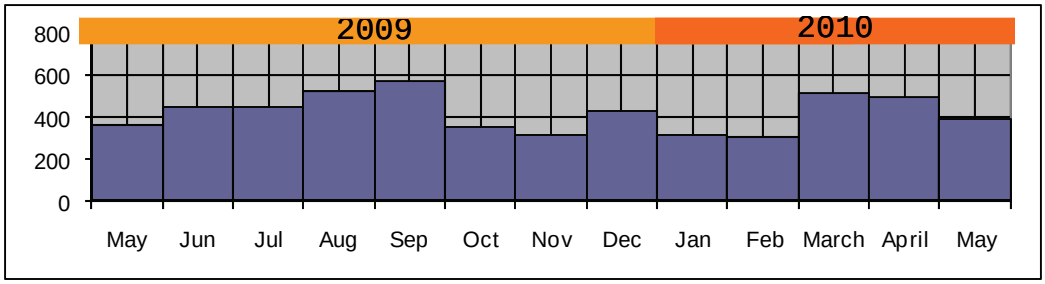
CIKR Monthly Open Source Cyber Digest (OSCD)

May 2010

IN THIS REPORT

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

DarkReading reported a single crime syndicate dubbed "Avalanche" was responsible for some 66 percent of the phishing traffic generated in the second half of 2009, according to a report published by the Anti-Phishing Working Group (APWG). A consumer group has called on the U.S. Federal Trade Commission (FTC) to investigate Google and the Wi-Fi sniffing has prompted a class-action lawsuit that could force the company to pay up to $10,000 for each time it snatched data from unprotected hotspots, court documents show Computerworld reported. Finally, University researchers have taken a close look at the computer systems used to run today's cars and discovered new ways to hack into them IDG News Service provided. In other news:

- Krebs on Security says that Carders.cc, a German online forum dedicated to helping criminals trade and sell financial data stolen through hacking, has itself been hacked.
- Marketwatch reported that The Securities & Exchange Commission chairwoman said on May 18 she expects her agency to issue preliminary findings on its inquiries into the "flash crash" on May 6, when the Dow Jones Industrial Average plunged nearly 1,000 points.
- Help Net Security says an overwhelming majority of Web browsers have unique signatures — creating identifiable "fingerprints" that could be used to track someone as they surf the Internet.
- The Register reported that the North Atlantic Treaty Organization (NATO) believes it is unlikely a conventional military attack on its members in the future, but that some form of cyber-attack is one of three most probable dangers facing the alliance.

May 2010

Special Coverage

Facebook experienced several exploits of its website during May and the resulting privacy debate continued to heat up during the month. V3.co.uk reported that after a malware attack hit the site on May 22, security experts called on Facebook to set up an early warning system on its network to notify users of security compromises. The attack was the second on successive Saturdays to use a "sexy video" to lure the recipient into clicking on a fake FLV Player upgrade message, which then downloads adware onto the PC. Computerworld reported the first attack on May 18 on the shear number of attacks, reaching 300,000 reports of the malicious Facebook app, AVG's chief research officer said.

Kaspersky Lab published a report showing that the number of phishing attacks on social networks has increased in the first quarter of 2010; especially for Facebook, the fourth most popular online target. Channel Web reported Facebook identified a hacker named Kirllos who tried to sell 1.5 million Facebook accounts in underground hacking forums. Although Kirllos claimed to have hacked 1.5 million, it is closer to a few thousand. IDG News Service also reported a bug that allows hackers to delete all of a users' site friends without permission. The flaw was reported May 19 by a college student, but on May 21 it could still be exploited to delete an IDG reporter's Facebook friends. Finally, Facebook engineers on May 5 disabled the site's live chat function after people outside the company discovered a bug that allowed users to eavesdrop on their friends' conversations. The site also had to take emergency action to correct a separate hole that allowed users to see their friends' pending friend requests The Register reported.

On May 6, the Electronic Privacy Information Center said it had joined 14 other organizations in filing a complaint with the Federal Trade Commission charging the social networking website with "unfair and deceptive" practices. The cadre of Facebook critics also fired off a letter to the US Congress urging legislators to closely monitor how the commission looks into Facebook privacy concerns according to Agence France-Press. Concurrently, IDG News Service reported a coalition of European data protection officials warned the social-networking site on May 12 that Facebook had made "unacceptable" changes to its privacy settings at the end of 2009 that are detrimental to users.

eWeek reported that amid the controversy about privacy, Facebook unveiled new security features designed to protect user accounts. "Over the last few weeks, we've been testing a new feature that allows you to approve the devices you commonly use to log in and then to be notified whenever your account is accessed from a device you haven't approved," a Facebook blog stated on May 13. According to IDG News Service, Facebook was fixing a Web programming bug that could have allowed hackers to alter profile pages or make restricted information public on May 18.

Cyber Attacks

Treasury Cloud computing host hacked

May 4 - (Government Facilities; Information Technology; Banking)

The Treasury Department blamed a cloud computing provider for the disruption of its Web site that provides the Internet face of the Bureau of Engraving and Printing, the agency that prints U.S. currency. A blog on May 3 reported that the sites were hacked. As of May 4, the bureau's Web site was inaccessible. On May 4, Treasury issued the following statement: "The Bureau of Engraving and Printing (BEP) entered the cloud computing arena last year. The hosting company used by BEP had an intrusion and as a result of that intrusion, numer-

[Return to top]

ous websites (BEP and non-BEP) were affected. BEP has since suspended the Web site. Through discussions with the provider, BEP is aware of the remediation steps required to restore the site and is currently working toward resolution." Treasury did not identify the host company. The chief research officer for IT security software vendor AVG wrote in his blog that "for a short while [May 3] a couple of treas.gov websites were hacked, and were reaching out to an attack site in Ukraine.
BankInfoSecurity.com: Treasury Cloud computing host hacked
See also, SPAMfighter News: US Treasury Websites Hijacked

Botnet hijacks web servers for DDoS campaign

May 12 - (Information Technology)

Researchers at Imperva have discovered an "experimental" botnet that uses around 300 hijacked Web servers to launch high-bandwidth **DDoS attacks**. The servers are all believed to be open to an unspecified security vulnerability that allows the attacker, who goes by the name "Exeman", to infect them with a tiny, 40-line Personal Home Page (PHP) script. This includes a simple Graphics Unit Interface (GUI) from which the attacker can return at a later date to enter in the IP, port and duration numbers for the attack that is to be launched. But why servers in the first place? **Botnets** are built from PCs and rarely involve servers. According to Imperva's chief technology Officer, they have no antivirus software and offer high upload bandwidth, typically 10 to 50 times that of a consumer PC. Are there disadvantages to this? There are simply fewer of them, the attacker needs to find vulnerable machines using PHP, and they appear to need manual control, although he did say that attacks could probably be automated using a separate script.
TechWorld : Botnet hijacks web servers for DDoS campaign

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

Fraud bazaar carders.cc hacked

May 18 - (Banking)

Carders.cc, a German online forum dedicated to helping criminals trade and sell financial data stolen through hacking, has itself been hacked. The once-guarded contents of its servers are now being traded on public file-sharing networks, leading to the exposure of potentially identifying information on the forum's users as well as countless passwords and credit card accounts swiped from unsuspecting victims. The breach involves at least three separate files being traded on Rapidshare.com: The largest is a database file containing what appear to be all of the communications among nearly 5,000 Carders.cc forum members, including the contents of private, one-to-one messages that subscribers to these forums typically use to negotiate the sale of stolen goods. Another file includes the user names, e-mail addresses and in many cases the passwords of Carder.cc forum users. A third file — which includes what appear to be Internet addresses assigned to the various Carders.cc users when those users first signed up as members — also features a breezy explanation of how the forum was compromised.
Krebs on Security: Fraud bazaar carders.cc hacked

Other Attacks articles:

- *May 10* – (Information Technology) ***TG Daily*: Hackers target WordPress in large-scale attack.** Hackers have reportedly targeted a number of Web sites powered by the popular WordPress platform. The attacks have affected sites hosted by various providers, including DreamHost, GoDaddy, Bluehost and Media Temple. In addition, other

[Return to top]

Personal Home Page (PHP) based management systems - such as Zen Cart eCommerce - have also been targeted in the ongoing cyber offensive.

- May 12 – (Telecommunications) ***The New New Internet*: Telecom DoS hides cyber crime.** The recent spike in unsolicited and mysterious telephone calls may be part of a new scheme to use telecommunications distributed denial of service (DDoS) attacks to distract individuals from ongoing cyber crime, the FBI warned recently. According to the FBI, cyber criminals are using telephone calls to mobile and land lines to distract victims from the attempts by criminals to empty their bank and trading accounts.
- *May 17* – (Health) ***IT Business Edge*: Security guard enters guilty plea for hacking employer's computers.** According to Computerworld, a former security guard has pleaded guilty to two counts of transmitting malicious code for hacking into his employer's computers while working the night shift at a Dallas hospital. He is a member of a hacking group known as the Electronik Tribulation Army and he installed the botnet code in an effort to take down a rival group's Web site.
- *May 19* – (Information Technology) ***The Register*: Man accused of DDoSing conservative talking heads.** Federal prosecutors have accused a man of carrying out a series of botnet offenses including attacks that brought down the Web sites of conservative talking heads. The suspect was an undergraduate student at the University of Akron in Ohio at the time of the distributed denial-of-service (DDoS) attacks, which lasted over a five-day period in March 2008, prosecutors alleged in court documents.
- *May 20*, – (Information Technology) ***The New New Internet*: Over 80 Chinese government Web sites hacked.** In China, 81 government Web sites were hacked from May 10 to May 16, according to a report by the National Computer Network Emergency Response Technical Team. This represents a drop in attacks by 35 percent from the previous week.

Data Breach/Information Gathering

Two-thirds of all phishing attacks generated by a single criminal group, researchers say.

May 12 - (Information Technology)

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

Like convenience stores and fast-food restaurants, **phishing** is no longer a mom-and-pop operation, according to a study released on May 12. A single crime syndicate dubbed "Avalanche" was responsible for some 66 percent of the phishing traffic generated in the second half of 2009, according to a report published by the Anti-Phishing Working Group (APWG). "This criminal enterprise perfected a system for deploying mass-produced phishing sites, and for distributing malware that gives the gang additional capabilities for theft," the study said. Avalanche successfully targeted some 40 banks and online service providers, as well as vulnerable or nonresponsive domain name registrars and registries, in the second half of 2009, according to APWG. Avalanche could be a successor to the "Rock Phish" criminal operation, which became notorious between 2006 and 2008, APWG said. Avalanche was first seen in December 2008, and was responsible for 24 percent of the phishing attacks recorded in the first half of 2009. "Avalanche uses the Rock's techniques but improves upon them, introducing greater volume and sophistication," it said. To speed its spread of attacks, Avalanche runs on a botnet and uses fast-flux hosting that makes mitigation efforts more difficult, APWG said.

DarkReading: Two-thirds of all phishing attacks generated by a single criminal group, researchers say

[Return to top]

May 2010

E-mail attack targets HR departments

May 13 - (Multiple Sectors)

A targeted attack aimed at human resources departments and hiring managers in the U.S. and Europe sent 250,000 e-mails during a four-hour period May 12. Researchers at Websense Security Labs discovered the attack, which included the subject line "New resume" and came with a ZIP file attachment and what appeared to be a picture file. When opened, the files spreads bot malware and, ultimately, fake antivirus software. "From what the Websense Security Labs has ascertained, the e-mail campaign would be most relevant to HR departments and managers considering hiring. Employees in these types of roles would most likely be encouraged to view the attachments," said a senior manager of security research for Websense Security Labs. An executable inside the ZIP file contains the Oficla bot, according to the researchers. The malware issues a warning message that the victim's PC is "infected," and then it downloads the Security Essentials 2010 fake AV program. The researcher said the attackers appear to be trying to make money both by selling fake AV, and by building out a botnet. "

DarkReading: **E-mail attack targets HR departments**

Macau resident convicted in U.S. of illegal defense exports

May 12 - (Telecommunications; Defense Industry Base)

A Portuguese citizen who lives in Macau has been convicted of trying to illegally export communications, encryption, and GPS equipment used by the U.S. military and NATO forces, the Department of Justice said May 12. He was convicted by a federal jury in San Diego May 11 of trying to export defense articles to Macau and Hong Kong without a license. He was arrested in Atlanta in June 2009. The Justice Department did not mention the ultimate destination for the equipment the suspect was seeking, but Wired magazine quoted a government affidavit in the case as saying he was acting at the direction of Chinese officials. The United States Department of Justice reported that following a five-week trial, a federal jury in Massachusetts found two Chinese nationals, one of whom resided in the United States, guilty of illegally conspiring to violate U.S. export laws, and illegally exporting electronic equipment from the United States to China, the Justice Department announced on May 17. Several Chinese military entities were among those receiving the exported equipment. The jury also convicted a Waltham, Massachusetts corporation, owned by one of the defendants, which procured the equipment from U.S. suppliers and then exported the goods to China through Hong Kong. The exported equipment is used in electronic warfare, military radar, fire control, military guidance and control equipment and satellite communications, including global positioning systems. The men were convicted of unlawfully exporting defense articles and Commerce controlled goods to China on numerous occasions between 2004 and 2007, and conspiring to violate U.S. export laws over a period of 10 years.

Agence France-Presse: **Macau resident convicted in U.S. of illegal defense exports**
See also, United States Department of Justice: **Two Chinese nationals convicted of illegally exporting electronics components used in military radar & electronic warfare**

Google Street View accidentally collected user data via WiFi

May 16 - (Information Technology)

Google May 14 said it will no longer collect WiFi data after discovering that its Street View cars unwittingly collected personal information from citizens' networks, a violation of pri-

[Return to top]

vacy sure to inflame leaders of countries already wary of Google's data-collection practices. The search engine initially said in April that its Street View cars did not collect data that people share between WiFi networks and computers, although the cars did collect WiFi network names and router addresses. Google learned after conducting a data audit on behalf of the German government that this was incorrect. "It's now clear that we have been mistakenly collecting samples of payload data from open (i.e. non-password-protected) WiFi networks, even though we never used that data in any Google products," wrote a senior vice president of engineering and research. Payload data can include user e-mails, passwords and Web browsing activity, data the sanctity of which Internet companies such as Google, Yahoo and Microsoft swear to protect. Germany, the United States, Britain and France were among the countries where Google collected this data. A consumer group has called on the U.S. Federal Trade Commission (FTC) to investigate Google and the Wi-Fi sniffing has prompted a class-action lawsuit that could force the company to pay up to $10,000 for each time it snatched data from unprotected hotspots, court documents show.
eWeek: **Google Street View accidentally collected user data via WiFi**
See also, IDG News Service: **FTC asked to investigate Google Wi-Fi 'snooping'**
See also, Computerworld: **Google hit with class-action lawsuit over Wi-Fi snooping**

Other Data Breaching/Information Gathering articles:

- May 10 – (Banking) ***The H Security*: Police apprehend Romanian phishing gang.** Romanian police investigators have exposed a gang of criminals who fraudulently gained online access to bank accounts and for months, continued to draw money from these accounts. The Romanian Directorate for Investigating Organized Crime and Terrorism (DIICOT) in Bucharest said that after conducting nationwide searches May 9, Romanian police questioned 28 suspects.
- May 13 – (Government Facilities) ***Krebs on Security:* Stolen laptop exposes personal data on 207,000 Army reservists.** A laptop stolen from a government contractor last month contained names, addresses and Social Security numbers of more than 207,000 U.S. Army reservists, Krebsonsecurity.com has learned.
- May 13 – (Banking) ***DarkReading:* Authorities arrest first suspect in massive identity-theft ring.** Indian police said May 12 that they have detained a Ukrainian man charged in the U.S. with stealing some 40 million credit and debit card numbers. He is one of 11 people wanted by the U.S. Justice Department in "the largest hacking and identity theft case ever prosecuted," which was filed in August 2008.
- May 18 – (Banking) ***Help Net Security*: Phishing page steals prepaid debit card account information.** Since pre paid debit cards are regularly used by low- to mid-income citizens, who really can not afford to lose small amounts of money, Symantec's revelation that there are phishing sites out there that are posing as the main Web site of a well-known prepaid debit-card service will provide an almost lifesaving warning.
- May 18 – (All Sectors) ***IDG News Service:* FTC targets privacy concerns related to copy machines.** The U.S. Federal Trade Commission has begun contacting copy machine makers, resellers and office-supply stores about privacy concerns over the thousands of images that can potentially be stored on the machines' hard drives. The FTC chairman, in a letter to a U.S. Representative, said the agency has been working to alert copy-machine manufacturers and sellers of the privacy risks of the information that many copy machines store on their hard drives.

[Return to top]

- May 20 – (Information Technology) ***Wired.com*: School spy program used on students contains hacker-friendly security hole.** A controversial remote administration program that a Pennsylvania school district installed on student-issued laptops contains a security hole that put the students at risk of being spied on by people outside the school, according to a security firm that examined the software.
- May 18 – (Information Technology) ***The Register*: Transit site coughs up private info for 168,000 passengers.** Dutch authorities have shuttered a transit website after a hacker demonstrated it gave him access to addresses, birthdates, and other sensitive information belonging to some 168,000 passengers. According to an article in Webwereld magazine, the site is wide open to simple attacks that allow hackers to read, change, or delete passengers' personal information. The glitch that exposed the database to the world is a **SQL injection**.

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

Threats and Vulnerabilities

Schapiro: SEC may push for market circuit-breakers

May 18 – (Banking and Finance)

The Securities & Exchange Commission chairwoman said May 18 she expects her agency to issue preliminary findings on its inquiries into the "flash crash" on May 6, when the Dow Jones Industrial Average plunged nearly 1,000 points. The "flash crash" saw bellwethers such as Procter & Gamble Co. plunge nearly 40 percent in seconds. Speaking via a video link to the CFA Institute's 2010 Annual Conference in Boston, the chairwoman said that her agency, in conjunction with the Commodity Futures Trading Commission, has been "looking at a number of issues that can be remediated quickly, even before the exact cause of the crash is known." Among the likely recommendations, she said is the implementation of circuit-breakers or "speed bumps" that give stocks "the opportunity to pause throughout all markets." Previously on May 11, the U.S. House of Representatives Financial Services Subcommittee on Capital Markets failed to pinpoint any single cause for the stock market plummet. The committee held several hearings during which members questioned the heads of the U.S. Securities and Exchange Commission (SEC), New York Stock Exchange and Nasdaq in an attempt to gain some insight on what caused the precipitous drop.

Marketwatch: Schapiro: SEC may push for market circuit-breakers
See also, Computerworld: House Committee fails to find smoking gun on market plunge
See also, Marketwatch: Stock sell-off leads to probe of faulty trade

How an unfixed Net glitch could strand you offline

May 6 - (Telecommunications)

A member of the "hacker think tank" called the L0pht told Congress in 1998 that he could use a **Border Gateway Protocol (BGP) vulnerability** to bring down the Internet in half an hour by misdirecting data. In recent years, the expert — who now works for the Pentagon's Defense Advanced Research Projects Agency — has said the exploit would still work. However, it would likely take a few hours. In 2003, the Presidential Administration concluded that fixing this flaw was in the nation's "vital interest." Fast forward to 2010, and very little has happened to improve the situation. The flaw still causes outages every year. And while there is some progress being made, there is little industry-wide momentum behind efforts to introduce a permanent remedy. Data carriers regard the fallibility of the routing system as the price to be paid for the Internet's open, flexible structure. Internet growth has also increased the risks exponentially.

BGP Vulnerability: A vulnerability exists in the reliance of the BGP on the Transmission Control Protocol (TCP) to maintain persistent sessions. Sustained exploitation of this vulnerability could lead to a denial-of-service condition affecting a large segment of the Internet community. Normal operations would most likely resume shortly after the attack stopped. (US-CERT)

[Return to top]

May 2010

Kernel Driver Hooks: The essential center of a computer operating system, the core that provides basic services for all other parts of the operating system. Hooks, or hooking, is an area in the message-handling mechanism of a computer system in which an application can install a subroutine to monitor the message traffic in the system. This application can also process certain kinds of messages before they can reach the targeted window procedure. Rootkits often use hooking techniques. (SANS and Computer Dictionary)

Associated Press: How an unfixed Net glitch could strand you offline

New attack tactic sidesteps Windows security software

May 11 - (Information Technology)

A just-published attack tactic that bypasses the security protections of most current anti-virus software is a "very serious" problem, an executive at one unaffected company said May 11. On May 5, researchers at Matousec.com outlined how attackers could exploit the **kernel driver hooks** that most security software uses to reroute Windows system calls through their software to check for potential malicious code before it is able to execute. Calling the technique an "argument-switch attack," a Matousec-written paper spelled out in relatively specific terms how an attacker could swap out benign code for malicious code between the moments when the security software issues a green light and the code actually executes. "This is definitely very serious," said vice president of engineering at Immunet, a Palo Alto, Calif.-based anti-virus company. "Probably any security product running on Windows XP can be exploited this way." According to Matousec, nearly three-dozen Windows desktop security titles, including ones from Symantec, McAfee, Trend Micro, BitDefender, Sophos, and others, can be exploited using the argument-switch tactic.

Computerworld: New attack tactic sidesteps Windows security software

Twitter-controlled botnets come to the unwashed masses

May 13 - (Information Technology)

A security researcher has unearthed a tool that simplifies the process of building bot armies that take their marching orders from specially created Twitter accounts. TwitterNet Builder offers hackers a point-type-and-click interface that forces infected PCs to take commands from a Twitter account under the control of attackers. Bot herders can then force the infected machines to carry out denial-of-service attacks or silently download and install software with the ease of their Twitter-connected smartphones. "All in all, a very slick tool and no doubt [hackers] everywhere are salivating over the prospect of hitting a website with a DDoS from their mobile phones," a researcher with anti-virus provider Sunbelt Software wrote. TwitterNet Builder requires accounts to be public, so spotting people who use the software is fairly straightforward.

The Register: Twitter-controlled botnets come to the unwashed masses

Car hackers can kill brakes, engine, and more

May 14 - (Critical Manufacturing)

University researchers have taken a close look at the computer systems used to run today's cars and discovered new ways to hack into them, sometimes with frightening results. The security researchers said that by connecting to a standard diagnostic computer port included in late-model cars, they were able to do some nasty things, such as turning off the brakes, changing the speedometer reading, blasting hot air or music on the radio, and locking passengers in the car. In a late 2009 demonstration at a decommissioned airfield in Blaine, Washington, they hacked into a test car's electronic braking system and prevented a test driver from braking a moving car — no matter how hard he pressed on the brakes. In other tests, they were able to kill the engine, falsify the speedometer reading, and automatically lock the car's brakes unevenly, a maneuver that could destabilize the car traveling at high speeds. They ran their test by plugging a laptop into the car's diagnostic system and then

[Return to top]

controlling the car's computer wirelessly, from a laptop in a vehicle riding next to the car.
IDG News Service: Car hackers can kill brakes, engine, and more

Web browsers leave 'fingerprints' as you surf

May 18 - (Information Technology)

An overwhelming majority of Web browsers have unique signatures — creating identifiable "fingerprints" that could be used to track someone as they surf the Internet, according to research by the Electronic Frontier Foundation (EFF). The findings were the result of an experiment EFF conducted with volunteers who visited a Web site that anonymously logged the configuration and version information from each participant's operating system, browser, and browser plug-ins — information that Web sites routinely access each time one visits — and compared that information to a database of configurations collected from almost a million other visitors. EFF found that 84 percent of the configuration combinations were unique and identifiable, creating unique and identifiable browser "fingerprints." Browsers with Adobe Flash or Java plug-ins installed were 94 percent unique and trackable.
Help Net Security: Web browsers leave 'fingerprints' as you surf

Iranian cyber army second largest in the world, claims Iranian commander

May 21 - (All Sectors)

After hacking Twitter and various Iranian Web sites and engaging in a cyber war with China, the Iranian Cyber Army is said to be looking at the Revolutionary Guards for direction, according to a senior Revolutionary Guards Corps commander. Fars news agency reports that the commander of the Ali Ebn-e Abi Taleb Guards in Qom, said May 20 that the Revolutionary Guards has been successful in establishing a cyber army and "today the cyber army of the Revolutionary Guards is the second largest cyber army in the world." The commander also claimed the objective of the Iranian Cyber Army is "to prevent the destruction of Iran's cultural and social system" and added the "cyber army of the Revolutionary Guards is a force to reckon with in this arena." The Iranian Cyber Army has not been officially claimed by any group. Last year, Defense Tech, a U.S. military and security organization announced that the Iranian Cyber Army belongs to the Revolutionary Guards of Iran.
The New New Internet: Iranian cyber army second largest in the world, claims Iranian commander

Other Threats and Vulnerabilities stories:

- May 3 – (All sectors) ***DarkReading*: New IM worm spreading fast.** A smiley-faced Instant Message (IM) with a photo link posing as if it is from someone on a user's buddy list is actually spreading a worm on Yahoo Instant Messenger: The IM ultimately delivers a worm that allows an attacker to take over the victim's machine, and to spread the worm to people on the victim's contact list.
- May 19 – (International) ***CSO:* Expert: Skype worm no cause for panic.** Security research firm Bkis earlier in May warned of a vicious virus targeting both Skype and Yahoo! Messenger. The owner of the Web site skypetips.com and author of 'Skype Me! From Single User to Small Enterprise and Beyond ,' spoke to CSO earlier in 2010 about Skype's benefits and challenges in the business environment. According to the owner and author it is not Skype's fault for this attack and there is no need for panic.
- May 10 – (Information Technology) ***IDG News Service:* Windows 7 'compatibility checker' is a Trojan.** Scammers are infecting computers with a Trojan horse program

[Return to top]

disguised as software that determines whether PCs are compatible with Windows 7. The attack was first spotted by BitDefender May 9 and is not yet widespread; the antivirus vendor is receiving reports of about three installs per hour from its users in the U.S. But because the scam is novel, it could end up infecting a lot of people due to the interest in Windows 7.

- May 18 – (Information Technology) ***Websense:*** **Zeus is forwarding Adobe updates again.** Websense Security Lab ThreatSeeker Network has detected a new batch of malicious e-mails containing Zeus payloads. This campaign is very similar to another which Adobe reported on around the end of April with the only different being the social engineering tricks on this campaign have gotten considerably better.
- May 19 – (Information Technology) ***IDG News Service*****: Microsoft chases 'click laundering'.** Microsoft said it has uncovered a new kind of click fraud, filing two lawsuits against people it said are using the scam. One of the suits, filed in the U.S. District Court for the Western District of Washington, accuses the Web site RedOrbit.com and the site's president of using click laundering, a term Microsoft came up with to describe a new way of boosting the number of clicks on advertisements on a Web site. Microsoft accuses RedOrbit, which was once an approved site on its AdCenter network, of using botnets and so-called parked sites to dramatically drive up the number of clicks on ads on the RedOrbit site. But rather than simply use the botnets and sites to direct clicks to ads on RedOrbit.com as fraudsters commonly do, RedOrbit directed the traffic to its own servers where it scraped out the traffic-referring information and replaced it with code that made it look like the traffic came directly to the approved RedOrbit site, Microsoft said.
- May 23 – (International) ***PC World*****: Bugnets could spy on you via mobile devices.** Imagine an individual sitting in a cafe discussing the details of a business proposal with a potential client. Neither the individual nor the client has a laptop; they are just two people having a conversation. But unbeknownst to either, someone half a world away is listening to every word they say. Later, as the individual leaves, they receive a text message referring to the proposal and demanding money in exchange for silence. Recent research from two universities suggests that such a remote-eavesdropping scenario may soon be possible.
- May 21 – (International) ***DarkReading:*** **New threat for wireless networks: Typhoid adware.** There is a potential threat lurking in your Internet cafe, say University of Calgary computer science researchers: Typhoid adware. Typhoid adware works in similar fashion to Typhoid Mary, the first identified healthy carrier of the typhoid fever that spread the disease to dozens of people in the New York area in the early 1900s. Typically, adware authors install their software on as many machines as possible. But Typhoid adware hijacks the wireless access point and convinces other laptops to communicate with it instead. Then the Typhoid adware automatically inserts advertisements in videos and Web pages on hijacked computers, the researchers said. Meanwhile, the carrier sees no advertisements and does not know they are infected, just like a symptomless Typhoid Mary.
- May 25 – (International) ***The New New Internet*****: Researcher finds new type of phishing attack.** A researcher has found a new method for carrying out phishing attacks "that takes advantage of the way that browsers handle tabbed browsing and enables an attacker to use a script running in one tab to completely change the content in another tab," according to ThreatPost.

[Return to top]

- May 25 – (International) ***The Register*****: Looking for code work? Write fake anti-virus scripts.** A scareware purveyor has brazenly advertized for recruits on a mainstream job market website. A job ad on Freelancer.com offers work for a coder prepared to turn his hand to the creation of fake anti-virus website redirection scripts. However, prospective applicants are warned not to expect a big payday -- the budget for the whole project is between $30 and $250. The market for scareware is booming. Individuals involved in the business are increasingly adopting the business structures of mainstream security firms - even to the point of running call centers designed to persuade people not to try to apply for refunds, and recruitment programs.

Policy, Legislation and Governance

Lawmakers unveil online privacy bill

May 4 - (Government Facilities)

Two U.S. lawmakers have released a draft bill that would require companies that collect personal information from customers to disclose how they collect and share that information, but several privacy and consumer groups said the proposal would legalize current privacy violations online. The draft legislation, released on May 3 by a Virginia Democrat, and, a Florida Republican, would apply to information collected online and off. The bill would require companies collecting personal information to allow customers to opt out of the collection, and would require companies to get permission before sharing customers' personal information with third parties.

Computerworld: **Lawmakers unveil online privacy bill**

Departments of Justice and Homeland Security announce 30 convictions, more than $143 million in seizures from initiative targeting traffickers in counterfeit network hardware

May 6 - (Information Technology)

Operation Network Raider, a domestic and international enforcement initiative targeting the illegal distribution of counterfeit network hardware manufactured in China, has resulted in 30 felony convictions and more than 700 seizures of counterfeit Cisco network hardware and labels with an estimated retail value of more than $143 million. In addition, nine individuals are facing trial and another eight defendants are awaiting sentencing. This operation is a joint initiative by the Federal Bureau of Investigation, U.S. Immigration and Customs Enforcement, and U.S. Customs and Border Protection working with the U.S. Department of Justice. On May 6, as a part of this joint initiative, a Saudi citizen who resides in Sugarland, Texas, was sentenced in the Southern District of Texas to 51 months in prison and ordered to pay $119,400 in restitution to Cisco Systems. A federal jury found him guilty on January 22 of charges related to his trafficking in counterfeit Cisco products. He purchased counterfeit Cisco Gigabit Interface Converters (GBICs) from an online vendor in China with the intention of selling them to the U.S. Department of Defense for use by U.S. Marine Corps personnel operating in Iraq.

Department of Justice: **Departments of Justice and Homeland Security announce 30 convictions, more than $143 million in seizures from initiative targeting traffickers in counterfeit network hardware**

NATO should tool up for cyber war, say globo-bigwigs

May 18 - (Government Facilities; Multiple Sectors)

[Return to top]

May 2010

The North Atlantic Treaty Organization (NATO) believes a conventional military attack on its members is unlikely in the future, but that some form of cyber-attack is one of three most probable dangers facing the alliance. The organization is the midst of finding itself a new purpose. A group of bigwigs have been appointed to find "a New Strategic Concept". NATO has gone through several changes since its creation in the wake of the Second World War as a defensive alliance against the Soviet Union. Although NATO said the possibility of conventional military attack could not be ignored, it is more likely to face an attack by ballistic missile, a terrorist attack or a cyber attack. Dealing with cyber attacks will require more cooperation with the European Union, the experts conclude, because the EU has more expertise in dealing with such attacks. The report warns: "The next significant attack on the Alliance may well come down a fiber optic cable. Already, cyber attacks against NATO systems occur frequently, but most often below the threshold of political concern." It recommends a major effort to increase monitoring of NATO's critical network in order to find and fix vulnerabilities.
The Register: **NATO should tool up for cyber war, say globo-bigwigs**

House panel approves bipartisan bill to overhaul cybersecurity

May 20 - (Government Facilities)

A House committee on May 20 approved by voice vote a bill that would overhaul federal cyber security laws to install a permanent cyber czar and chief technology officer, ensure continuous monitoring of networks, and do away with paperwork requirements that some said distracted managers from securing computer systems. "This has truly been a bipartisan effort. This is a very good bill," said a New York representative who is the chairman of the House Oversight and Government Reform Committee. The 2010 Federal Information Security Amendments Act (H.R. 4900) aims to bolster the government's defenses against cyber attacks that have grown in number and intensity since the original information security law was enacted almost a decade ago.
Nextgov: **House panel approves bipartisan bill to overhaul cybersecurity**

DHS tries sharing cyber threat data differently

May 14 - (All Sectors)

The Homeland Security Department is testing an approach that could change the way the government secures its computer networks. DHS and the Defense Department are in the middle of a pilot program with financial services companies to share cyber threat data in real time from each of their networks and to review intrusions and activity on their networks. "This is an opportunity for us to really look at data across government and industry," says the DHS's assistant secretary for cybersecurity and communications at the 37th Annual Communications and Computer Association's Washington Caucus on May 13. "The pilots are moving us in the direction of being more operational. The end goal is to reduce risk. We are trying to find ways to information share that is operationalized and actually helps both government and industry reduce the amount of risk involved." A second pilot focuses on letting cleared personnel from companies view secret or classified threat data at state fusion centers.
Federal News Radio 1500 AM: **DHS tries sharing cyber threat data differently**

[Return to top]

Other Threats and Vulnerabilities stories:

- May 5 – (Government Facilities) ***Federal Computer Week*****: Cloud security: Feds on cusp of change.** The federal government is on the cusp of fundamental changes in the way it manages information-technology security risks, but those risks will grow more complicated as agencies begin embracing on-demand computing, according to a panel of public-sector, cloud-computing experts. The conference, on May 4, was sponsored by 1105 Government Information Group covering such topics as cloud computing, knowledge management and open-government innovations.
- May 11– (Telecommunications) ***Federal News Radio:*** **FCC to establish cyber certification program.** The Federal Communications Commission (FCC) wants to establish a cybersecurity certification program for private sector telecommunications networks. In a Federal Register notice released May 11, the agency says the undertaking would be voluntary for broadband and other communication service providers.
- May 13 – (Multiple Sectors) ***Homeland Security NewsWire:*** **Cybersecurity summit pays little attention to control system's security.** Despite threats of infrastructure attacks, scant attention was paid to control systems during a global security conference. As online attacks increase in severity and reach, targeting everyone from Google to the Pentagon, leading security experts and government officials met last week in Dallas at the EastWest Institute's first annual Cybersecurity Summit.
- May 17 – (Government Facilities) ***IDG News Service:*** **Survey: Gov't agencies use unsafe methods to transfer files.** Employees at many U.S. government agencies are using unsecure methods, including personal e-mail accounts, to transfer large files, often in violation of agency policy, according to a survey.
- May 19 – (Banking and Finance) ***SC Magazine:*** **US regulators form plans to encourage banks to better protect customers from online fraud.** A panel of regulators in the U.S. are drafting plans to force banks to protect their customers better from a surge in online account fraud. According to a report in the Financial Times (FT), a panel with representatives from the FDIC, the Federal Reserve System and other agencies is reacting to the rapid evolution of malicious computer programs designed to drain accounts.
- May 21 – (Transportation) **Aviation Week: FAA brass pushes NextGen.** The Federal Aviation Administration's (FAA) biggest guns — current and past — turned out to urged the swift implementation and funding of NextGen, the satellite-based, air-traffic management system, at Aviation Week's "NextGen ahead" symposium in Washington, D.C.
- May 18 – (Government Facilities) **Homeland Security Newswire: U.S. Air Force shifts 30,000 troops to "cyberwar front lines".** The USAF has assigned 30,000 to cyberwarfare specialties; 3,000 will become cyberspace officers. This is close to a third of the number of U.S. troops deployed in Afghanistan. The Air Force Times reports that 27,000 enlisted airmen and women are now classified as cyberspace specialists.

Reports and Publications

With cybersecurity becoming an increasingly visible issue, Congress has added its voice to the growing discussion with a number of bills currently pending.

- Data Breach Legislation (S. 139): This bill would make a national data breach to standardize the 46 State data breach laws.
- Data Accountability and Trust Act (H.R. 2221): Recently voted down in the House, this

[Return to top]

bill requires ISPs to inform users when they become infected.

- Data Breach Legislation (S. 139): This bill would make a national data breach to standardize the 46 State data breach laws.
- International Cybercrime Reporting and Cooperation Act (S. 1438 and H.R. 4692): These bills, among other things, authorizes the State Department to create a cybersecurity Ambassador.
- Cybersecurity Enhancement Act (H.R. 4061): This bill passed the House earlier this year and gives NIST additional responsibility and supports research and development in the cyber realm.
- FISMA II (S. 921): This bill is designed to update the current FISMA guidelines which are widely seen as compliance driven. Instead, the new bill will make the guidelines performance based, based upon the tool implemented by John Streufert at the Department of State.
- Cybersecurity Act of 2009 (S. 773): "The bill combines audits, industry-developed and government-backed standards, increased information-sharing, and other mechanisms to bolster private sector cybersecurity," an analyst writes.
- The Grid Reliability and Infrastructure Defense Act (H.R. 5026): "The bill amends the Federal Power Act and directs the Federal Energy Regulatory Commission to protect the electric transmission and distribution grid from vulnerabilities," an analyst writes.
- Energy and Water Appropriations Act 2010 (Law): "It appropriates additional funds for Cybersecurity: $46.5 million for energy delivery cyber security, an increase of $34.5 million from 2009, to develop secure grid technologies as cyber attacks increase worldwide and the grid becomes increasingly network-connected," an analyst writes.

Government Computer News: **Federal mortgage watchdog agency struggles with its information security** The Federal Housing Finance Agency has not fully implemented an information security program, resulting in weaknesses in its information technology security, according to the Government Accountability Office.

M86 Security: **M86 Security Labs report details Web exploit kits** M86 Security Tuesday announced the release of their latest security report which details the rise of distributed, monetized "exploit" kits, with M86 Security Labs counting more than a dozen new attack kits being launched in just the last six months.

Help Net Security: **Security risks of web application programming languages** A new WhiteHat report examined the security of specific programming languages. Nearly 1,700 business-critical websites were evaluated to provide organizations with insight into the relative security of the development frameworks they deploy, and the associated vulnerabilities that put them at risk.

Help Net Security: **U.S. federal data security vulnerabilities** Data-security vulnerabilities continue within U.S. federal agencies due to employees' use of unsecure methods to exchange information, such as File Transfer Protocol (FTP) — despite the Secure File Sharing Act, which the U.S. House of Representatives passed March 24, 2010 to prevent government employees from using peer-to-peer file-sharing software, including FTP.

[Return to top]

May 2010

News Radio Survey: Most federal CISOs not moving to cloud yet The second annual State of Cybersecurity from the Federal CISO's Perspective survey has been released. (ISC) 2 and Cisco, along with Garcia Strategies, put together their second annual report based on questions answered by a broad cross-section of U.S. government chief information security officers.

ComputerWorld: P2P networks a treasure trove of leaked health care data, study finds Nearly eight months after new rules were enacted requiring stronger protection of health care information, organizations are still leaking such data on file-sharing networks, a study by Dartmouth College's Tuck School of Business has found.

PC Advisor UK: USB worm named biggest PC threat A worm that is spreading via USB flash drives has been named the biggest security threat to PC users by McAfee. According to the security vendor's Threats Report: First Quarter 2010, an AutoRun-related infection was also the world's third biggest PC threat during the first three months of the year, while the rest of the top five biggest PC threats were made up of password-stealing Trojans.

Nextgov: IG: Poor controls over access to IRS portal put taxpayer data at risk The Internal Revenue Service (IRS) failed to implement adequate security measures to protect sensitive data that tax professionals entered into a Web portal, according to a Treasury inspector general for Tax Administration report released on May 17.

Technology Review: Commercial quantum cryptography system hacked When it comes to secure messaging, experts say nothing beats quantum cryptography, a method that offers perfect security. Messages sent in this way can never be cracked by an eavesdropper, no matter how powerful, according to experts. At least, that is the theory. On May 17, three researchers at the University of Toronto in Canada said they have broken a commercial quantum cryptography system made by the Geneva-based quantum technology startup ID Quantique, the first successful attack of its kind on a commercially available system.

eSecurity Planet: Malware is South America's new growth industry Malware syndicates in China have been implicated in a number of recent high-profile, targeted cyber attacks against American companies and organizations, but the latest data from security software vendor Zscaler indicates a new and equally dangerous threat is emerging in South and Central America according to the first-quarter "State of the Web" report by Zscaler.

CSO: Business continuity, not data breaches, among top concerns for tech firms 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 largest U.S. public technology companies. The research, released by BDO, a professional ser-

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]