The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

14 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 12, SC Magazine – (International) **Gameover Zeus most active banking trojan in 2013, researchers report.** Dell SecureWorks Counter Threat Unit released a report covering banking trojans in 2013 and found that the Gameover ZeuS trojan was the most actively observed trojan during the year, with 38 percent of activity, followed by the Citadel trojan at 33 percent of activity. Source: http://www.scmagazine.com//gameover-zeus-most-active-banking-trojan-in-2013-researchers-report/article/333795/

February 13, Softpedia – (International) **Oracle confirms existence of 30 security holes in Java Cloud Service.** Oracle confirmed the existence of 30 security vulnerabilities in its Java Cloud Service reported to the company by Security Explorations researchers. The researchers stated that over half can be exploited to bypass the Java security sandbox. Source: http://news.softpedia.com/news/Oracle-Confirms-Existence-of-30-Security-Holes-in-Java-Cloud-Service-426666.shtml

February 13, V3.co.uk – (International) **Android apps with Trojan SMS malware infect 300,000 devices, net crooks $6m.** Researchers at Panda Labs identified a new Android trojan app campaign that uses fake permission notifications to get users' devices to send SMS messages to a premium-rate number owned by the attackers behind the trojan apps. The campaign has infected at least 300,000 devices and netted the attackers at least $6 million. Source: http://www.v3.co.uk/v3-uk/news/2328691/android-apps-with-trojan-sms-malware-infect-300-000-devices-net-crooks-usd6m

February 13, Help Net Security – (International) **Linksys home routers targeted and compromised in active campaign.** A security researcher reported that an unknown vulnerability is allowing Linksys E1000 routers to be targeted and infected with a worm dubbed TheMoon. The vulnerability is currently being heavily exploited in attacks. Source: http://www.net-security.org/malware_news.php?id=2707

February 13, Softpedia – (International) **ASUS fixes vulnerabilities in RT-N66U, RT-N66R and RT-N66W routers.** ASUS released firmware updates for three RT-N66 model routers, closing five security issues. Source: http://news.softpedia.com/news/ASUS-Fixes-Vulnerabilities-in-RT-N66U-RT-N66R-and-RT-N66W-Routers-426689.shtml

February 12, Threatpost – (International) **US government delivers cybersecurity framework for critical infrastructure.** The National Institute of Standards and Technology (NIST) announced February 12 that it has released the Framework for Improving Critical Infrastructure Security, a document which outlines cybersecurity practices and standards for industry and government to consider when developing security programs for critical infrastructure. Source: http://threatpost.com/us-government-delivers-cybersecurity-framework-for-critical-infrastructure/104243

February 12, SC Magazine – (International) **Pre-installed security software leaves computers vulnerable to remote hijack, experts reveal.** Kaspersky Lab researchers released a report February 12 warning that the Absolute Computrace anti-theft software pre-installed on some desktops and laptops contains vulnerabilities which could allow attackers to remotely hijack systems. Source: http://www.scmagazine.com/pre-installed-security-software-leaves-computers-vulnerable-to-remote-hijack-experts-reveal/article/333808/

February 12, IDG News Service – (International) **Denial-of-service vulnerability puts Apache Tomcat servers at risk.** Researchers published a proof-of-concept exploit for a recently-disclosed vulnerability affecting Apache Tomcat servers that could allow attackers to execute denial-of-service (DoS) attacks against Web sites hosted on the servers. Source: http://www.networkworld.com/news/2014/021214-denial-of-service-vulnerability-puts-apache-tomcat-278708.html

February 13, Associated Press – (International) **FBI, Secret Service investigating Sands hacking.** The FBI, U.S. Secret Service, and the Nevada State Gaming Control Board are investigating a cyberattack on the Las Vegas Sands casino company's Web sites and email system. The company is working to determine whether systems may have been compromised in the attack that took the sites offline for more than a day. Source: http://www.nbc29.com/story/24705154/las-vegas-sands-investigating-website-hacking

Scary New Malware Is Tearing Up The Internet And No One Knows Where It Came From
Yahoo, 14 Feb 2014: "Careto" is the name of "a sophisticated suite of tools for compromising computers and collecting a wealth of information from them," reports The Washington Post. Here's how it works: It sends out emails designed to look as though they were sent legitimately from news sources like The Guardian and others. A population of people end up clicking on a link that takes them to a shady site that scans their computer for vulnerabilities. It works against Windows, OS X and Linux systems, and there may be iOS and Android versions on the way. Once infected, a computer surrenders pretty much any info the malware wants. It can collect "network traffic, keystrokes, Skype conversations, analyze Wi-Fi traffic, PGP keys, fetch all information from Nokia devices, screen captures and monitor all file operations." And lest you need a reminder, no one knows where it came from. If you want to dig into the nitty-gritty of it all, Kaspersky Labs released this extensive report [**LINK**] on Careto that gets into a lot of the scarier technical details. To read more click **HERE**

Forbes Hacked by Syrian Electronic Army
SoftPedia, 14 Feb 2014: The website of Forbes appears to have been hacked by the Syrian Electronic Army. A story entitled "Hacked by the Syrian Electronic Army" has been added to the list of articles written by Forbes' Andy Greenberg, Matthew Herper, John Dobosz, Steve Forbes (the chairman and editor-in-chief of Forbes Media), and Travis Bradberry. It appears the hackers have gained access to login credentials for the site's administrative panel. This wouldn't be surprising, considering that the Syrian hacktivists have often used this attack vector. In most cases, they've gained access to credentials after sending phishing emails to the targeted organization's employees. I'm trying to get in touch with members of the Syrian Electronic Army to see what they have to say about the attack. So far, they haven't publicly announced anything on Twitter. I'll update this post if more information becomes available. Update. The Syrian Electronic Army has confirmed targeting Forbes. They've also confirmed that they've breached an administrative account. They've provided me with a screenshot of the website's WordPress administration panel. The hackers have hijacked three Twitter accounts belonging to Forbes and its employees: @samsharf, @ForbesTech, @TheAlexKnapp. At the time of writing, only the one of Samantha Sharf shows a "Syrian Electronic Army Was Here" messages. The hacktivists tell me that besides posting the articles, they haven't caused any other damage. They've attacked Forbes because the publication has "posted many articles against the SEA, with much hate for Syria." To read more click **HERE**

Zero-Day Vulnerability Confirmed in Internet Explorer 9 and 10

SoftPedia, 14 Feb 2014: Security company FireEye Labs has discovered a new zero-day vulnerability in Internet Explorer 9 and 10 that would allow an attacker to install malicious software on an unpatched computer. According to a security research, the attack is performed with the help of a compromised website whose HTML code is modified to load a malicious webpage created by the attacker in the background. "The attacker's HTML/JavaScript page runs a Flash object, which orchestrates the remainder of the exploit. The exploit includes calling back to the IE 10 vulnerability trigger, which is embedded in the JavaScript," FireEye Labs explained. At this point, it turns out that Internet Explorer 9 and 10 with Adobe Flash up and running are the only two browsers vulnerable to attacks, with Microsoft confirming that it's currently investigating reports and is now trying to determine how many users have fallen victims to exploits. "Microsoft is aware of limited, targeted attacks against Internet Explorer 9 and 10," a Microsoft spokesperson told TNW. "As our investigation continues, we recommend customers upgrade to Internet Explorer 11 for added protection." The easiest way to stay protected until Microsoft comes up with an official patch to address the vulnerability is to update to Internet Explorer 11, as it's available on Windows 7 computers as an optional download. "The vulnerability is a previously unknown use-after-free bug in Microsoft Internet Explorer 10. The vulnerability allows the attacker to modify one byte of memory at an arbitrary address," FireEye Labs explained in a blog post. "The exploit targets IE 10 with Adobe Flash. It aborts exploitation if the user is browsing with a different version of IE or has installed Microsoft's Experience Mitigation Toolkit (EMET). So installing EMET or updating to IE 11 prevents this exploit from functioning To read more click **HERE**

Email Addresses and Passwords of over 2,000 Tesco Customers Leaked Online

SoftPedia, 14 Feb 2014: On February 12, a file containing the email addresses, clear text passwords, and loyalty card balances of 2,239 customers of the supermarket giant Tesco were published by someone on Pastebin. The company has deactivated the accounts of impacted customers. The company's representatives have told the BBC that credentials haven't been obtained from Tesco's website. Instead, the cybercriminals took data leaked in older attacks and tried it out on Tesco's site. They've been counting on the fact that many people use the same username/password combination for multiple online accounts. The supermarket says that it's replacing the vouchers of a "very small number" of affected customers. Security expert Troy Hunt has some interesting theories on how the cybercriminals may have carried out this attack. Even if Tesco's databases have not been hacked, the company does a poor job in preventing cybercriminals from matching credentials stolen in other high-profile attacks with the ones of the supermarket's customers. For instance, the password recovery feature tells you if the email account you're requesting the reset link to exists or not. This makes it easy for the attacker to determine if the email address is valid. Furthermore, the website doesn't have any protection against brute-force attacks, allowing hackers to try out a large number of passwords in a short period. All this can be done automatically, the attacker doesn't have to manually try out the passwords one by one. Another problem with Tesco's security systems lies in password policies. Passwords must be between six and ten characters in length, and they "can" (not must) contain a mixture of letters and numbers. "All of this dramatically decreases the character space of passwords which in turn dramatically increases the likelihood of an account being brute forced. This practice almost certainly played a part in the breach if brute force was indeed involved," Hunt explained. The Tesco data has been added by Hunt to the "Have I Been Pwned?" service. The expert says 15% of them have already been included in the haveibeenpwned.com database. In case you want to see if the Tesco breach impacts you, check out Have I Been Pwned? To read more click **HERE**

Thousands of FTP Servers Compromised, UNICEF and NYT Impacted

SoftPedia, 14 Feb 2014: Cybercriminals possess the credentials needed to access more than 7,000 FTP servers belonging to organizations from all over the world, including small businesses, ISPs, multinational corporations and individual accounts. The hackers are using this access to host malware, scam websites, rogue pharmacies, exploits and other content. According to experts, the attackers have planted PHP scripts with backdoors and viruses in a number of

directories in hopes that they can gain access to the targeted organizations' web services. HTML files that seamlessly redirect users to malicious sites have also been uploaded to the compromised servers. The FTP sites are hijacked in several ways. Some of them are easy to compromise because they use anonymous, default of publicly available credentials. Botnets also aid cybercriminals in gathering FTP credentials. Hold Security's Chief Information Security Officer Alex Holden has told IDG that the list of affected servers includes ones operated by The New York Times and UNICEF. NYT representatives have told the publication that they're working on securing the server in question. The security experts discovered that the attackers had uploaded an HTML file to NYT's server. Cybercriminals could have tricked users into clicking on a link to lure them to the NYT FTP site, from where they would be redirected to a website hosting a work-from-home scam. UNICEF says that the affected FTP application is part of a system that's no longer in use, so they've disabled it. The organization's representatives have explained that they rely on the services of third parties to ensure that their systems are not vulnerable. Hold Security urges companies to review their FTP implementations to ensure that their servers cannot be abused by cybercriminals. End users, on the other hand, should be careful what embedded links they click on in order to avoid ending up on malicious websites. To read more click **HERE**

Silk Road 2.0 Claims All Bitcoins Were Lost in Hack

SoftPedia, 14 Feb 2014: It's been a few months since Silk Road was shut down, and nearly just as long since a copycat of the site was re-opened. Now, Silk Road 2.0 claims that all its Bitcoin reserves were stolen in a hack. According to the complaint made by a site administrator, they lost around two or three million dollars' worth of Bitcoins in the fraudulent attack. According to the admin, the Bitcoins were stolen by hackers by exploiting the transaction malleability loophole to withdraw funds. "This attack hit us at the worst possible time. We were planning on re-launching the new auto-finalize and Dispute Center this past weekend, and our projections of order finalization volume indicated that we would need the community's full balance in hot storage," said Defcon, the admin. The exploit used seems similar to the issue reported by MtGox last week, the world's largest Bitcoin exchange market. The issue led, in that case, to the suspension of any type of fund withdrawals. Given how this happened a week ago, the Bitcoin prices have dropped considerably. "I have failed you as a leader, and am completely devastated by today's discoveries. I should have taken MtGox and Bitstamp's lead and disabled withdrawals as soon as the malleability issue was reported," Defcon said. Most of the funds seem to have been routed to an individual in France, while another couple of people in Australia got the rest, the Silk Road admin said. Forbes reports that Nicholas Weaver, a researcher at the International Computer Science Institute, estimates that the total theft over at Silk Road counts about 4,400 coins, which puts the value at over $2.5 million, depending on the day. Silk Road users are none too happy about the issue and many are calling the excuse made by Defcon as fake, especially since so many asked for something to be done about this possible vulnerability over the past week. To read more click **HERE**

IE Zero-Day Served by DeputyDog Cybercriminals from VFW Site

SoftPedia, 14 Feb 2014: A sophisticated group of cybercriminals, the ones who have previously conducted the DeputyDog and Ephemeral Hydra campaigns, are using an Internet Explorer zero-day in a new operation dubbed SnowMan. Security researchers from FireEye have spotted the zero-day exploit, which impacts IE 9 and 10, on the website of the US Veterans of Foreign Wars (vfw.org). Experts believe that this is part of an attack targeting US military personnel. The cybercriminals behind this attack are known for targeting high-profile organizations. They've previously attacked US government entities, defense industrial base companies, law firms, Japanese companies, and NGOs. They've also targeted IT and mining companies, mostly by relying on remote access Trojans (RATs). Microsoft has confirmed the existence of the exploit. The company advises customers to update Internet Explorer to version 11 to protect themselves against such attacks. Additional technical details on the IE zero-day exploit and the SnowMan campaign are available on FireEye's blog [**LINK**]. To read more click **HERE**

Fake "Reactivate Your Microsoft Email Account" Emails Lead to Phishing

SoftPedia, 14 Feb 2014: Emails purporting to come from Microsoft and the "WWW email domain host" are being sent out by cybercrooks in an attempt to lure Internet users to a phishing site where they're asked to hand over their passwords and other information. The emails spotted by Hoax Slayer carry the subject line "REACTIVATE YOUR EMAIL ACCOUNT!!!" and they read something like this: "In compliance with the email upgrade instructions from Microsoft Corporation and WWW email domain host, all unverified email accounts would be suspended for verification. To avoid suspension of your email account and also to retain all email Contents, please perform one time automatic verification by completing the online verification form. Please CLICK HERE." The notifications have nothing to do with Microsoft. When the link is clicked, victims are taken to a phishing site where they're asked to enter their email address, password, date of birth, and phone number. If you come across such emails, delete them. In case you're a victim of this scam, change your password (or passwords if you've been using the same one for multiple accounts) as soon as possible. To read more click **HERE**

The cyberwar threat from North Korea

FoxNews.com, 14 Feb 2014: North Korea's effort to build a cyberarmy that can conduct a string of attacks on neighboring states has experts asking some key questions: Is Pyongyang gearing up for a cyberassault on the United States? Does it have the capability? "They do have the capability, obviously," says Alexandre Mansourov, a visiting scholar at the U.S.-Korea Institute at the Johns Hopkins School of Advanced International Studies. "But I don't think they have the intention." But not everyone is so unsure. Like the Cold War in the 1950s and '60s, cyberwarfare is becoming an arms race. Many nations, including the United States, are building up their offensive and defensive capabilities amid an increase of espionage and a proliferation of attacks on public and private computer networks. Experts say the number of attacks on South Korea over the last five years looks more like a coordinated war than the work of random hackers. This has some officials in the U.S. girding for a broader fight. "We should never underestimate Pyongyang's willingness to engage in dangerous and provocative behavior to extract more aid and concessions from the international community," Rep. Mike Rogers (R-Mich.), chairman of the House Select Committee on Intelligence, said in a statement to FoxNews.com. 'They are saying quite publicly they have several thousand men and women working on a daily basis on cyber.' - Jarno Limnéll, director of cybersecurity at Stonesoft Corp. "North Korea is certainly not the most capable nation-state threat actor today, but even relatively minor cyberplayers can sometimes find vulnerabilities in complicated civilian architectures and cause significant disruptions." While no one knows exactly what North Korea has up its sleeve, a number of hackers who have defected, as well as the increasingly sophisticated attacks on South Korea, suggest that its leader, Kim Jong-un, isn't limiting his muscle-flexing to nuclear tests in the Pacific. According to reports beginning in 2010, North Korea has been training thousands of top computer science students to be sophisticated cyberwarriors. Some experts, like Professor Lee Dong-hoon of the Korea University Graduate School of Information Security, estimate that Pyongyang has been pouring money into cyberwarfare since the 1980s. The proof is in the attacks, of course, though it is difficult to pin down the responsible parties: A wave of "distributed denial of service (DDoS)" attacks in 2009 struck both U.S. government and South Korean websites. A virus launched from unknown sources (South Korean officials accused Pyongyang) through a series of "zombie" computers sent waves of Internet traffic to a number of websites in the two countries. The U.S. Treasury and Federal Trade Commission sites were shut down for a weekend, but the action crippled a number of government sites and media outlets in South Korea. A DDoS attack on South Korean banks in March 2011 left 30 million people without ATM access for days. At the time, Dmitri Alperovitch, vice president of threat research for McAfee Labs, said the attacks had the mark of a North Korean "cyberwar drill" and theorized that Pyongyang had built an army of zombie computers, or "botnets," to unleash malicious software. He guessed that the 2009 attack had been a similar operation. An attack in March 2013 was the biggest one yet, infecting and wiping clean the critical master boot records of 48,000 computers and servers associated with South Korean banks and media outlets, using their own networks. Experts traced the "cyberweapon" back through more than 1,000 IP addresses used on different continents, but South Korean officials accused North Korea of directing the attack. Systems were crippled for

days. Gen. James Thurman, commander of U.S. forces in South Korea, told Congress in 2012 that "the newest addition to the North Korean asymmetric arsenal is a growing cyberwarfare capability," in which North Korea "employs sophisticated computer hackers trained to launch cyberinfiltration and cyberattacks" against South Korea and the U.S. Observers say the alleged North Korean attacks are launched from servers all over the world in order to avoid detection. "It's all untraceable," Mansourov said. "But there is a presumption of guilt -- I think it's a valid presumption." Jarno Limnéll, director of cybersecurity at Finland-based Stonesoft Corp. (part of the McAfee cybersecurity company), said that while it is "hard to know what cyber-capabilities your enemies or even your friends have, [this is] something [North Korea] has taken very seriously … and what they are saying quite publicly is they have several thousand men and women working on a daily basis on cyber. They want to give a very clear impression that they are a strong player in this field." For its part, Pyongyang has accused South Korea and the U.S. of launching similar attacks against North Korea. Last March, around the time of the attacks on banks and broadcasters in Seoul, North Korean offices said an online attack took down the servers at Loxley Pacific Co., the broadband provider for the North. Mansourov said there is a "Cold War situation going on," a tit-for-tat between the North and South. And it's not limited to the Korean Peninsula: China has accused the U.S. of cybersnooping, and the U.S. has accused China not only of spying, but of launching expensive cyberattacks against public and private networks in the U.S. Meanwhile, Israel and the U.S. were widely fingered for launching the Stuxnet virus that crippled Iran's nuclear program in 2010. "It's effectively an arms race," said C. Matthew Curtin, founder of the computer security consulting firm Interhack and author of Brute Force: Cracking the Data Encryption Standard. "We need to assume that hostile nation states -- even non-state actors like al Qaeda -- have offensive cyber-capabilities, and we need to be in a position to render their capabilities moot." He said the best way to confront cyberthreats is to secure domestic networks and force other countries to spend more money to get to us. "Then it becomes like the [Cold War-era] Soviet Union, where they will eventually have nothing left to spend," he said. Rogers still hopes to see the Cyber Intelligence Sharing and Protection Act (CISPA), which the House passed in April, succeed in the Senate and be signed into law by President Obama. It would allow greater information sharing between the government and private companies to prevent and respond to cyberattacks. But critics say it will give the government greater ability to monitor citizens' Internet communications. "It's not a black-and-white issue," said Curtin, who noted that "nothing is free" and that breaking down these "barriers" of information will require ordinary citizens to give up some privacy. But the threat is real, he said, whether it comes from North Korea or Iran. "If someone was trying to shut down our power grid when there is a huge polar vortex blowing through the country, that would have a serious impact on us," he said. To read more click **HERE**