The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

6 February 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, Sandia Labs

February 4, St. Joseph Health System – (Texas) **St. Joseph Health System confirms data security incident.** St. Joseph Health System confirmed February 4 that in December 2013 the organization experienced a data security breach that allowed unauthorized parties to gain access to a single server containing personal files of approximately 405,000 former and current patients, employees, and employees' beneficiaries. Once the health system learned of the breach the affected server was taken offline and additional security measures were put in place. Source: http://www.sacbee.com/2014/02/04/6127822/st-joseph-health-system-confirms.html

February 5, Help Net Security – (International) **Adobe Flash flaw exploited in the wild, update now.** Adobe issued an emergency patch for a critical vulnerability in its Flash Player for Windows, Linux, and OS X systems that could allow an attacker to gain remote control of targeted systems. The vulnerability is being actively exploited in the wild and users were advised to install the patch immediately. Source: http://www.net-security.org/secworld.php?id=16313

February 5, The Register – (International) **iFrame attack injects code via PNGs.** Researchers at Sucuri identified an iFrame injection attack in the wild that embeds malicious code in .PNG files. Source: http://www.theregister.co.uk/2014/02/05/iframe_attack_injects_code_via_pngs/

February 5, Softpedia – (International) **13 security holes fixed with the release of Firefox 27.** Mozilla released the newest version of its Firefox browser, closing a total of 13 security vulnerabilities, including 4 rated as high-impact. Source: http://news.softpedia.com/news/13-Security-Holes-Fixed-with-the-Release-of-Firefox-27-424025.shtml

Even North Korea Rips Off Apple: Look at Kim Jong Un's New Operating System
BetaBeat, 4 Feb 2014: For those lucky enough to have computers in North Korea, their official operating system created by the government is about to get a sleek new update. Although it wasn't announced in a flashy keynote, Red Star OS's new look will have a lot of similarities to Apple's Mac OS X. The revamp is part of the country's doctrine that emphasizes "self-reliance," except that Red Star OS is based on crowd-sourced Linux. And just like Mac OS X, the program features bouncy icons, a grey color scheme and orb-shaped buttons. The Telegraph reports that it actually took a staff of more than 1,000 with offices in four countries to create it. Red Star OS has been on the public radar since 2010 when a Russian student revealed that the extremely secretive country invented its own software. And it shouldn't be too much a surprise since Kim Jong Un is a known Apple fan. Red Star OS come preloaded with iWork, but it does have plenty of quirks: It was reported that the software uses a calendar which counts years from the birth of Kim Il-Sung, making 2014 the 103rd year. It is only available in Korean and the bundled Firefox browser has the North Korean government website as a default home page. To read more click **HERE**

Hacked in Sochi in minutes: Russian cyberspace full of risks

Yahoo News, 5 Feb 2014: Privacy in all forms is a very rare commodity at the Sochi Olympics, according to a report from NBC News. Athletes, journalists and fans are reportedly seeing their cell phones, computers and tablets hacked. The report, by NBC News' Richard Engel, demonstrates how quickly the hackings occur. In an experiment conducted with the help of an American computer security expert, Engel created a fake online identity with fake contact lists, phony names and addresses. In Russia, the pair fired up two new laptop computers loaded with Engel's fake profile to see how long it would take hackers to do their business. They didn't have to wait long — in less than a minute, Engel received what appeared to be a custom email welcoming him to Sochi and asking him to click on a link for information he might find useful. After clicking, Engel said, his computer was "hijacked." It was the same scenario with Engel's cell phone. "Malicious software hijacked our phone before we even finished our coffee, stealing my information and giving hackers the option to tap and record my phone calls," Engel said. For those traveling to Sochi for the Games, Engel recommends not bringing phones or laptops if at all possible. If you can't be without a connection, delete any sensitive information from devices before logging on. And as with "phishing" scams, don't click on anything in an email or a Web page that takes you to an external link, as Web sites that appear to belong to banks or other "secure" third parties can be easily faked. Hackers who hail from Russia are known to be among the world's most skilled. The 2013 hacks of retailers Target and Neiman Marcus were traced back to a Russian teenager. However, according to Bloomberg, "China accounted for 41 percent of the world's attack traffic" during the fourth quarter of 2012. To read more click **HERE**

Insecure file sharing puts corporate data at risk

Heise Security, 6 Feb 2014: Personal email could be 2014's biggest threat to corporate data. A new survey of more than 500 professionals by Globalscape found that in the past 12 months, 63 percent of employees have used personal email to send sensitive work documents. Perhaps more surprisingly, 74 percent of those employees believe that their companies approve of this type of file-sharing behavior. The threat of consumer-grade file transfer methods extends far beyond employees' use of personal email. In the past 12 months:

- 63 percent of employees have used remote storage devices, like USB drives, to transfer confidential work files
- 45 percent of employees have used consumer sites like Dropbox and Box.net to share sensitive business information
- 30 percent of employees have used cloud storage services for work-related files.

"Millions of employees are actively using consumer-grade tools, like personal email, social media, and file sharing sites, to move confidential work files every day," said James Bindseil, president and CEO of Globalscape, a developer of secure information exchange solutions. "While the intent is typically harmless, these actions can have serious security and compliance ramifications." Employees' reliance on consumer-grade tools to transfer files is not an isolated problem. Nearly half of all employees surveyed transfer work files through unsecured channels (remote storage, personal email, cloud storage, or consumer file-transfer sites) several times a week. "We found that 80 percent of employees surveyed that use personal email to transfer sensitive work files do it at least once a month," says Bindseil. "Even scarier: nearly a third of that group knows for a fact that their personal email has been hacked at least once – yet they continue to put company information at risk." IT departments are struggling to create effective information-sharing policies and educate employees on the risks of using unsecured channels. According to Globalscape's survey, only 47 percent of employees think the companies they work for have policies for sending sensitive files. Almost a third said that there were no policies in place, and 22 percent weren't sure. Policy enforcement is also lacking. Of the employees at companies that have policies for sending sensitive files, 54 percent still use personal email, and 62 percent still use remote devices. While there are many reasons that employees find alternatives to their company-provided file-transfer tools, the biggest drivers are simplicity and ease of use. According to Globalscape's survey:

- 52 percent said it's more convenient to use a tool that they know well
- 33 percent reported that recipients have had trouble accessing files sent through the company system
- 18 percent said they use alternatives because the company's tool does not offer mobile access.

"Employees need and expect instant access to information, and the ability to send and store files at the press of a button. When internal technology and tools come up short, employees will find a workaround." To read more click **HERE**

Windows, IE, Java are most vulnerable

Heise Security, 4 Feb 2014: When compared with the numbers from the previous year, 2013 has seen an increase in reported security vulnerabilities and, what's more, the number of critical vulnerabilities has also risen - although it's considerably smaller than in 2009. GFI researchers have combed through the details provided by the US National Vulnerability Database (NVD), and have discovered that in 2013, an average of 13 new vulnerabilities were reported each day, bringing the total to 4794 - 447 more that in 2013. 50 percent of the flaws were found in products of only 10 vendors out of 760. The numbers are both a testament to the number of different offerings these big firms have and to their popularity, which naturally points to the conclusion that they are more often targeted by hackers and analysed by security researchers for security flaws. Oracle has topped the list not only because of Java vulnerabilities, but also because of hardware flaws found in the company devices. Still, Microsoft can't sigh a sigh of relief, as the company has had a huge rise in "high severity" vulnerabilities when compared to 2012 numbers. Critical vulnerabilities found in its various operating systems made Microsoft occupy 8 of the first 9 spots on the list of most targeted OSes in 2013. Finally, Microsoft's Internet Explorer, Oracle's Java and Google's Chrome have ended up occupying the first three spots (respectively) on the list of most targeted applications. "From a security perspective, Oracle and Java had a bad year in 2013 with 193 vulnerabilities reported for Java, 102 of them critical," noted GFI's Christian Florian. "To make matters worse, an high number of the critical vulnerabilities in Java were zero-days flaws." Another thing to take into consideration is the fact that cyber attackers have a preference for exploiting Java vulnerabilities, because the software can be found on many computers who run different operating systems. Keeping all this in mind, the best advice you can get to keep safe is still to keep your operating system, applications, and security software up to date, and to remove software you don't use or need in order to minimise the attack surface. To read more click **HERE**