CIKR Monthly Open Source Cyber Digest (OSCD)

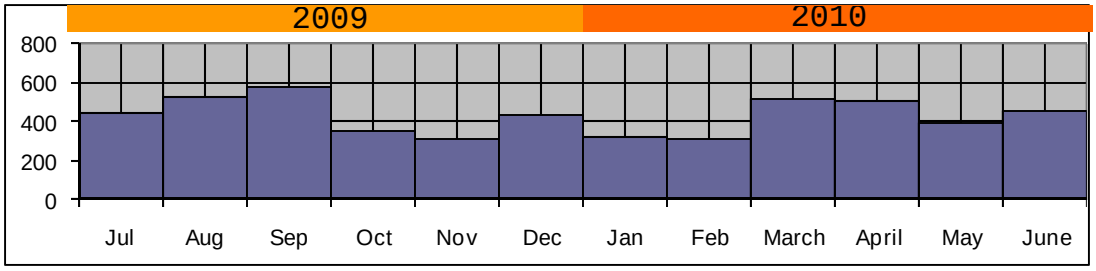
June 2010

IN THIS REPORT

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

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 New New Internet reported that the Webmaster of a Taliban-endorsed Web site has claimed that the site was hacked. An administrator for a jihadi forum endorsed by the Taliban wrote in a post that the "group's main site and the site of its online journal Al-Sumud, have been the subject of an 'infiltration operation.'" While no one has claimed credit for the hack, the Department of Defense has previously announced its intentions to take-down terrorist-affiliated Web sites. The H Security said that according to the latest analysis, the mass Web site hacks that have been showing up since June 9 are aimed at stealing access credentials for online games. The hackers' most prominent victims serving the malware have been the Wall Street Journal and the Jerusalem Post Web sites. According to Computerworld, three out of four companies will soon face more security risks because they continue to run the soon-to-be-retired Windows XP Service Pack 2 (SP2), said a report published June 22. Finally, a U.S. senate committee has approved a sweeping piece of legislation that creates a new cyber-security office within the White House and expands the authority of the Department of Homeland Security in securing critical infrastructure, eWeek reported. In other news

- Defense Tech reported While installing software upgrades to ground control stations for a new fleet of GPS satellites, Air Force inspectors discovered a glitch in software compatibility that rendered dark up to 10,000 GPS receivers for at least two weeks.
- Cnet News, cited a June 22 report that found that about 20 percent of the 48,000 apps in the Android marketplace allow a third-party application access to sensitive or private information. Some of the apps were found to have the ability to do things such as make calls and send text messages without the mobile user's knowledge.

June 2010

Sniff(ed): A sniffer is a tool that monitors network traffic as it is received in a network interface.

Special Coverage

According to The Register, Connecticut's attorney general June 7 became the latest law enforcement official to order Google to give a detailed accounting of the information its Street View cars surreptitiously **sniffed** from unsecured Wi-Fi networks over a three-year period. In a letter to Google officials, the attorney general demanded they provide additional details about the data collection, including what type of information was intercepted, the duration and location of the snooping operation, and where the data is stored now. He joins officials in the state of Missouri; and the countries of France, Germany, Spain, Canada and Australia in ordering the search giant to be more forthcoming about the privacy violation. IDG News Service reported that Wi-Fi traffic intercepted by Google's Street View cars included passwords and e-mail, according to the French National Commission on Computing and Liberty (CNIL). CNIL launched an investigation last month into Google's recording of traffic carried over unencrypted Wi-Fi networks, and has begun examining the data Google handed over as part of that investigation.

Also in the month of June, the Washington Post reported that AT&T said June 9 that a security breach had exposed the e-mail addresses of Apple iPad users. The nation's second-largest wireless service provider said that the problem had been fixed, and that it would inform customers of the breach, which also exposed iPad identification numbers used to authenticate a wireless user. Gawker reported that the information was obtained by a hacker group calling itself Goatse Security, and that 114,000 e-mail addresses were exposed. The Wall Street Journal says that the FBI had opened an investigation into a possible security breach of AT&T Inc.'s Web site that exposed the e-mail addresses of some owners of Apple Inc. iPad devices. The security hole highlights how corporations still have problems protecting private information. The Federal Communications Commission (FCC) weighed in June 11 on both the Google WiFi snooping and the iPad hacks stating AT&T's failure to safeguard information for more than 100,000 iPad users, and Google's collection of user data over Wi-Fi networks were "each worrisome in its own way," according to The Register. "Our Public Safety and Homeland Security Bureau is now addressing cyber security as a high priority," the FCC's chief of consumer and governmental affairs said in a blog post entitled "Consumer View: Staying Safe from Cyber Snoops." Newsfactor Network reported June 14 that the hacker site Goatse Security said "all iPads are vulnerable" because of a weakness in Apple's Safari browser. Newsfactor also shed some light on the e-mail list of individuals who were hacked, including staff members in the U.S. Senate and House of Representatives, and employees at the Justice Department, NASA, Department of Homeland Security, The New York Times, Dow Jones, Viacom, Time Warner, and News Corp. Infoworld reported that hack of iPad user info on the AT&T site may be much worse than an embarrassment, according to a security researcher who specializes in mobile devices. On his blog, the IOActive researcher said the Integrated Circuit Card IDs (ICCIDs) exposed in the iPad attacks are intended to be public. But he noted that hackers could exploit lax security in other areas of AT&T's GSM network and, using the e-mail addresses exposed in the attacks, attack iPad accounts and gain access to sensitive information. DarkReading says that the recent breaches of Apple iPad customer data at AT&T have drawn attention to security issues in both the mobile device and service provider spaces. But after analyzing the leaks, analysts said the lessons to be learned are not related to mobile or service vulnerabilities — they are lessons about the links between Web applications and back-end databases

[Return to top]

June 2010

Cyber Attacks

South Korea says cyber attacks came from China sites

June 10 - (IT)

South Korea said a government Web site was attacked June 9 from Internet addresses in China. The report comes amid concerns that North Korea is mounting cyber attacks in response to international pressure over the sinking of a South Korean warship in March. The attacks took place between 8:20 p.m. and midnight, the Ministry of Public Administration and Security said in a statement posted on its Web site June 10. The ministry blocked access after spotting the intrusions, and a probe is being conducted with related government offices, it said. North Korea's postal ministry was the source of similar cyber attacks last July that sought to cripple dozens of Web sites in South Korea and the U.S., the JoongAng Ilbo reported in October, citing the director of the South's spy agency. Tensions have risen on the Korean peninsula since an international panel concluded May 20 that the North was behind a torpedo attack that sank the Cheonan warship, killing 46 of the South's sailors.

Bloomberg: **South Korea says cyber attacks came from China sites**

Taliban hacked, DoD starts cyber offensive

June 14 - (IT)

The Webmaster of a Taliban-endorsed Web site has claimed that the site was hacked. An administrator for a jihadi forum endorsed by the Taliban wrote in a post that the "group's main site and the site of its online journal Al-Sumud, have been the subject of an 'infiltration operation,'" according to Wired.com. The post goes on to warn online jihadists "to not enter any of the links that concern these Web sites, and not even to surf [the content] until you receive the confirmed news by your brothers, Allah-willing." Outages of jihadist Web sites are relatively common, though this may be the first example of a site being hacked, a spokesman of Flashpoint Partners told Wired. While no one has claimed credit for the hack, the Department of Defense has previously announced its intentions to take-down terrorist affiliated Web sites.

The New New Internet: **Taliban hacked, DoD starts cyber offensive**

Other Attacks articles:

- *June 2* – (Commercial) ***SC Magazine*: Jewish Chronicle confirms that it was hit by a denial-of-service attack on Monday following Gaza flotilla incident.** The Jewish Chronicle was hit by a massive **denial-of-service (DoS)** attack on May 31. Following the Gaza flotilla incident, a column in the Spectator claimed that the website of the paper was down following 'a massive denial-of-service, apparently to shut down its balanced coverage of the Ashdod flotilla incident.'
- *June 9* – (IT) ***The New New Internet*: Vietnam accused of cyber attacking bloggers.** The Vietnamese government is being accused of conducting cyber attacks to bring down the Web sites of independent bloggers, as well as arresting some of the dissidents. Human Rights Watch recently listed a series of arrests and police harassment of Web dissidents since mid-April.
- *June 16* – (Banking) ***The Register*: Eastern European banks under attack by next-gen crime app.** Banks in Russia and Ukraine are under siege by criminal gangs wielding a sophisticated, next-generation exploitation kit that hacks the financial institutions' authentication system and then hits it with a denial-of-service attack. The attacks are being carried out with the help of a top-to-bottom revision of **BlackEnergy**.

Denial of Service Attack: A DoS attack that attempts to prevent legitimate users from accessing information or services. (US-CERT)

BlackEnergy: a popular easy to use toolkit that until recently was used primarily to launch DDoS (The Register)

[Return to top]

- *June 22* – (IT) ***The New New Internet:*** **Cyber war part of Kyrgyzstan ethnic conflict.** The recent ethnic troubles in Kyrgyzstan have also included attacks in cyberspace against government and media Web sites, according to Russian cybersecurity experts. The assaults appear to be a result of distributed denial of services (DDoS) attacks which flood Web sites with illegitimate data requests from "bot" computers, blocking any legitimate data requests from getting through.

Data Breach/Information Gathering

Digital River sues over data breach

June 4 - (IT)

A massive data theft from the e-commerce company Digital River Inc. has led investigators to hackers in India and a 19-year-old in New York who allegedly tried to sell the information to a Colorado marketing firm for half a million dollars. The Eden Prairie company obtained a secret court order last month to block a suspect of Brooklyn from selling, destroying, altering or distributing purloined data on nearly 200,000 individuals. Digital River suspects that the information was stolen by hackers in New Delhi, India, possibly with help from a contractor working for Digital River. The suspect has said he got the information from India, but would not say how or from whom. "I fully suspect that [the suspect] hacked the hacker," said an attorney with Robins, Kaplan, Miller and Ciresi who is overseeing Digital River's investigation. The matter came to light June 3 when a U.S. district judge convened a public status conference in the case.

Minneapolis Star Tribune: **Digital River sues over data breach**

Two Mexican botnets taken down

June 10 - (IT)

Early in June, Trend Micro was alerted to a **phishing** attack that was aimed at Spanish-speaking users and was discovered to be originating from a Mexican botnet. The attack was using the news of a missing girl and her violent death to try to get visitors to download a video. Of course, the video in question was no such thing, but a client program of a bot. Searching deeper, Trend Micro researchers managed to access the **botnet**'s C&C center, and to discover - and publish - details about its management functions and interface, as well as get a good look into what this botnet was able to do. They found out that it was also responsible for downloading malware on the target computers, and for targeting users with phishing attacks that impersonated PayPal's site and that of the largest bank in Mexico. Finally, they named it Tequila botnet. Since then, the Tequila botnet has been taken down - surprisingly enough, by its owners. The researchers speculate that the reason behind this decision was the fact that they have exposed the proxy servers and hosts.

Help Net Security: **Two Mexican botnets taken down**

Mass website hack aimed at online gamers

June 15 - (IT)

According to the latest analysis, the mass Web site hacks that have been showing up all over since June 9 are aimed at stealing access credentials for online games. The hackers' most prominent victims serving the malware have been the Wall Street Journal and the Jerusalem Post Web sites. The hacked Web servers are all Microsoft Internet Information Server (IIS) and ASP-NET-based, but analysis by a number of security services providers has shown that the attacker has used SQL injection vulnerabilities in custom Web applications to hack the

Phishing: Use of e-mail or malicious Web sites to solicit personal information by posing as a trustworthy organization. Often referred to as "Phishing Attacks". (US-CERT)

Botnet ("bot"): A large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack. (PC Magazine)

[Return to top]

SQL Injection: SQL injection is an attack in which malicious code is inserted into strings that are later passed to a SQL Server for parsing and execution. (Microsoft)

sites. Administrators are advised to check their systems for any signs of interference and tampering. **The SQL injection** vulnerability allows attackers to write their own HTML and JavaScript to the hacked sites content-management system's database. Specifically, the attackers embedded code, which uploads an exploit for the recently discovered vulnerability in Flash Player, into an iFrame. The code then tries to infect the hacked sites visitors' systems with Trojans. It appears the attackers objective is to steal access data to Asian gaming Websites such as aion.plaync.co.kr, aion.plaync.jp and df.nexon.com. The Flash Player vulnerability has been fixed in version 10.1. A Chinese group known as dnf666, which was also responsible for a major SQL injection attack in March, appears to be behind the attack.
The H Security: **Mass website hack aimed at online gamers**

Paraguyan government website hosts phishing data.

June 17 - (IT)

Phishing gangs are growing increasingly bold, evidenced by researchers finding phishing data on a Web site owned by the Paraguayan government. Sunbelt researchers discovered that a Web site belonging to the Paraguayan government is hosting data on banks and insurance companies in the United Kingdom gathered through phishing attacks. The researchers have notified the Web site owners regarding the data cache. Typically, researchers will sit on the data and try to learn more information about the cyber criminals. Hosting stolen data on another server is considerably safer for cyber criminals, and operates similar to a "slick" used by spies. The data remains accessible but if anyone stumbles upon the data, the police are unable to arrest the criminals.
The New New Internet: **Paraguyan government website hosts phishing data**

Other Data Breach/Information Gathering articles:

- June 1 – (Banking) ***BankInfoSecurity*: ACH fraud sparks another suit.** A Maine business has sued its bank, alleging that the institution failed to prevent fraudulent ACH transactions totaling more than $500,000.
- June 4 – (Banking) ***Techworld*: HSBC browser plugin attacked by Trojan.** Trusteer's Rapport, a popular anti-keylogging tool used by online banks such as HSBC, has come under direct attack by malware writers trying to bypass its protection settings.
- June 7 – (Banking) ***IDG News Service*: BofA call center worker pleads guilty to data theft.** A Bank of America call-center employee has pleaded guilty to charges that he stole sensitive client information and then tried to sell it for cash. He allegedly logged account holders' names, birth dates, addresses and account histories between September 2009 and April 2010 and unwittingly sold them to an undercover FBI agent.
- June 7 – (Banking) ***The New New Internet*: Hacker steals more than $640K from NYC DOE.** A report released last week by the New York City's Special Commissioner Office revealed a hacker stole more than $640,000 from the Department of Education's petty-cash account at JP Morgan Chase and distributed the codes to others to use to pay for student loans, gas bills and other purchases.
- June 21 – (Gov Fac) ***Ball State Daily News*: Phishing attacks on Ball State accounts continue.** A phishing attack on Ball State University e-mail accounts could still be a threat to its users. University Computing Services has worked to clear damaged computers, but faculty and students at the Muncie, Indiana institution were still receiving bogus e-mails as of June 18.

[Return to top]

- June 21 – (Communications) ***Erie Times News*: Verizon warns of scammers 'phishing' for account information.** The manager of media relations at Verizon Communications Inc. said Erie, Pennsylvania residents should be on the lookout for suspicious e-mails allegedly from Verizon employees asking individuals for updated information.

Threats and Vulnerabilities

Software glitch renders dark thousands of GPS receivers, for days

June 1 - (Gov Fac; DIB; Communications)

While installing software upgrades to ground control stations for a new fleet of GPS satellites, Air Force inspectors discovered a glitch in software compatibility that rendered dark up to 10,000 GPS receivers for at least two weeks. The new software was installed back in January and initially the Air Force blamed the contractor for writing a bad program, the Air Force says the trouble was caused by a compatibility problem instead of defective code; the affected receivers all came from the same source. It took Air Force techs less than two weeks to discover the outage and begin putting in place a temporary fix; a more permanent fix is being distributed. Apparently, the outage affected GPS receivers on the Navy's in-development carrier-launched drone, the X-47B. While willing to identify that Navy program, the Air Force refused to identify other weapons that might have been impacted by the software problem. A spokesperson for the Air Force's Space and Missile Systems Center told The Associated Press that the military's GPS system, and its heavily encrypted communications channel, is safe from cyber attack and that it has never been hacked.

Defense Tech: Software glitch renders dark thousands of GPS receivers, for days

Researchers: Poor password practices hurt security for all

June 7 - (All Sectors)

A large-scale study of password-protected Web sites revealed a lack of standards across the industry that harms end-user security, according to two researchers working at the University of Cambridge in England. In particular, the weak implementations of password-based authentication at lower-security sites compromises the protections offered at higher-security sites because individuals often re-use passwords, the two researchers asserted in a paper presented at the Workshop on the Economics of Information Security in Cambridge, Massachusetts June 7. Attackers can use low-security Web sites such as news outlets to figure out passwords associated with certain e-mail addresses, and then use those passwords to access accounts at higher-security sites such as e-commerce vendors, one of the researchers said. In an effort that the researchers said is the largest empirical investigation into password implementations to date, they collected data from 150 Web sites and found widespread "questionable design choices, inconsistencies, and indisputable mistakes." The researchers seemed disinclined to blame users for re-using passwords or making them easy to guess, arguing that most users have too many online accounts to manage them all securely. The large majority — 78 percent — of sites examined failed to provide users with feedback or advice on choosing a strong password. Only five sites let the user register password hints, a strategy that encourages users to come up with stronger passwords. Just seven sites required users to mix numbers and letters, and only two demanded passwords include non-alphanumeric characters as well.

IDG News Service: Researchers: Poor password practices hurt security for all

[Return to top]

June 2010

Tool automates social engineering in man-in-the-middle attack

June 10 - (IT)

French researchers have developed an automated social-engineering tool that uses a man-in-the-middle attack and strikes up online conversations with potential victims. The proof-of-concept (PoC) HoneyBot poses convincingly as a real human in Internet Relay Chats (IRC) and Instant Messaging (IM) sessions. It lets an attacker glean personal and other valuable information from victims via these chats, or lure them into clicking on malicious links. The researchers had plenty of success in their tests: They were able to get users to click onto malicious links sent via their chat messages 76 percent of the time. The researchers who created the PoC — all of Institut EURECOM in France — are also working on taking their creation a step further to automate social-engineering attacks on social networks. The researchers originally wrote their HoneyBot PoC tool as a way to demonstrate large-scale automated social-engineering attacks. While spammers typically send IM messages that attempt to lure users to click on their malicious links, these attacks are often fairly conspicuous and obvious to the would-be victim. Such an attack could occur via an online shopping Web site or bank site that contains an embedded chat window, the researchers said. An attacker then could set up a phishing site and wage a man-in-the-middle attack on the chat window.

DarkReading: Tool automates social engineering in man-in-the-middle attack

Kaspersky Lab: Mobile malware evolves as an industry focus on it is the next step

June 18 - (Communications, IT)

The threat of malware and botnets for mobile phones could become as much of a problem as they are for PCs. The mobile research group manager and senior analyst at Kaspersky Lab pointed at threats such as the “brother” and “Ikee” worms, and said that it was now seeing 30 developments per month in mobile malware, and that 35 percent of malware is now designed to infect mobile Internet. He said: “This threat will not go away, and the reasons for the whole Internet-based malware appearance is that new technologies will be the future. A mobile botnet will have the same impact as a simple PC botnet. They will be able to send SMS, MMS, Google spam and mask passwords, and maybe provide telephone DDoS attacks. Imagine a big organization and they have four main telephone numbers, and the competitor does not want to work honestly and decides to do bad things such as a telephone DDoS. Imagine all of the smartphones all started to dial four numbers, that will always be busy so users will have no chance to dial and the company will not be able to do anything.” Asked about the specific threats for mobiles, the analyst told SC Magazine that the threats are more Web-based and are mainly Trojans. He said: “Cyber criminals try to mask applications to download software, so when people use computers for downloading software for mobile, that is how we detect Trojan programs.”

SC Magazine: Kaspersky Lab: Mobile malware evolves as an industry focus on it is the next step

Most firms face security ‘red alert’ as XP SP2’s retirement looms

June 22 - (All Sectors)

Three out of four companies will soon face more security risks because they continue to run the soon-to-be-retired Windows XP Service Pack 2 (SP2), said a June 22 report. Toronto-based technology systems and services provider Softchoice Corp. said that 77 percent of the

[Return to top]

organizations it surveyed are running Windows XP SP2 on 10 percent or more of their PCs. Nearly 46 percent of the 280,000 business computers Softchoice analyzed rely on the aged operating system. "This is a red alert," said Softchoice's services development manager. "This isn't something you can safely ignore." He was referring to the impending end-of-support deadline that Microsoft Corp. has set for Windows XP SP2, a service pack that debuted in the fall of 2004. After July 13, Microsoft will stop issuing security updates for SP2, a move that has users scrambling to update to Windows XP SP3, which will be supported until April 2014. "Windows XP SP2 is deployed in 100 [percent] of the companies [surveyed] to some extent," said the manager. "But that doesn't tell the whole story. On average, 36 [percent] of the PCs in every organization run SP2." Softchoice obtained its data from customers of its IT assessment services, which include asset, hardware life cycle and licensing management. It analyzed PCs in 117 U.S. and Canadian organizations in the education, financial, health care, and manufacturing industries. The firm weighted the number of XP SP2 systems in each polled organization to arrive at the average usage mark .
Computerworld: **Most firms face security 'red alert' as XP SP2's retirement looms**

Report says be aware of what your Android app does

June 22 - (IT)

About 20 percent of the 48,000 apps in the Android marketplace allow a third-party application access to sensitive or private information, according to a June 22 report. Some of the apps were found to have the ability to do things like make calls and send text messages without requiring interaction from the mobile user. For instance, 5 percent of the apps can place calls to any number and 2 percent can allow an app to send unknown SMS messages to premium numbers that incur expensive charges, security firm SMobile Systems concluded in its Android market-threat report. SMobile said that while not all apps are malicious, there is the potential for abuse. Users should know what the apps they downloaded are doing because they have expressly granted the apps permission to conduct those activities. In addition, the Android architecture limits the apps to the permissions granted so any damage from a potentially malicious app would be very limited, according to Google. The report found that dozens of apps have the same type of access to sensitive information as known spyware does, including access to the content of e-mails and text messages, phone-call information, and device location, said the chief technology officer at SMobile Systems.
Cnet News: **Report says be aware of what your Android app does**

Other Threats and Vulnerabilities stories:

- June 1 – (IT) ***The Register*****:** **'Clickjacking' worm hits hundreds of thousands on Facebook.** A vulnerability on Facebook forced hundreds of thousands of users to endorse a series of Web pages over the Memorial Day weekend, making the social networking site the latest venue for an attack known as clickjacking.
- June 1 – (IT) ***DarkReading*****:** **Botnets target websites with 'posers'.** Botnets increasingly are creating phony online accounts on legitimate Web sites and online communities in order to steal information from enterprises. This alternative form of targeted attack by botnets has become popular as botnet tools have made bots easier to purchase and exploit.
- June 4 – (ESS) ***Firehouse.com*****:** **Software failure linked to Minn. woman's death .** An ongoing investigation has revealed that a software glitch likely led to a woman's death aboard a fire department ambulance in Minnesota April 22.

[Return to top]

- June 6 – (All Sectors) ***Computerworld*: Update: Attackers exploit critical bug in Adobe's Flash, Reader.** Adobe June 4 warned that attackers are exploiting a critical vulnerability in the company's most widely-used software: Flash Player and Adobe Reader. Adobe said that the bug affects Flash Player 10.0.45.2, the most up-to-date version of the popular media player, as well as older editions on Windows, Macintosh, Linux and Solaris.
- June 8 – (IT) ***The Register*: Researchers release point-and-click Web site exploitation tool.** Researchers have released software that exposes private information and executes arbitrary code on sensitive Web sites by exploiting weaknesses in a widely used Web-development technology. Short for Padding Oracle Exploitation Tool, POET is able to decrypt secret data encrypted by the JavaServer Faces Web development framework without knowing the secret key.
- June 10 – (All Sectors) ***SC Magazine*: New zero-day vulnerability in Microsoft Windows XP and 2003 discovered.** Microsoft warned June 10 of a new zero-day vulnerability for Windows XP/2003. The vulnerability is in the Windows Help and Support Center component and is accessed through the protocol handler "hcp://."
- June 11 – (Communications) ***UPI*: Solar flare activity might threaten GPS.** A Cornell University expert on global positioning and satellite systems is warning they will be challenged as solar flare activity increases
- June 15 – (Energy) ***Cnet News*: Money trumps security in smart-meter rollouts, experts say.** In a rush to take advantage of U.S. stimulus money, utilities are quickly deploying thousands of smart meters to homes each day — smart meters that experts say could easily be hacked. The security weaknesses could potentially allow miscreants to snoop on customers and steal data, cut off power to buildings, and even cause widespread outages, according to a number of experts who have studied the meters.
- June 22 – (All Sectors) ***Help Net Security*: Flaw in VPN systems nullifies its promise of privacy.** A security flaw in the virtual private network (VPN) systems - caused by the combination of IPv6 and PPTP-based VPN services - can be exploited and a user's IP address, MAC address and their computer name can be identified.
- June 23 – (Water) ***Lake Chelan Mirror*: Computer failure interrupts flow from city water plant.** There was no water flow for some Chelan, Washington residents in the early hours of June 13, because of a computer failure at the city's water-treatment plant.
- June 24 – (All Sectors) ***V3.co.uk*: Asprox botnet causing serious concern.** Security researchers are warning of a rapidly growing number of Web sites infected by the Asprox spam botnet. Asprox is capable of launching SQL-injection attacks, and has more than doubled its appearance on application service provider (ASP) sites from 5,000 to 11,000, according to M86 Security.
- June 24 – (All Sectors) ***DarkReading*: Kraken botnet making a resurgence, researcher says.** The Kraken botnet — one of the Internet's largest and most difficult to detect in 2008 — is rearing its ugly head again. In fact, the old security nemesis — which was reported dismantled in 2009 — has compromised more than 318,000 systems, nearly half of the 650,000-node size it achieved at its peak in 2008, according to a research scientist at the Georgia Tech Information Security Center.
- June 28 – (IT) ***V3.co.uk*: Hackers target instant-messaging applications.** Security experts in Germany are warning of a new threat to MSN Messenger and Windows Live Messenger. G Data SecurityLabs research has found a recent surge in spam and phishing sites that link to the services, as well as a wave of seemingly "endless" fake-friend

[Return to top]

requests.

Policy, Legislation and Governance

NSA leader urges cybersecurity protocols

June 3 - (All Sectors)

The commander of the newly created U.S. Cyber Command said June 3 the nation needs precise rules of engagement that would set the standards for a quick counterattack to a serious breach of U.S. military or civilian data networks. It also would be helpful if there were international rules on how nations can respond to cyber attacks, he said. The commander took over the new command, which is primarily responsible for protecting the military's cyber networks, in mid-May. He retains his duties as head of the National Security Agency, which conducts electronic surveillance of suspected adversaries and possible terrorists. During an appearance at the Center for Strategic and International Studies, he said his command is looking at current rules of engagement, how they conform to the laws and his responsibilities, and "how we can articulate those so the people know what to expect." The cyber commander said there probably need to be two sets of rules of engagement, one to cover peacetime situations and another for war. He said the issue is complicated by the possibility that an adversary may use a neutral country's computers to launch the attack. In addition, there are differences between an attack on U.S. military systems and one against government or civilian networks.

Congress Daily: **NSA leader urges cybersecurity protocols**

After Google hack, warnings pop up in SEC filings

June 8 - (DIB; IT)

Five months after Google was hit by hackers looking to steal its secrets, technology companies are increasingly warning their shareholders that they may be materially affected by hacking attempts designed to take valuable intellectual property. In the past few months Google, Intel, Symantec and Northrop Grumman — all companies thought to have been targets of a widespread spying operation — have added new warnings to their U.S. Securities and Exchange Commission filings informing investors of the risks of computer attacks. Google does not talk about the specific attack against its systems, but it now warns shareholders that this type of event is a material risk. "[O]utside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information in order to gain access to our data or our users' or customers' data," Google wrote in a section added to its annual financial report in February, a month after it disclosed the hacking incident. Google warned that it could lose customers following a breach, as users question the effectiveness of its security. Google's admission that it had been targeted put a public spotlight on a problem that had been growing for years: targeted attacks, known to security professionals as the advanced persistent threat.

IDG News Service: **After Google hack, warnings pop up in SEC filings**

Judge limits DHS laptop border searches

June 10 - (All Sectors)

A federal judge has ruled that border agents cannot seize a traveler's laptop, keep it locked up for months, and examine it for contraband files without a warrant half a year later. The U.S. district judge in the Northern District of California rejected the U.S. President administration's argument that no warrant was necessary to look through the electronic files of an

[Return to top]

American citizen who was returning home from a trip to South Korea. "The court concludes that June search required a warrant," the judge ruled June 2, referring to a search of a suspect's computer that took place a year ago. The Justice Department invoked a novel argument which the judge dubbed "unpersuasive" claiming that while the suspect was able to enter the country, his laptop remained in a kind of legal limbo where the Bill of Rights did not apply.
Cnet News: **Judge limits DHS laptop border searches**

Controversial cyber bill passes Senate homeland security committee

June 24 - (All Sectors)

A U.S. Senate committee has approved a sweeping piece of legislation that creates a new cyber-security office within the White House and expands the authority of the Department of Homeland Security in securing critical infrastructure. The panel gave the thumbs up to a controversial cyber-security bill that some claim expands executive powers too far in the event of a cyber-attack. The Protecting Cyberspace as a National Asset Act was approved by the Homeland Security and Governmental Affairs Committee June 24 in a unanimous vote. Critics have accused the bill's authors of giving the President the authority to shutdown parts of the Internet in the event of an attack, something a Senator and others say is exaggerated. The legislation, supporters argue, mandates among other things that the President use the "least disruptive means feasible" to respond to a threat. Among other things, the bill creates a White House Office of Cyberspace Policy to lead federal and private sector efforts to protect the nation's critical infrastructure. The office would be led by a director approved by the Senate. The bill also creates a new center within the Department of Homeland Security to implement cyber-security policies for public and private networks.
eWeek: **Controversial cyber bill passes senate homeland security committee**

U.S. outlines security strategy for online identity

June 28 - (All Sectors)

The White House has published a draft of a strategy designed to make the concept of trusted identities and authentication a reality in the digital world. In a 39-page document entitled the "National Strategy for Trusted Identities in Cyberspace" (NSTIC), the White House promotes the "Identity Ecosystem," an interoperable environment where individuals, organizations and devices can "trust each other because authoritative sources establish and authenticate their digital identities." The ecosystem will consist of three main layers – a governance layer that establishes the rules of the environment; a management layer that applies and enforces the rules; and the execution layer that conducts transactions in accordance with the rules. "The federal government, in collaboration with individuals, businesses, non-profits, advocacy groups, associations, and other governments, must lead the way to improve how identities are trusted and used in cyberspace," the document reads. "Ongoing collaboration ... has already resulted in significant gains towards establishing Identity Ecosystem components. However, much more remains to be done."
eWeek: **U.S. outlines security strategy for online identity**

Other Policy Legislation and Governance stories:

- June 3 – (IT) ***The Register*****: FTC slaps down commercial keylogger firm.** CyberSpy Software, which markets the controversial RemoteSpy commercial keylogging applica-

[Return to top]

tion, has agreed to rewrite the software and clean up its business practices to settle a case brought by the FTC.

- June 4 – (Banking) ***IDG News Service*: Visa launches one-time passcode cards in Europe.** Visa has launched a payment card in Europe that contains a keypad and an eight-character display for showing a one-time passcode, an additional defense against potentially fraudulent Internet transactions.
- June 7 – (All Sectors) ***IDG News Service*: FTC examines privacy risks of copier hard drives.** The FTC is urging the photocopier industry to address privacy risks arising from the fact that digital copiers store thousands of documents on their internal hard drives.
- June 9 – (Health) ***ExecutiveGov*: Maryland given green light on health IT exchange plan.** The federal government has given Maryland's health IT plan the go-ahead, making the state one of three recipients of recent approvals from the Department of Health and Human Services to develop a health records exchange.
- June 13 – (Energy) ***Fierce Government IT*: House approves GRID Act.** The President would gain new powers over the U.S. electrical grid under a bill the House of Representatives approved June 9. The Grid Reliability and Infrastructure Defense (GRID) Act would permit the President to order immediate emergency measures to protect the reliability of the bulk-power system or defend critical electric infrastructure against an imminent grid security threat. The GRID Act passed the House on voice vote; it now lies before the Senate Energy and Natural Resources Committee.
- June 17 – (All Sectors) ***DarkReading*: Cybersecurity not a 'Command And Control' effort.** Cybersecurity initiatives will always be distributed efforts, which is what makes the cybersecurity czar's position so crucial, according to the Department of Homeland Security's cybersecurity director.
- June 18 – (Banking) ***USA Today*: Microsoft opens center for reports of stolen identities, data.** In a major step to slow cybercrime, Microsoft June 17 launched a coalition that will serve as a clearinghouse for reports about caches of stolen data stashed all across the Internet. The Internet Fraud Alert Center — spearheaded by Microsoft, and managed by the National Cyber-Forensics & Training Alliance — will serve as a reporting hub.

Reports and Publications

The New New Internet: Attempts to infect computers increases Attempts to infect computers have increased more than 25 percent according to Kaspersky Lab. In the first quarter of 2010, more than 327 million attempts were made to infect user computers in a variety of countries around the globe.

Network World: Cyberattacks seen as top threat to zap U.S. power grid Cyber attacks, pandemics and electromagnetic disturbances are the three top "high impact" risks to the U.S. and Canadian power-generation grids, according to a report from the North American Electric Reliability Corp. (NERC).

Computerworld: Group lists top five social media risks for businesses As businesses increasingly try to figure out how to use social-networking tools in the enterprise, an IT governance group has released a ranking of the top five risks social media poses to companies. The study, which lists the biggest risks businesses need to prepare for when they are using

[Return to top]

social media, was released June 7 by the Information Systems Audits and Control Association.

PC Advisor UK: **One third of search engine results are poisoned** A third of search engine results are poisoned links, said Symantec. The security vendor uncovered the size of the threat after its researchers spent two weeks investigating the top 100 results when searching for the 300 most popular terms. In one incident, 99 out of the top 100 search results for a phrase navigated to malicious Web sites designed to infect Web users.

DarkReading: **Smartphone malware multiplies** The number of malware and spyware programs found on smartphones has more than doubled in the past six months — and some types of malware are more prevalent on certain smartphone platforms than others according to Lookout.

DarkReading: **New paper outlines potential vulnerabilities in software supply chain** Application-security problems do not just occur when developers are writing code — they can occur as that code is exchanged or distributed, a new report argues. Sometimes security vulnerabilities are introduced when software makers exchange code — or when it is sent out to customers, according to "An Overview of Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain," a white paper issued June 14 by the Software Assurance Forum for Excellence in Code.

PC Advisor UK: **3.7 billion phishing emails were sent in the last 12 months** Cybercriminals sent 3.7 billion phishing e-mails over the last year, in a bid to steal money from unsuspecting Web users, says CPP. Research by the life-assistance company revealed that 55 percent of phishing scams are fake bank emails, which try and dupe Web users into giving hackers their credit card number and online banking passwords.

DarkReading: **Trojans now 70 percent of all malware, report says** Trojans comprise almost three-quarters of all malware sent by e-mail. At the same time, the volume of malware has climbed considerably since the beginning of the year. These findings are reported in the E-Mail Security Report June 2010 presented today by the leading German e-mail security specialist eleven. The vast majority (87 percent) of all spam e-mail is pharmaceutical-related. Germany continues to be among the top spam senders worldwide.

U.S. Government Accountability Office: **Cybersecurity: Continued attention is needed to protect federal information systems from evolving threats** Pervasive and sustained cyber attacks continue to pose a potentially devastating threat to the systems and operations of the federal government, the Government Accountability Office reported. In recent testimony, the Director of National Intelligence highlighted that many nation states, terrorist networks, and organized criminal groups have the capability to target elements of the United States information infrastructure for intelligence collection, intellectual property theft, or disruption.

InfoSecurity: **Social Security flexible workplace program leaves personal data at risk** Data security and breach prevention ranks low as a risk factor for most big technical companies, according to new research that identifies the most widespread concerns among the 100

[Return to top]

largest U.S. public technology companies. The research, released by BDO, a professional services firm, examines the risk factors listed in the fiscal year 2009 10-K SEC filings of the companies; the factors were analyzed and ranked in order by frequency cited.

The Register: **Security firms taking days to block malware** Anti-malware vendors can take up to 92.48 hours to block malicious sites, potentially leaving clients in blissful ignorance of threats to their systems in the meantime. Security researchers at ISS Labs reviewed a range of endpoint security products from 10 big-name security vendors and their response to "socially engineered or consensual malware threats."

The H Security: **Malware: certified trustworthy** According to anti-virus vendor F-Secure, the number of digitally signed malware samples for Windows is increasing - and more and more scareware programs also include a valid digital signature. Virus authors use this method to overcome various hurdles on Windows systems, and suppress alerts such as those triggered when a program attempts to install an ActiveX control in Internet Explorer, or before installing a driver.

CIO: **Credit card data breaches cost big bucks** Javelin Strategy & Research estimates that credit and debit card issuers spent $252.7 million in 2009 replacing more than 70 million cards compromised by data breaches. In 2009, an estimated 39 million debit cards and 33.3 million credit cards were reissued due to data breaches, for a total of 72.2 million. An estimated 20 percent of those affected by the breaches had more than one card replaced.

Help Net Security: **The truth about social media identity theft** The use of social media can increase consumer vulnerability to identity theft because of the amount and type of personal information people share on these networks. However, consumers do little or nothing to protect themselves, according to a recent study by the Ponemon Institute.

V3.co.uk: **Staff should lead in preventing security attacks** A company's employees are its best defense against security threats, and should be empowered and educated about technology risks, according to a new report from PricewaterhouseCoopers. The consulting firm said in its Protecting Your Business report that organizations are too complacent about security, and assume that they will not be affected. This lax attitude filters down to workers, who then believe that security is "someone else's problem".

eWeek: **Inside text message phishing attacks** Not all phishing takes place online. Text-message-based phishing, called smishing, is still out there, and though on the decline, a report from security vendor Internet Identity shows it is still being used to target credit unions.

Your comments and suggestions are highly valued. Please send us feedback at:
cikr.productfeedback@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:
CIKRISEaccess@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]