The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
14 March 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

March 13, Softpedia – (International) **PayPal rewards researcher for finding EL injection vulnerability in Zong.** A researcher identified and reported an Expression Language (EL) vulnerability in mobile payments processor Zong which could be used for code execution and other tasks. PayPal then issued a reward to the researcher after verifying the finding. Source: http://news.softpedia.com/news/PayPal-Rewards-Researcher-for-Finding-EL-Injection-Vulnerability-in-Zong-431930.shtml

March 12, Pittsburgh Tribune-Review – (Pennsylvania) **Security breach compromises credit-card info at Bloomfield medical practice.** Partners in Nephrology & Endocrinology in Pittsburgh confirmed March 12 that an attacker hacked into a vendor's system that processes credit card payments for the practice and potentially accessed credit card numbers and personal information of about 5,000 patients in November 2013. Authorities are investigating the incident. Source: http://triblive.com/news/adminpage/5753432-74/card-credit-practice

March 12, Softpedia – (International) **Harvard Law National Security Journal hacked, abused to promote rogue pharmacies.** Harvard representatives stated that they are investigating after the Harvard Law School National Security Journal Web site was compromised and attackers used the site to promote various rogue pharmacies. Officials reported that the problem remains unresolved but they are working to fix the issue. Source: http://news.softpedia.com/news/Harvard-Law-National-Security-Journal-Hacked-Abused-to-Promote-Rogue-Pharmacies-431767.shtml

March 13, The Register – (International) **Ethical hacker backer hacked, warns of email ransack.** The EC-Council, which runs the Certified Ethical Hacker program, notified its members that attackers who defaced its Web site in February also gained access to the site's control panel, allowing them access to the organization's email system. The EC-Council is continuing to investigate and notified members as a precaution. Source:http://www.theregister.co.uk/2014/03/13/ethical_hacker_cert_org_pwned/

March 13, Help Net Security – (International) **Rbrute trojan hacks Wi-Fi routers to help spread Sality.** Researchers at Dr. Web identified and analyzed a trojan dubbed Rbrute, which compromises Wi-Fi routers in order to spread the Sality malware family. Source: http://www.net-security.org/malware_news.php?id=2731

March 12, Computerworld – (International) **Twitter crashed – again – on Tuesday.** Twitter was down for around 1 hour March 11 due to unexpected issues arising from a planned deployment of an upgrade. The social media network experienced a similar disruption March 2. Source: http://www.networkworld.com/news/2014/031214-twitter-crashed----again----279654.html

UK Supermarket Chain Morrisons Suffers Data Breach

SoftPedia, 14 Mar 2014: Morrisons, the United Kingdom's fourth largest supermarket chain, has suffered a major data breach. The company says that someone has managed to steal the personal and financial information of employees and posted it on a website. "We are extremely sorry to inform you that there has been a theft of colleagues' personal information, which was uploaded onto a website. As soon as we became aware of this last night we took immediate steps to ensure the data was removed from the website," Morrisons wrote in a statement published on Facebook. The stolen staff payroll information includes names, addresses, and bank account details. Employees from all levels are said to be impacted by the incident. The leaked information was allegedly available on a website only for a few hours before being pulled down. The Telegraph reports that the information was also sent to a newspaper on a disk, but the newspaper has not been named. The company calls the incident "an illegal theft of data" and says that it is working with the police and cybercrime authorities to get to the bottom of it. "Our immediate priority is the security of your financial information. We are currently working with Experian and the major banks to ensure that we provide full support and assistance to all affected colleagues. This will include support and advice around protection of your bank account," the company noted. Morrisons says it's confident that no customer information has been stolen. The supermarket says there's no evidence that this is an external attack. The company's Chief Executive, Dalton Philips, is leading the response. The company promises to provide more details soon. In the meantime, it urges employees who might have any questions to send them an email to data.advice (at) morrisonsplc.co.uk. The announcement comes shortly after Morrisons announced its intentions to cut down prices to compete with discount chains after suffering an annual loss of £176 million ($292 million / €210 million). Another incident that shows insider threats should never be neglected, especially by a large company. To read more click **HERE**

Hackers Target Russian Government in Response to Anti-Putin Sites Being Blocked

Softpedia, 14 Mar 2014: The Russian government has blocked Internet users from accessing a number of websites that are known for criticizing the country's President, Vladimir Putin. In response, hacktivist groups have disrupted some of the government's websites. Russia's Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) reports that the Grani newspaper (grani.ru), the site of the famous chess player Garry Kasparov (kasparov.ru), ej.ru and navalny.livejournal.com have been blocked. The website of the radio station Ekho Moskvy (echo.msk.ru) is also reportedly inaccessible. The sites have all been blocked at ISP level. Apparently, the Prosecutor General of the Russian Federation has asked that these websites be blocked because they call on visitors to take part in illegal activities and public events "held in violation of the established order." navalny.livejournal.com, the website of anti-corruption crusader Alexei Navalny, has been allegedly blocked because Navalny violated the conditions of his house arrest by accessing the Web. Garry Kasparov posted the following message on Twitter in response to the blockade:

These are huge news sites, not political groups. Giant Echo of Moscow site now just gone. Grani, EJ, Navalny's blog, all blocked in Russia.

— Garry Kasparov (@Kasparov63) March 13, 2014

While the government is denying that these actions represent a form of censorship, many believe that this is an attempt to silence Putin's critics. Among those who believe that this is the case, there are some hacktivists who have launched distributed denial-of-service (DDOS) attacks against a number of high-profile websites. The list includes the website of the Kremlin (kremlin.ru) and the Central Bank of Russia (cbr.ru). At the time of writing, the Central Bank's website is still inaccessible. The site of the Kremlin is working, but pages are loading slowly. More cyberattacks might follow if the websites are not unblocked. The Electronic Frontier Foundation (EFF) has noted that it profoundly opposes the censorship of the Internet by the Russian government. "We are especially concerned about the censorship of

independent news and opposing political views, which are essential to a thriving civil society," the EFF said. The organization is urging Russians who still want to be able to access the websites to use the anonymity network Tor. Russia enacted the law that enables the government to block websites in 2012. At the time, officials argued that the legislation would primarily be utilized to block websites related to drug use, sites containing child abuse content, and ones that promoted suicide. However, now it's being used against major news websites. Many fear that Russia will slowly become just like China, which is well known for its censorship. To read more click **HERE**

Researchers Rewarded with a Total of $850,000 / €613,000 at Pwn2Own 2014

SoftPedia, 14 Mar 2014: "All your web browser are belong to us" appear to have said contestants at Pwn2Own 2014. On the second day of the hacking competition, all major web browsers were found to be vulnerable. If on the first day, contestants hacked Internet Explorer and Firefox, on the second day, they managed to "pwn" Safari, Firefox, Internet Explorer and Chrome. In addition to web browsers, on the second day, serious flaws were also found in Adobe Flash. Let's take a look at each of the vulnerabilities. First, an anonymous participant managed to execute arbitrary code in Chrome by leveraging an arbitrary read/write bug with a sandbox bypass. However, this has been catalogued as only partially valid as the vulnerability presented by the contestant collided with another flaw shown earlier at Pwnium. Chrome has also been hacked by VUPEN, the team that earned a total of $300,000 (€215,000) the previous day. The team has managed to break Google's web browser with a use-after-free affecting the WebKit and Blink. Combined with a sandbox bypass they've found, they've managed to execute arbitrary code. Zeguang Zhou of team509 and Liang Chen of Keen Team have managed to break Adobe Flash with a heap overflow vulnerability and a sandbox bypass. Chen of the Chinese Keen Team has also managed to execute code in Safari through a heap overflow and a sandbox bypass. Safari was also hacked on day one of the competition, but part of Pwn4Fun, a new challenge in which ZDI and Google experts presented their exploits. All money went to the Canadian Red Cross. George Hotz has found an out-of-bound read/write security hole resulting in code execution in Firefox. Sebastian Apelt and Andreas Schmidt have managed to find two use-after-free bugs and a kernel flaw in Internet Explorer. The total prize money given out at Pwn2Own 2014, without the amount that goes to charity, is $850,000 / €613,000. Contestants have also been rewarded with ZDI points, laptops and other prizes. All vulnerabilities have been disclosed to vendors. Pwn2Own 2014 has broken the record for number of entries. Interestingly, no one took a crack at Oracle Java, although this might be explained by the fact that the prize for hacking Java has been of only $30,000 (€22,000). Unsurprisingly, no one managed to take the "Exploit Unicorn" grand prize. As part of this new challenge, organizers were prepared to hand out $150,000 (€111,000) to the researcher who demonstrated SYSTEM-level code execution on Windows 8.1 x64 on IE 11 x64 with EMET bypass. To read more click **HERE**

Prolexic Warns of Significant Increase in NTP Amplification DDOS Attacks

SoftPedia, 14 Mar 2014: Distributed denial-of-service (DDOS) attacks that abuse Network Time Protocol (NTP) servers for amplification are becoming more and more common. In fact, Akamai subsidiary Prolexic warned that in February, it detected a 371% increase in the number of such attacks. "During the month of February, we saw the use of NTP amplification attacks surge 371 percent against our client base. In fact, the largest attacks we've seen on our network this year have all been NTP amplification attacks," revealed Stuart Scholly, SVP/GM Security, Akamai Technologies. Experts highlight the fact that NTP amplification attacks are becoming more and more popular because cybercriminals can send 100 Gbps or even more to a certain server by abusing just a few vulnerable servers. NTP amplification attacks haven't targeted just a single sector. Instead, companies from industries like finance, e-commerce, gaming, telecom, media, education, security and SaaS providers have been targeted. Simulations made by Prolexic have shown that these attacks produce responses amplified 300 times when it comes to bandwidth and 50 times for volume. Statistics show that compared to January, in February, the average peak DDOS attack bandwidth increased by 217%, while the average peak volume increased by a whopping 807%. In a recent interview we had with Marc Gaffan, co-founder of Incapsula, he noted that DNS amplification attacks are still the most common. However, at this rate, the situation could change

very soon. The complete report from Prolexic on NTP amplification attacks is available on the company's **website** (registration required). To read more click **HERE**

US-CERT Recommends Windows XP Users to Abandon Internet Explorer

SoftPedia, 14 Mar 2014: Everybody knows that Windows XP support is coming to an end in only 25 days and while people might be thinking that Microsoft is trying to spam them as much as possible with news on the retirement date, security organizations across the world are telling basically the same thing as the Redmond-based giant. The United States Computer Emergency Readiness Team has itself issued a notice for Windows XP users, telling them that Microsoft would stop providing patches and security updates for their OS version on April 8, but also giving advice regarding their Windows XP machines. Basically, the US-CERT said almost the same thing as Microsoft did, but with different words: consumers are recommended to stop using Windows XP and move to a newer platform that has what it takes to provide enhanced security and keep data away from hackers. But what's more important is that the US-CERT is also telling users who plan to stick to Windows XP after the retirement date to abandon Internet Explorer completely, as this particular browser could increase the risk of getting hacked after April. Internet Explorer is the browser that gets patches via Windows Update every Patch Tuesday, so without any other fixes released by Microsoft, such an application would also increase the risks of being hacked. "Users who choose to continue using Windows XP after the end of support may mitigate some risks by using a web browser other than Internet Explorer. The Windows XP versions of some alternative browsers will continue to receive support temporarily. Users should consult the support pages of their chosen alternative browser for more details," the US-CERT said in a security advisory (which you can find below just after the jump). Microsoft has started to show upgrade notifications on Windows XP computers with the help of a patch delivered via Windows Update on March 8, so everyone should be aware that support for XP is coming to an end. The question, however, is how many of the 29 percent of the desktop users still running XP right now are willing to migrate? Not many, people say, especially because the transition to a newer platform would also involve hardware upgrades, so the costs of such a decision would be fairly big. Windows 8.1 is Microsoft's platform of choice for those still on Windows XP, so the company encourages everyone still on the ancient platform to buy new computers running the modern operating system. To read more click **HERE**

Beware of well-executed Google Docs phishing scam

Heise Security, 14 Mar 2014: A realistic phishing spam campaign is currently targeting Google Docs and Google Drive users. It all starts with an email that tells potential victims that an important document is waiting to be viewed on Google Docs, and can be viewed by following the offered link. Unfortunately, the link directs the users to a legitimate-looking but spoofed Google login page. "The fake page is actually hosted on Google's servers and is served over SSL, making the page even more convincing. The scammers have simply created a folder inside a Google Drive account, marked it as public, uploaded a file there, and then used Google Drive's preview feature to get a publicly-accessible URL to include in their messages," Symantec researchers explain. The scam attempt is even more difficult to recognize in time when you know that logging into Google is something that users are usually asked to do when accessing a Google Docs link. But once the victims submit their login credentials, they are sent to a remote server, and the victims are redirected to a real Google Docs document in order to complete the illusion. To read more click **HERE**