors) **Softpedia**: [Disney, Warner Bros and others sued for spying on Internet users](#). A complaint filed recently in California alleges that several companies including Disney, Warner Bros. Records, Ustream and others have installed illegal codes on millions of computers with the purpose of tracking online activity. At the center of the suit, which seeks class action status, are the so-called Flash cookies.
 - *August 18* – (IT) **The Register**: [Facebook login page still leaks sensitive info](#). Facebook’s log-in system continues to spill information that can be helpful to phishers, social engineers and other miscreants attempting to scam the more than 500 million active users of the social networking site. A difference in wording makes it possible for anyone to discern whether a given e-mail address is registered on Facebook, even when the corresponding password is unknown. The flaw was flagged by a Register reader who is a security analyst for EMC Corporation’s Critical Incident Response Center who calls it “one of the oldest security malpractices in the book.”
 - *August 20* – (Health) **Associated Press**: [Laptop with patient info stolen](#). Authorities said a laptop computer with personal information on 7,000 Cook County, Illinois health system patients has been stolen. A Cook County Health and Hospital System spokesman said the computer was stolen June 1, but its theft was not disclosed until August 20, after the completion of an internal investigation.
 - *August 23* – (Banking) **Associated Press**: [Judge approves Countrywide ID theft settlement](#). A federal judge August 23 granted final approval to a settlement between Countrywide Financial Corp. and millions of customers left at high risk for identity theft because of a security breach. Countrywide, now owned by Bank of America, will provide free credit monitoring for up to 17 million people whose financial information was exposed, according to the settlement.

Threats and Vulnerabilities

Defense agencies should provide ways for industry to fix security issues

August 2 – (Gov Fac/IT)

The federal government has the right to refuse technology components that could introduce cybersecurity risks into the Defense Department’s classified systems, but it should provide manufacturers the opportunity to fix the vulnerabilities to ensure they do not affect commercial and other federal networks, said a security expert. TechAmerica, a technology lobbying group in Washington D.C.; the Professional Services Council, a trade association; and other industry organizations called for Congress to drop Section 815(c) from the 2011 Senate Defense authorization bill, which would authorize Defense agency heads to exclude from procurements specific companies “to avoid unacceptable supply-chain risk.” The provision, which would apply only to the acquisition of classified national security systems, defines supply-chain risk as the potential for adversaries to gain access to and attack the system. The decision to exclude a company would be at the sole discretion of an agency head or a senior

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



August 2010

procurement executive, and would not be subject to review in a bid protest before the Government Accountability Office or in any federal court. But determining a company's trustworthiness is difficult because so much technology development occurs overseas, which is harder to oversee and track, said the chairman and chief executive officer of security software company NetWitness, and former director of the Homeland Security Department's National Cybersecurity Division. Defense agencies, however, should have the right to refuse a technology component that could pose a risk to classified systems, if they also provide industry with enough information to mitigate those risks, he said.

NextGov: [Defense agencies should provide ways for industry to fix security issues](#)

DHS quietly dispatching teams to test power plant cybersecurity

August 4 – (Energy)

DHS is quietly creating specialized teams of experts to test industrial control systems at U.S. power plants for cybersecurity weaknesses. An August 4 Associate Press report indicated DHS has so far created four teams to conduct such assessments, according to the director of control system security. The official told the news service that 10 teams are expected to be in the field next year as the program's annual budget grows from \$10 million to \$15 million. A DHS spokeswoman confirmed the DHS plan. She said the special teams are part of an Industrial Control Systems Computer Emergency Response Team (ICS CERT) that DHS has been building over the past year in response to worldwide cybersecurity threats against industry control systems (ICS). The teams are being set up to help companies in critical infrastructure industries respond to and mitigate cyber incidents affecting ICS, she said. Each DHS team is said to be equipped with forensic tools, cables, converters and data-storage equipment to be used to probe for and fix security vulnerabilities in control systems. According to the report, the specialized DHS teams conducted 50 security assessments at power plants in the past year. In addition, teams were dispatched 13 times to investigate cyber incidents — nine were found to be cyber intrusions and four were caused by operator error.

Computerworld: [DHS quietly dispatching teams to test power plant cybersecurity](#)

Hacked Smartphones pose military threat

August 16 – (IT/DIB/Gov Fac)

Smartphones with malware could pose a significant military threat. Hacked smartphones could endanger troops by sending location data to the enemy using mechanisms similar to those employed by recently discovered Android malware, experts said. Malicious software that commandeers phone functions could give wartime enemies valuable information about troop locations and movements, according to a software security professor at Columbia University and conference chairman for the RSA Conference, and an analyst who works on the PayPal online security and malware strategy team.”

Network World: [Hacked smartphones pose military threat](#)

See also; **Computer Weekly:** [Android phones hit by text-based Trojan](#)

Trojan-ridden warning system implicated in Spanair crash

August 20 – (Trans)

Malware may have been a contributory cause of a fatal Spanair crash that killed 154 people 2 years ago. Spanair flight number JK 5022 crashed with 172 on board moments after taking off from Madrid's Barajas Airport on a scheduled flight to Las Palmas, Spain August 20,



August 2010

2008. Just 18 survived the crash and subsequent fire aboard the McDonnell Douglas MD-82 aircraft. The airline's central computer, which registered technical problems on planes, was infected by Trojans at the time of the fatal crash and this resulted in a failure to raise an alarm over multiple problems, according to Spanish daily El Pais. The plane took off with flaps and slats retracted, something that should in any case have been picked up by the pilots during pre-flight checks or triggered an internal warning on the plane. Neither happened, with tragic consequences, according to a report by independent crash investigators. The accident on take-off happened after pilots had abandoned an earlier take-off attempt, and a day after two other reported problems on board. If the airlines' central computer was working properly, a take-off after three warnings would not have been allowed, thereby averting the tragedy. A mechanic who checked the plane before take-off, and an airport maintenance chief, are under investigation and face possible manslaughter charges. An investigating judge has ordered Spanair to supply data on the state of its systems at the time of the crash. An investigation commission is due to report on the case by December.

The Register: [Trojan-ridden warning system implicated in Spanair crash](#)

Navy drone wanders into restricted airspace around Washington

August 25 – (DIB/Gov Fac/Trans)

A United States Navy drone wandered into restricted airspace August 2 around Washington D.C. before operators could stop it. A Navy spokesman could not say August 25 if anyone on the ground was alarmed by the drone — officially an MQ-8B Fire Scout Vertical Takeoff and Landing unmanned aerial vehicle — which looks like a small windowless helicopter, and was flying at 2,000 feet. The Navy said the drone got within 40 miles of Washington before operators were able to re-establish communication. The Navy is calling the problem a “software issue” that foiled the drone's operators.

New York Times: [Navy drone wanders into restricted airspace around Washington](#)

Virginia repairs SAN failure that caused statewide outage

August 27 – (Gov Fac/IT)

Virginia's IT operations arm has repaired the cause of a statewide IT system failure that affected online services and network operations of more than 20 of its agencies, including the Department of Motor Vehicles. The outage happened when an EMC storage area network (SAN) and its redundancy failed the afternoon of August 25, according to the Virginia Information Technologies Agency (VITA). When this occurred, 228 servers attached to the network — which host shared applications and software used statewide — could not access data. By the afternoon of August 27, the SAN had been repaired and technicians were bringing servers back online. Agencies also began testing applications to see if they were working properly again, said a VITA spokeswoman. Virginia's IT system is maintained by VITA, and Northrop Grumman, which signed a \$2.3 billion contract with VITA in 2005 to look after communications and computer services, a move deemed risky, and which has been criticized by state officials.

InformationWeek: [Virginia repairs SAN failure that caused statewide outage](#)

Other Threats and Vulnerabilities articles:

- *August 2 – (All Sectors) InfoWorld:* [Stealing corporate secrets proves to be all too easy](#). Organizers of a contest to highlight the dangers of social engineering said that employees of some of the top U.S. corporations, including BP, Ford, and Coca-Cola, were



August 2010

eager to cough up private data to contestants, exposing a serious lack of investment in user education about the dangers of scams and other human-focused attacks. The contest, held July 30 and 31 at the annual Defcon hacking conference in Las Vegas, was organized by social-engineer.org, a nonprofit.

- *August 5 – (IT) **The Register**: [Virus writer charged with destroying property](#).* Japanese police have arrested a suspected virus writer over allegations he created and distributed an old-school virus that destroyed data. The 27-year-old from Osaka allegedly created the “ika-tako” (squid-octopus) virus. The Japan Times reports that he is believed to be the first person charged with destroying property with a computer virus.
- *August 5 – (IT) **The H Security**: [Cisco security products vulnerable to DoS](#).* Cisco is warning of multiple vulnerabilities in its Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers. The company said that after processing crafted SunRPC or certain TCP packets, the vulnerabilities could cause the FWSM to restart. If an attacker repeatedly exploits the issue, it could result in a sustained Denial-of-Service (DoS) condition.
- *August 6 – (IT) **V3.co.uk**: [Experts uncover flaws in ‘private browsing’](#).* Security experts have warned that many claims about the resilience of ‘secure browsing’ features are overstated, and that private surfing may be anything but. The researchers at Stanford University were due to discuss their findings at the Usenix Security Symposium in Washington. The top four browsers - Internet Explorer, Firefox, Safari and Chrome - suffer from weak security in their secure browsing options, according to the report, and often fail to prevent user history being exposed.
- *August 9 – (Crit Man) **IDG News Service**: [Tire tags reveal driver whereabouts](#).* Researchers from Rutgers University and the University of South Carolina have found that wireless communications between new cars and their tires can be intercepted or even forged. While the potential for misuse may be minimal, this vulnerability points to a troubling lack of rigor with secure software development for new automobiles, said a co-lead on the study.
- *August 10 – (IT) **V3.co.uk**: [Browser hijackers raking in millions](#).* Criminal networks are making gangs millions of pounds a year through browser-hijacker Trojans, which redirect users to sponsored advertising, according to research from security vendor Trend Micro.
- *August 11 – (IT) **SC Magazine UK**: [Vulnerabilities in the Palm Pre and Android smartphones detailed that can see credentials stolen and conversations intercepted](#).* Major vulnerabilities in the Palm Pre and Android smartphones have been detected that could allow data to be stolen. Research by MWR Labs has revealed a major flaw in the Palm Pre that would allow conversations to be intercepted, while a flaw in the Android operating system from 2.0 onwards exists in the browser and allows log-in credentials and cookies to be harvested.
- *August 11 – (IT) **SC Magazine UK**: [80 million websites could be compromised due to a flaw in Adobe ColdFusion](#).* As many as 80 million Web sites could easily be compromised due to a flaw in Adobe’s ColdFusion programming language. Users of Adobe’s ColdFusion programming language are at risk of losing control of applications and Web sites, according to penetration-testing company ProCheckUp.
- *August 12 – (Trans/Gov Fac) **Associated Press**: [FAA computers still vulnerable to cyberattack](#).* Federal Aviation Administration computer systems remain vulnerable to

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



August 2010

- cyber attacks despite improvements at a number of key radar facilities in the past year, according to a new government review.
- *August 13 – (IT) **The Register:** [Rise in Latvian botnets prompts Spamhaus row](#).* Over the previous year, Spamhaus’ monitoring staff had measured a steady increase in Latvian spam and DDOS traffic, particularly from a small ISP called Microlines. It is unclear who the offending cybercriminals were, but in common with its normal practice, Spamhaus contacted Microlines’ abuse address to ask them to take down the relevant servers.
 - *August 17 – (IT) **Help Net Security:** [Facebook Hacker: A dangerous tool](#).* Phishing is the weapon of choice for cybercriminals after log-in credentials. However, a new attack tool — Facebook Hacker — has drawn attention to people desiring passwords and usernames that are not theirs. This kit helps wrongdoers steal log-in credentials without the user even having to type anything.
 - *August 17 – (IT) **The Register:** [Network Solutions pulls widget that tainted up to 5M websites](#).* Network Solutions admitted that a software widget designed to help small businesses build Web sites was contaminated with malware. Early reports suggest anywhere from 500,000 to 5 million Web sites have been affected by the tainted code
 - *August 18 – (Banking) **The New New Internet:** [Zeus Trojan spreading through zip files](#).* Researchers with F-Secure have found a new spam set working to disseminate the Zeus malware through infected zip files.
 - *August 27 – (Banking) **SC Magazine:** [Kaspersky Lab warns of advanced instant messenger threat](#).* Warnings have been made about worms spreading via instant messaging (IM) clients. Kaspersky Lab said the new family of worms are multilingual and capable of infecting users via several IM clients simultaneously, including Yahoo! Messenger, Skype, Paltalk Messenger, ICQ, Windows Live Messenger, Google Talk and the XFire client for gamers. It said four variants of IM-Worm.Win32.Zeroll have been detected so far.
 - *August 27 – (Nuclear) **Global Security Newswire:** [Nation’s nuclear power plants prepare for cyber attacks](#).* The threat to digital systems at the country’s nuclear power plants is considerable, but the sector is better prepared to defend against potentially devastating cyber attacks than most other utilities, according to government and industry officials and experts.

Policy, Legislation and Governance

Pentagon takes aim at China cyber threat

August 19 – (All Sectors)

The United States for the first time is publicly warning about the Chinese military’s use of civilian computer experts in clandestine cyber attacks aimed at American companies and government agencies. In a move that is being seen as a pointed signal to Beijing, the Pentagon laid out its concerns in a carefully worded report. The People’s Liberation Army (PLA), the Pentagon said, is using “information warfare units” to develop viruses to attack enemy computer systems and networks, and those units include civilian computer professionals. The assertion shines a light on a quandary that has troubled American authorities for some time: How does the U.S. deal with cyber espionage emanating from China and almost certainly directed by the government — despite the fact that U.S. officials do not have or cannot show proof of those ties? Asked about the civilian hackers, a Defense Department spokesman said the Pentagon is concerned about any potential threat to its computer net-

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



August 2010

works. The Pentagon, said a spokesman will monitor the PLA's buildup of its cyberwarfare capabilities, and "will continue to develop capabilities to counter any potential threat."

Associated Press: [Pentagon takes aim at China cyber threat](#)

Other Policy, Legislation and Governance articles:

- *August 2* – (Gov Fac) **Defense Systems:** [Army moves closer to private cloud with release of RFP](#). The U.S. Army took another step toward its goal of a private, cloud computing environment with the July 15 release of a request for proposals. The move is part of the department's plans to consolidate data centers from 200 to less than 20.
- *August 11* – (Comms) **Executive Gov:** [FCC seeks public comment on creation of cybersecurity plan](#). The Federal Communications Commission released a notice earlier the week of August 9 requesting public comment on the creation of an anticipated FCC plan that looks to address cybersecurity. The plan, the Cybersecurity Roadmap, seeks to identify vulnerabilities to core Internet protocols and develop solutions in response to cyber threats and attacks.
- *August 12* – (Banking) **Bank Info Security:** [PCI Updates Unveiled](#). The long-anticipated new version of the Payment Card Industry Data Security Standard includes no new requirements — just clarifications and new guidance on existing components.
- *August 12* – (Gov Fac) **Federal Computer Week:** [VA data breach reports available online](#). The Veterans Affairs Department has begun publishing monthly online accounts of its data breaches and lost BlackBerry handheld devices and laptop computers as part of its open government program.
- *August 13* – (DIB) **The Atlantic:** [Pentagon wants to secure dot-com domains of contractors](#). To better secure unclassified information stored in the computer networks of government contractors, the Defense Department is asking whether the National Security Agency should begin to monitor select corporate dot.com domains, several officials and consultants briefed on the matter said.
- *August 19* – (Health) **Computerworld:** [Panel drafts privacy recommendations for health data exchanges](#). A "tiger team" that advises the federally chartered Health IT Policy Committee will submit a list of recommendations August 19 for ensuring the privacy and security of personally identifiable health information in Health Data Exchanges. The recommendations were developed in response to a specific set of privacy-related questions raised by the Office of the National Coordinator for Health Information Technology.
- *August 20* – (Gov Fac) **Federal Computer Week:** [National Guard Bureau tells what not to write on Facebook](#). The National Guard Bureau is giving guard members specific guidance on how to control their privacy settings on Facebook, and what to avoid publishing on social media sites. The guidance advises guard members to use "friends only" privacy settings on social networking sites. It also warns that members' social network "friends" and "followers" could be factors in background investigations when the members apply for security clearances.
- *August 23* – (Gov Fac) **Government Technology:** [IT security incidents prompt Nashville, Tenn., to strengthen policy, hire IT security chief](#). When more than 320,000 Nashville voters' personal information was breached in late 2007, it was a turning point that propelled the incorporated Metropolitan Government (Metro) of Nashville and Davidson County to assess and define IT security policy. A comprehensive security pol-

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



August 2010

icy is set to go into effect this fall, and the Metro technology chief is in the process of hiring a chief information security officer to lead the effort.

- August 26 – (Gov Fac) *Nextgov*: [Defense looks for ways to detect insiders stealing classified files](#). The Defense Advanced Research Projects Agency kicked off August 25 a project that would give the Defense Department the ability to quickly detect and stop insiders intent on stealing information from military and government computer systems.
- August 26 – (Banking) *Bank Info Security*: [ACH fraud: action plan in Oct](#). A working group created by the Financial Services Information Sharing and Analysis Center is working on developing best practices to fight corporate account takeover. These incidents, resulting from ACH and wire fraud against business accounts, have been the focus of industry experts for one year.

Reports and Publications

Government Computer News: [Government-wide security certification could bolster cloud, Symantec study shows](#). A government-wide certification and accreditation process for securing cloud computing infrastructures could accelerate adoption of the computing model among agencies, but barriers include management and oversight issues, according to a Symantec report on security and the cloud. Eight-three percent of the 202 federal information technology decision-makers surveyed for the report, “[Symantec 2010 Break in the Cloud](#),” said it will take 3 or more years for the government to implement a comprehensive C&A process.

Infosecurity: [Nationwide banks experience surge as phishing targets](#). Since February of this year, RSA’s Anti-Fraud Command Center has seen a marked [uptick](#) in phishing attacks targeting the largest nationwide banks. From June 2009 through February 2010, larger financial institutions were targeted in the 19 to 30 percent range, depending on the month. The latest trend, however, shows that these large nationwide banks are receiving almost two-thirds of all phishing attempts in the finance sector, topping out at 68 percent in June.

DarkReading: [Attitudes about PC and mobile device security converging, study says](#). The thought process surrounding PC and laptop security is quickly being integrated with strategies for protecting mobile and portable devices, according to a study published the week of August 2. The report entitled “[Managing and Securing Corporate and Personal Mobile Devices in Financial Services](#),” found that more than half of financial services enterprises already support personally owned mobile devices, according to the study. More than one-third of the IT professionals indicated that their enterprise supports multiple mobile operating systems (OSs), with 10 percent supporting four or more.

DarkReading: [Healthcare suffers more data breaches than financial services so far this year](#). Healthcare data breaches have swollen in 2010, according to the [Identity Theft Resource Center](#). In a report the organization released in August, it shows compromised data stores from healthcare organizations far outstrip other verticals. According to figures updated in early August, healthcare organizations have disclosed 119 breaches so far this year, more than three times the 39 breaches suffered by the financial services industry.

Help Net Security: [6 million malicious files found in the past 3 months](#). Malware has reached its highest levels, making the first six months of 2010 the most active half-year ever

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



August 2010

for total malware production, according to a new McAfee [report](#). At the same time, spam leveled out with only 2.5 percent growth from Q1 2010. Malware continued to soar in Q2 2010, as there were 10 million new pieces cataloged in the first half of this year.

Nextgov: [Most attacks on federal networks financially motivated](#). Most malware attacks against federal agencies are financially motivated, seeking to trick computer users into buying fake security software or providing personal information that can be used to hack into their bank accounts, according to data collected from the U.S. Computer Emergency Readiness Team at the Homeland Security Department.

IDG News Service: [NSS Labs: Testing shows most AV suites fail against exploits](#). A majority of security software suites still fail to detect attacks on PCs even after the style of attack has been known for some time. NSS Labs [tested](#) how security packages from 10 major companies detect so-called “client-side exploits.” In such incidents, a hacker attacks software vulnerabilities such as Web browsers, browser plug-ins or desktop applications such as Adobe Acrobat and Flash.

Help Net Security: [The dramatic increase of vulnerability disclosures](#). Vulnerability disclosures are increasing dramatically, having reached record levels for the first half of 2010, according to the [IBM X-Force 2010 Mid-Year Trend and Risk Report](#) released August 25. Overall, 4,396 new vulnerabilities were documented by the X-Force Research and Development team in the first half of 2010, a 36 percent increase over the same time period last year. Fifty-five percent of all disclosed vulnerabilities had no vendor-supplied patch at the end of the period.

Help Net Security: [25% of new worms are designed to spread through USB devices](#). In 2010, 25 percent of new worms have been specifically designed to spread through USB storage devices connected to computers, according to PandaLabs. These types of threats can copy themselves to any device capable of storing information such as cell phones, external hard drives, DVDs, flash memories and MP3/4 players.

Your comments and suggestions are highly valued. Please send us feedback at:
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

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](#).

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