

{ bytes in brief }

LAW AND TECHNOLOGY NEWS MONTHLY

EDITORS: Sharon D. Nelson, Esq. and John W. Simek
ASSOCIATE EDITOR: Jason R. Foltin EDITOR EMERITUS: G. V. Nelson



© 2010 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

ISSUE 152 – JANUARY 2010

PLEASE NOTE: The URLs referenced in Bytes frequently link to newspapers and other current news sources. These links may fail over time. [Click here to visit Sensei's home page at www.senseient.com](http://www.senseient.com)

ADVANCED ANTIVIRUS

On November 25th, PCWorld.com reported that it had reviewed several of the top security programs in light of today's vast threatscape of duplicitous Trojan horses, invisible exploits, and slithering worms. To rate the programs, the review first determined the products' detection rates for malware both known and brand-new. Similarly, the PCWorld.com researchers also measured scan speed and disinfection performance, along with the rate of false alarms. In addition to looking into those features that are designed to protect the average consumer, the review also examined each app's user interface and simulated a variety of scanning scenarios to ensure it was user friendly. According to the research performed, G Data AntiVirus 2010 did the best job at malware detection, both in traditional, signature-based tests and in proactive protection tests that gauge how well an application can detect new malware without a full signature. And although the program has a straightforward interface, it also asks the most questions and thus may be better suited for more technically oriented individuals. Finishing a close second was Symantec's Norton Anti-Virus 2010, with its smooth and simple features. In general, the researchers found that the application did a good job of blocking and removing malware, though it trailed G Data in one type of proactive protection. With its appealing features and more than adequate malware protection abilities, Norton appears to be a good choice for computer owners who want a minimum of fuss from the software they use. An article discussing how to pick the right anti-virus software may be found at http://www.pcworld.com/article/182545/picking_the_right_security_software.html

Full reviews of the top five paid antivirus products may be found at http://www.pcworld.com/article/182539/advanced_antivirus.html

Reviews of the top free antivirus products may be found at http://www.pcworld.com/article/170587/can_you_trust_free_antivirus_software.html

IBM STAFFER POSTS PICS ON FACEBOOK, LOSES BENEFITS

On November 24th, the Associated Press reported that 29-year-old IBM employee Natalie Blanchard lost her sick-leave benefits after her insurer, Manulife Financial, found photos on her Facebook page that the company alleged refuted her claims of depression and the inability to work. The photos Blanchard posted were of her at a Chippendales show, a birthday party and on a beach holiday vacation. According to Manulife, the Facebook photos demonstrated that Blanchard was cheerful and happy rather than depressed and thus was able to work; a fact which resulted in no more sick-leave payments. However, Blanchard has explained that she went on the three trips to help cure her bout with depression. Further, she noted that she did so only after consulting with her psychiatrist. Manulife has confirmed that it does use social-networking sites to check up on its customers, but noted that it would not terminate a valid claim based solely on information published on social networking sites. The case will be heard in the Quebec Superior Court on December 8th. Until then, a copy of the story may be found at http://news.cnet.com/8301-17852_3-10404633-71.html

SPAM 'GODFATHER' GETS 51 MONTHS IN PRISON

On November 16th, the man dubbed the “Godfather of Spam,” Alan M. Ralsky, was sentenced to 51 months in prison. The sentence came after a federal grand jury named Ralsky and 10 other co-conspirators from China, Canada, Hong Kong and Russia in a 41-count indictment for wire fraud, mail fraud, money laundering and violations of the CAN-SPAM Act. According to the government, Ralsky was a top promoter of pump-and-dump schemes, schemes in which fraudsters buy up a bunch of low-priced microcap stock, blast out millions of spam e-mails touting it as a hot buy and then dump their shares as soon as the share price ticks up from all of the spam respondents buying into the scam. Along with his four plus year prison stint, Ralsky will be subject to five years of supervised release and will forfeit \$250,000 the government seized from him in December 2007. The Ralsky decision was just one of the more recent notable cyber justice cases. In a separate action, Neil Felahy pleaded guilty in a case involving the sale of counterfeit high-tech computer parts to the U.S. military. Prosecutors alleged that Felahy and several co-defendants sold the knockoff parts to the U.S. Navy using a number of California companies, taking trademark-branded integrated circuits and other computer components, grinding off the original markings, re-branding them with other trademarks and passing the devices off as military grade. Expected to be sentenced sometime next year, Felahy faces up to 51 months in prison and more than \$2 million in fines. A copy of the story may be found at http://voices.washingtonpost.com/securityfix/2009/11/spam_godfather_alan_ralsky_get.html



POLICE ARREST EXEC FOR NOT USING TWITTER

On November 23rd, CNET News reported that the senior vice president of Island Def Jam Records, James A. Roppo, was arrested after failing to comply with a request by the Nassau County police to send out a Twitter message in an attempt to disperse an unruly crowd. The request came after thousands of fans packed into Roosevelt Field mall to see teen sensation Justin Bieber and get their albums signed. Police soon became concerned that the crowd was becoming unmanageable and turned to Roppo for help. According to Kevin Smith of the Nassau County Police, Roppo’s non-cooperation put lives in danger and the public at risk and, as a result, he could face a litany of potential charges including criminal nuisance, endangering the welfare of a minor, and obstructing government administration. Further information may be found at http://news.cnet.com/8301-17852_3-10403864-71.html



SURVEY: ONE-THIRD OF YOUTHS ENGAGE IN SEXTING

On December 3rd, Wired.com reported that MTV and the Associated Press have released a survey highlighting where the younger generation currently stands on sexting and digital abuse. And the results are shocking. Close to a third of youths admitted that they’ve engaged in sexting – an activity involving sending sexually explicit messages or e-mailing a photo or video of themselves in the nude or being the recipient of such images. Of those admitting to distributing suggestive photos of themselves, about 61 percent reported that they did so only after being pressured into the act. In general, girls were more likely to share a naked image of themselves than boys and those individuals who were already sexually active were much more likely to send an image than those who were not. Further, while the majority of the respondents sent the images to a significant other or a person of romantic interest to them, alarmingly, 29 percent said they shared naked images of themselves with someone they knew only online. In addition, the survey also revealed that close to 50 percent of those who responded have been the victims of some form of digital abuse, the most common type being a smear campaign. The survey also showed a correlation, though not necessarily a causation, between digital abuse and emotional distress. Those targeted by abuse were found to be almost three times as likely to report that they have contemplated suicide or dropping out of school. The survey is just one aspect of a multi-faceted campaign aimed at educating teens and college-aged students about safe and appropriate digital behavior. MTV will also air a half-hour news special on the sexting and will be launching a contest called “Redraw the Line Challenge” to develop projects to address digital abuse, such as web-based tools or games, that will help educate people. A copy of the report may be found at http://www.athinline.org/MTV-AP_Digital_Abuse_Study_Full.pdf



AT&T DROPS VERIZON 3G LAWSUIT BUT BAD PUBLICITY LIVES ON

On December 2nd, ZDNet.com reported that while AT&T has dropped its lawsuit against Verizon Wireless for its allegedly misleading ad campaign, the bad publicity lives on. Primarily, those who had questioned AT&T's decision to sue have argued that AT&T's biggest mistake was trying to squash the ad on the basis that it was misleading, instead of inaccurate. The company claimed that consumers were being misled into thinking that the maps in the ad represented all of AT&T's coverage, instead of just its 3G coverage. The problem was that the commercial, and the information in it, was not inaccurate. Rather, as Verizon said in response to the lawsuit, "The truth hurts." Making matters worse, a recent Consumer Reports article gave AT&T's overall cell phone voice quality a "poor" rating and suggested that consumers might love the iPhone but should expect to be disappointed with the call quality on the AT&T network. As one blogger explained, AT&T would have been better off launching its own ad campaign, or even spending some of that lawyer money beefing up its network instead of paying lawyers to file silly lawsuits. A copy of Verizon's motion in opposition of AT&T's request for a temporary injunction to block any more ads from being aired may be found at <http://i.zdnet.com/blogs/verizons-opp-to-motion-for-tro.pdf?tag=col1;post-27394>

EFF SUES FEDS FOR INFO ON SOCIAL-NETWORK SURVEILLANCE

On December 1st, the Electronic Frontier Foundation (EFF) filed a lawsuit against the CIA, the U.S. Department of Defense, the Department of Justice, and three other government agencies for allegedly refusing to release information about how they are using social networks in surveillance and investigations. The suit follows the EFF's request to more than a dozen federal agencies or departments in early October to provide records regarding federal guidelines on the use of social networking sites for investigative or data gathering purposes. According to the lawsuit, government officials have used Facebook to hunt for fugitives and search for evidence of underage drinking; researched the activities of an activist on Facebook and LinkedIn; watched YouTube to identify riot suspects; searched the home of a social worker because of Twitter messages regarding police actions he sent during the G-20 summit; and used fake identities to trick Facebook users into accepting friend requests. EFF maintains that it needs access to the information requested to help inform Congress and the public about the effect of such uses and purposes on citizens' privacy rights and associated legal protections. As one individual put it, social-networking sites are a part of everyday life. And while individuals may think that they are sharing private information with just their friends, government agencies are using the sites in ways that are not contemplated by citizens when they sign up as users. A copy of the complaint may be found at http://www.eff.org/files/filenode/social_network/social_networking_FOIA_complaint_final.pdf

FACEBOOK AND MYSPACE DELETE N.Y. SEX OFFENDERS

On December 1st, New York Attorney General Andrew Cuomo announced that more than 3,500 sex offenders from the state of New York have been removed from Facebook and MySpace. This latest wave of removals comes after the implementation of New York's new Electronic Securing and Targeting of Online Predators Act ("E-Stop"), which has made it easier for the sites to identify perpetrators from the Empire State. The E-Stop Law bans many registered offenders from using social-networking sites while on parole or probation and requires all registered offenders to disclose their e-mail addresses, screen names, and other Internet identifiers. That data is then provided to social networking sites like MySpace and Facebook to run against their user base. Currently, sex offender data is collected by the states and there is no official federal database; however, the federal Adam Walsh Act calls for such a database but it hasn't yet been fully funded. While Attorney General Cuomo praised Facebook and MySpace's cooperation, he went on to say that many other social-networking sites remain slow at adopting available new protections against sexual predators online. Additionally, it is important to note that the removal of sex offenders involves only registered sex offenders—individuals who have been caught and convicted—and does not include the countless numbers of individuals who have eluded prosecution. A copy of the story may be found at http://news.cnet.com/8301-19518_3-10406914-238.html

REPORT: HOW RISKY IS CLOUD COMPUTING?

On November 20th, a free report was released by the European Network and Information Security Agency (ENISA), which outlines the benefits and potential pitfalls of cloud computing. The report first noted that cloud computing provides several clear benefits: it's computing on tap, available instantly, commitment-free and on-demand. But for all its rewards, cloud computing does come with many risks. The number one issue holding businesses and individuals back is security. Though cloud-service providers promise 24-7 availability, data centers can and do go down. Further, security is out of the hands of the customer, who must place trust in the service provider. By entrusting data to the cloud, companies could face risks and challenges from regulatory audits. Finally, some cloud providers may not fully and properly delete data even if a customer requests it. According to the report, companies must perform risk assessments, compare different cloud providers to narrow the list and then obtain service-level assurances from selected providers, and specify which services and tasks will be handled by internal IT and which by the cloud provider. To assist in the process, the report included a checklist and detailed questions that customers can use when shopping for a cloud provider. A copy of the report may be downloaded at <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/>

NEW STUDY CALLS FOR CYBERSECURITY OVERHAUL IN U.S.

On December 3rd, YAHOO News reported that the Internet Security Alliance (ISA) has issued a report arguing that the U.S. government and private businesses need to overhaul cybersecurity and then suggesting that the government offer businesses new incentives to fix the various security problems. In the report, which was intended to be a response to President Obama's promise to increase cybersecurity efforts, the ISA called for permanent cybersecurity collaboration centers, new security standards for VoIP (voice over Internet Protocol) communications, and educational programs for corporate leaders. Further, while U.S. lawmakers have generally focused on implementing new regulations to combat cybercrime, this report focuses on changing the economics of cybersecurity. In fact, ISA's president Larry Clinton has stated that part of the problem is that many individuals and corporations don't see the benefits from greater cybersecurity efforts. All too often, he says, consumers don't worry when their credit cards are hacked, because credit card companies cover most of the loss, but all consumers end up paying for the losses in higher interest rates and fees. In his mind, regulations simply are not enough. As he puts it, cybersecurity is a "21st-century problem that's going to require a 21st-century solution." As such, the report suggested that Congress pass a law providing marketing and insurance benefits to companies creating new cybersecurity technology and standards. Moreover, it states that the U.S. government should also tie federal grants, loans and stimulus money to cybersecurity standards, and it should push for greater security in the technology products it buys. The report also explored ways to address malicious firmware embedded in hardware the government purchases from foreign suppliers. ISA believes that working with suppliers to improve their overall cybersecurity protections, would, in turn, reduce the potential for a malicious firmware nightmare. A copy of the report may be found at http://www.isalliance.org/images/stories/downloads_pdf/Implementing_the_Obama_Cyber_Security_Strategy.pdf

FACEBOOK ADOPTS NEW PRIVACY SETTINGS TO GIVE USERS MORE CONTROL OVER CONTENT

On December 9th, the social networking giant Facebook introduced its new privacy settings that are designed to provide users more control over what information they share and with whom. With the new program, Facebook members can customize just about every piece of data about them on the site; they can control who sees personal information such as age, name, gender and workplace, in addition to status updates and photos. In some cases, they can restrict access to photos to just one or two people or allow basic profile information to go out to the entire Web. However, some public interest groups are concerned that Facebook's recommended settings – which are also the default settings – will open up a user's account to almost anyone unless instructed otherwise. For example, under the default settings, status updates that were formerly limited to a user's network of friends will now be recommended for friends of friends. Additionally, the default setting for a user's profile information will be available for all who visit the site to view. Some have explained that while Facebook users will be able to choose the level of privacy they want; many people don't take the time to do so and may simply stick with the defaults. Thus, these individuals may be permitting others to view their account, when they might not want them to do so. When the change occurred, all Facebook users saw a pop-up window prompting them to adjust their settings or to stick with their old settings. A copy of the story may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/09/AR2009120904200.html>

HACKERS FIND A HOME IN AMAZON'S EC2 CLOUD

On December 12th, InfoWorld.com reported that security researchers have spotted the Zeus botnet running an unauthorized command and control center on Amazon's EC2 cloud computing infrastructure, marking the first time that Amazon's cloud has been used for this type of illegal activity. According to Don DeBolt, director of threat research with HCL Technologies, the hackers didn't do this with Amazon's permission, but rather, it is likely that they got onto Amazon's cloud infrastructure by first hacking into a Web site that was hosted on Amazon's servers and then secretly installing their command and control infrastructure. Additionally, DeBolt also stated that he believed the attack was more a target of opportunity than a target of choice. Generally speaking, in the past few years, law enforcement crack-downs and bad publicity have made it harder for hackers to host their malicious infrastructure in legitimate or even semi-legitimate datacenters, so they have moved to Web-based services. And while it wasn't the case here, many law enforcement officials have expressed concern that criminals might start using stolen credit cards to purchase cloud-based computing services from companies such as Amazon. The researchers' findings may be found at

<http://community.ca.com/blogs/securityadvisor/archive/2009/12/09/zeus-in-the-cloud.aspx>

HEARTLAND DATA BREACH LAWSUIT DISMISSED

On December 7th, the U.S. District Court for the District of New Jersey granted Heartland's motion to dismiss a lawsuit filed against Heartland Payment Systems over what is believed to be the biggest data breach in U.S. history. The suit was filed in January by shareholders who alleged that Heartland failed to adequately safeguard the compromised consumer data and did not notify consumers about the breach in a timely manner as required by law. The data breach occurred last year, but company officials explained that they only found evidence of the intrusion the week before they announced the breach and immediately notified law enforcement and credit card companies. In dismissing the suit, the court held that the Plaintiffs had not proved their allegations that Heartland executives knew the company had inadequate security and misled the public about it. A copy of the statement released by Heartland regarding the court's decision may be found at

<http://www.heartlandpaymentsystems.com/article.aspx?id=3031>

LA. FIRM SUES CAPITAL ONE AFTER LOSING THOUSANDS IN ONLINE BANK FRAUD

On December 4th, JM Test Systems, an electronic testing firm, filed suit against its bank, Capital One, alleging that the financial institution was negligent when it failed to stop hackers from transferring nearly \$100,000 out of its account earlier this year. In the lawsuit, JM Test has alleged that it first discovered that an unauthorized \$45,640 wire transfer had been made against its account to an account at Alpha-Bank in Moscow. After alerting Capital One, the bank issued it a new user name and password. However, thieves broke back into the account and initiated a batch of unauthorized payroll payments totaling \$51,556.44. JM Test has alleged that, although it notified Capital One of the fraud, the bank failed to stop the problem from escalating. Further, JM Test argued that Capital One violated its own online banking terms and conditions, which said that once a Capital One customer calls to report fraudulent activity, Capital One will close the affected customer's existing account to prevent further unauthorized charges. The lawsuit is just the latest challenge questioning whether banks are doing enough to protect customers from losses when a virus infection, phishing attack or hacker break-in compromises a company's online banking credentials. These cases may become more and more common. Some companies that have been victims of similar fraud have stated that they are weighing whether or not to sue their banks. According to David Johnson, a digital media lawyer, the banks cannot let this situation go on or people will start to lose confidence in them. He believes that if people start thinking they can lose real money when they deposit their money into the bank, that becomes a real business issue. A copy of the petition filed with the Louisiana court may be found at <http://voices.washingtonpost.com/securityfix/Cap%20One%20Petition%20-%20filed%20copy.pdf>

WOMAN SUES BURGER KING OVER SPAM TEXTS

On December 8th, CNET News reported that Elizabeth Espinal had filed a class-action lawsuit against the fast food giant Burger King for its alleged spam text messaging practices. Espinal has claimed that she received several texts encouraging her to try some of Burger King's menu items. After receiving the first, she allegedly texted back "stop," but she claims that the messages kept coming. The crux of the suit is likely to rely on Section 47 of the Telephone Consumer Protection Act, which prohibits unsolicited voice and text calls to cellular phones. What makes this suit interesting is the potential ramifications that might result if Espinal wins. Some have questioned whether a victory for Espinal would open the door to suits against anyone who texts an individual with unwanted inducements. Additionally, the damages claimed to be suffered has eyebrows being raised. Espinal and her lawyers seek \$5 million dollars for the actual harm caused and the aggravation suffered, leading some to suggest that she is a very sensitive human being, or that she believes that the only way to deal with an alleged harasser is to harass them right back. A copy of the story may be found at http://news.cnet.com/8301-17852_3-10411983-71.html

CISCO SEES SOCIAL NETWORKING AND BANKING SCAMS ON THE RISE

On December 15th, Cisco Systems released a report which showed that many different types of "old-school" cybercrime have been supplanted by new, more menacing forms of cyber attacks. Two major types of attacks that are really on the rise are social media and data-theft Trojans. These new attacks include the Koobface worm, which spreads via Facebook and Twitter. Koobface asks victims to look at a fake YouTube video, which ultimately leads to a malicious download. According to the report, Cisco estimates that the Koobface worm has infected more than 3 million computers. Security vendors such as Symantec expect these attacks to continue to grow. Another sneaky attack growing in popularity with cyber criminals is the Zeus password-stealing Trojan. According to Cisco, Zeus variants infected almost 4 million computers in 2009. Typically, the Zeus Trojan is used to hack into bank accounts. When hackers infiltrate the accounts, they then use their network of money mules to move the stolen funds out of the U.S. However, one old-school cybercrime – spam – may never be replaced. In fact, according to Cisco, spam volume is expected to rise between 30 and 40 percent next year, even though countries such as the U.S. have knocked some spammers offline. A copy of the report may be found at http://cisco.com/en/US/prod/collateral/vpndev/cisco_2009_asr.pdf

LAWSUIT SAYS ADS IN SOCIAL GAMES ARE SCAMMING PLAYERS

On December 7th, USA Today.com reported that a class-action lawsuit has been filed against Facebook and Zynga, a popular virtual-world game developer. The suit highlights the plight of Rebecca Swift, a 41-year-old self-employed resident of Santa Cruz, California, who was lured into accepting two "special offers" from advertisers to gain extra game credits for YoVille, a popular virtual-world game developed by Zynga. However, Swift has claimed she got more than she bargained for, claiming that more than \$200 dollars was illegally charged to her credit card after she signed up for the offers. While Zynga declined to comment on the lawsuit, Facebook stated the ads came from third parties and called the lawsuit frivolous and without merit. The lawsuit highlights the fuss over misleading social-gaming ads that have frustrated consumers and scared away legitimate advertisers, who do not want to be lumped with scamsters. Today, social games are the hot ticket, with millions of consumers flocking to social networking sites and elsewhere to play free games that test their wits and skills against friends. But, unbeknownst to some of the players, they may be required to sign up for special offers to gain entry to new levels of the game. And some of these offers automatically charge the game player. Making matters worse is the fact that there is no governing body to specifically regulate the social-gaming industry. A copy of the story may be found at http://www.usatoday.com/tech/gaming/2009-12-07-games07_ST_N.htm

Bytes in Brief[®] is a FREE monthly digest of Internet law and technology news delivered to you by e-mail. For members of the legal and business community interested in Internet law and technology developments, *Bytes in Brief* provides a synopsis of related news and links to sources with more expanded coverage. In the time it takes to drink a cup of coffee, *Bytes in Brief* is designed to make sure you are tracking major developments in this fast moving area.

If staying current in this field is important to you and you find yourself buried under unread magazines, newspapers and journals, *Bytes in Brief* can help you stay in touch without a major outlay of time or expense.

To subscribe, enter your e-mail address into the sign-up box below. It will take you offsite to the *Constant Contact* website, where our opt-in only list is maintained and updated. After you confirm your e-mail address, you will receive an e-mail asking for confirmation that you do wish to become a *Bytes In Brief* subscriber. Once you reply to that e-mail, you will be added to the subscription list.

Subscribe to *Bytes in Brief!*

Email:

Privacy by  **SafeSubscribe**SM
For Email Marketing you can trust

Copyright © 2010 Sensei Enterprises, Inc. All rights reserved.