THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

3 September 2014

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

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

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

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, and Sandia National Labs

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings. Credit is given to the NMCIWG for the compilation of this open source data

September 1, IDG News Service – (International) **Rigged industrial software site points to watering hole attack.** Researchers at AlienVault reported that the Web site of an unnamed industrial software company was compromised with a piece of reconnaissance malware called Scanbox that collected information on visitors to the site, including visitors' IP addresses, language, operating system, and security programs. The unnamed company produces system engineering and simulation software for several industries including manufacturing, automotive, and aerospace firms. Source: http://www.computerworld.com/article/2600767/security/rigged-industrial-software-site-points-to-watering-hole-attack.html

August 29, KHOU 11 Houston – (Texas) **Memorial Hermann notifies patients of privacy breach.** A former clinical employee at the Memorial Hermann Health System in Houston accessed 10,604 patients' electronic medical records without authorization from December 2007 to July 2014, the hospital announced August 29. Patients' were notified that their names, dates of birth, addresses, and some Social Security numbers were viewed in the breach. Source: http://www.khou.com/story/news/health/2014/08/29/memorial-hermann-notifies-patients-of-privacy-breach/14826833/

August 29, WRAL 5 Raleigh – (North Carolina) **Patient info stolen from Duke Health office.** Duke University Health System notified patients August 29 that an unencrypted thumb drive containing patients' names, medical record numbers, and physicians' names was stolen from an administrative office in Durham in July. Source: http://www.wral.com/patient-info-stolen-from-duke-health-office/13936465/

August 29, New Orleans Times-Picayune – (Louisiana) **Louisiana experiences second data breach with state-issued debit cards.** JP Morgan Chase notified Louisiana's government that the company's security system was breached and hackers may have accessed the personal information of residents using prepaid debit cards issued by 3 State agencies. Source: http://www.nola.com/politics/index.ssf/2014/08/louisiana_experiences_second_d.html

September 2, Softpedia – (International) **FBI starts investigation of celeb photo hack.** The FBI stated that it began an investigation to identify and apprehend the individuals behind a leak of personal photos belonging to several celebrities that were stored in Apple's iCloud service. Source: http://news.softpedia.com/news/FBI-Starts-Investigation-of-Celeb-Photo-Hack-457278.shtml

September 2, The Register – (International) **SHARE 'N' SINK: OneDrive corrupting Office 2013 files.** Users of Microsoft's OneDrive cloud service began reporting August 27 that some Microsoft Office 2013 files stored on OneDrive were inaccessible. Users found that only individuals running Windows 8.1 appeared to be affected and that syncing OneDrive to a computer running Windows 7 would make the files accessible again. Source: http://www.theregister.co.uk/2014/09/02/share_n_sink_onedrive_corrupting_office_2013_files/

September 2, The Register – (International) **iOS phone phlaw can UNMASK anonymous social media users.** Researchers found that users of iOS devices could have their phones forced to dial numbers without prompting or have photos taken through their phone's cameras due to a feature in iOS that is not properly implemented in several popular services such as Twitter, Google, and Facebook. Source: http://www.theregister.co.uk/2014/09/02/crap_ios_schema_can_reveal_anonymous_social_media_users/

September 1, Securityweek – (International) **Tor-enabled Bifrose variant used in targeted attack.** Trend Micro researchers identified a new variant of the Bifrose backdoor after it was used in an attack on an unnamed device manufacturer. The new variant uses the Tor network for command and control communications and can perform actions including downloading and uploading files, deleting content, and performing actions as the infected user. Source: http://www.securityweek.com/tor-enabled-bifrose-variant-used-targeted-attack

August 29, SC Magazine – (International) **Syrian Malware Team makes use of enhanced BlackWorm RAT.** FireEye researchers reported that a hacktivist group known as the Syrian Malware Team has used an enhanced version of the BlackWorm remote access trojan (RAT) known as "Dark Edition" in its campaigns. The new variant allows attackers to bypass user account control (UAC) features, spread itself over network drives, and disable firewalls. Source: http://www.scmagazine.com/syrian-malware-team-makes-use-of-enhanced-blackworm-rat/article/368902/

North Korean tactics in cyber warfare exposed

CNet, 2 Sep 2014: North Korea's cyber warfare capabilities are on the rise despite being entrenched in aging infrastructure and dampened by a lack of foreign technology. According to a report released by Hewlett-Packard researchers, the so-called "Hermit Kingdom" may keep Internet access from the masses and maintain an iron grip on information exchange, but this hasn't stopped the country from training up the next generation of cybersecurity and cyber warfare experts. According to HP, the country is "remarkably committed" to improving its cyber warfare capabilities. South Korea views the regime's cyber capabilities as a terroristic threat, and has prepared for a multifaceted attack in the future -- although it is important to note no such attack has yet occurred. According to a report written by Captain Duk-Ki Kim, a Republic of Korea Navy officer, "the North Korean regime will first conduct a simultaneous and multifarious cyber offensive on the Republic of Korea's society and basic infrastructure, government agencies, and major military command centers while at the same time suppressing the ROK government and its domestic allies and supporters with nuclear weapons." South Korea also claims that North Korea's "premier" hacking unit, Unit 121, is behind the US and Russia as the "world's third largest cyber unit." In 2012, South Korea estimated that North Korea's hacking team comprises of roughly 3000 staff, while a report released by South Korean publication Yonhap upgraded this figure to 5900. According to the PC maker, it is difficult to gather intelligence on the isolated North Korea's hacking teams. Reports not only often come from the US and South Korea, but reports coming from the latter may be biased due to the political tension between the two regions. Another problem is North Korea's heavy restriction on Internet use, which is censored by the state and only used by the social elite. However, this means that any attacks originating from the country are highly likely to be state-sponsored, and rogue actors are unlikely to exist. As cyberattacks will therefore be attributed to the country's governing body, HP says that many attacks sponsored by the regime originate from other countries, including China, the US, Europe, and even South Korea. North Korea's Reconnaissance General Bureau (RGB) is in charge of both traditional and cyber operations, and is known for sending agents abroad for training in cyber warfare. The RGB reportedly oversees six bureaus that specialize in operations, reconnaissance, technology, and cyber matters -- and two of which have been identified as the No. 91 Office and Unit 121. The two bureaus in question comprise of intelligence operations and are based in China. The RGB also reportedly oversees state-run espionage businesses located in 30 to 40 countries, often hosted in unsuspecting places such as cafes. Members of this espionage network reportedly "send more than $100 million in cash per year to the regime and provide cover for spies," the report says. In addition, the country's Worker's Party oversees a

faction of ethnic North Koreans living in Japan. Established in 1955, the group -- dubbed the Chosen Soren -- refuse to assimilate in to Japanese culture and live in the country in order to covertly raise funds via weapons trafficking, drug trafficking, and other black market activities. The group also gathers intelligence for the country and attempts to procure advanced technologies. Despite aging infrastructure and power supply problems, North Korea reportedly was able to gain access to 33 of 80 South Korean military wireless communication networks in 2004, and an attack on the US State Department believed to be approved by North Korean officials coincided with US-North Korea talks over nuclear missile testing in the same time period. In addition, a month later, South Korea claimed that Unit 121 was responsible for hacking into South Korean and US defense department networks. North Korea also tested a logic bomb in 2007 -- malicious code programmed to execute based on a predefined triggering event -- which led to a UN sanction banning the sale of particular hardware to the country. According to the report, the regime regularly exploits computer games in order to gain financially and orchestrate cyber attacks. In 2011, South Korean law enforcement arrested five men for allegedly collaborating with North Korea to steal money via online games, specifically the massive multiplayer online role-playing game (MMORPG) "Lineage." The games were believed to act as conduits for North Korea to infect PCs and launch distributed denial of service (DDoS) attacks against its southern neighbor. However, it is worth noting that North Korea's DDoS capabilities are lacking as there are few outgoing connections due to heavy censorship and Internet restriction. This is why researchers believe the country uses the networks of other nations and botnets instead. The full HP report is available here (.PDF). The analysis is based on open source intelligence gathered HP's security team. To read more click HERE

Former NSA Chief Says JPMorgan Hack May Be a Warning

Bloomberg, 2 Sep 2014: Hackers who stole gigabytes of data from JPMorgan Chase & Co. may have been trying to send a message that U.S. financial institutions can be disrupted, the former director of the National Security Agency said The FBI is investigating the cyberattack on JPMorgan and whether other banks were penetrated in retaliation for U.S.- backed sanctions on Russia, according to people familiar with the investigation who asked not to be identified because the probe is still underway. Keith Alexander, the NSA director from 2005 until last March, said he had no direct knowledge of the attack though it could have been backed by the Russian government in response to sanctions imposed by the U.S. and EU over the crisis in Ukraine. "How would you shake the United States back? Attack a bank in cyberspace," said Alexander, a retired U.S. Army general who has started his own cybersecurity company to sell services to U.S. banks. "If it was them, they just sent a real message: 'You're vulnerable.'" As NSA chief and head of the U.S. Cyber Command, Alexander tracked and tried to thwart international hackers, giving him knowledge of their tactics. He was head of the NSA in 2008 when the country of Georgia was invaded by Russia and experienced a series of disruptive cyberattacks believed to be the work of Russian hackers. The hackers who attacked JPMorgan, the biggest U.S. bank, were "a group with exceptional skills or a nation-state backed group," Alexander said in an interview. The attack occurred last month and resulted in the loss of gigabytes of sensitive data, said the people familiar with the investigation. Authorities are investigating whether recent infiltrations of major European banks using a similar vulnerability are linked to the attack, one of the people said. Security experts say the sophistication of the attacks appeared to be beyond the capability of ordinary criminal hackers. The incidents occurred at a low point in relations with Russia as the West tightens sanctions aimed at crippling Russian companies, including some of the country's most important banks, over its suspected support for Ukrainian rebels. JPMorgan spokeswoman Patricia Wexler declined to comment on Alexander's claims. She noted that the company in statements it issued last week said it is cooperating with investigators, has enhanced its security and hasn't seen any unusual fraud levels. Spokesmen for the FBI had no immediate comment on Alexander's assessment. The attack could have been intended to give U.S. policymakers pause as they are making international and economic decisions, Alexander said. "If you can steal the data -- if you can reach in that far and steal it -- you can do anything else you want," he said. "You collapse one bank and our financial structure collapses." JPMorgan Chief Executive Officer Jamie Dimon, 58, has warned shareholders in annual letters that hackers' efforts to breach the bank's computers were growing more

frequent, sophisticated and dangerous. The bank expects to boost annual spending on cybersecurity by 25 percent to about $250 million by the end of the year from 2013 levels, he wrote in April. To read more click HERE

Home Depot Looks Into Massive Credit Card Breach

SoftPedia, 2 Sep 2014: A large cache of credit card data available for sale on an underground forum is believed to belong to customers of American retailer Home Depot. Information from several financial institutions about a possible breach on the systems of Home Depot stores was received by security blogger Brian Krebs, who noticed a sizable amount of stolen credit and debit card details going on sale on underground store rescator[dot]cc. The store is used by cybercriminals to trade such data and it is the same one used by crooks to move card information stolen from P.F. Chang's PoS systems. Krebs believes that the alleged compromise of the Home Depot computer network has been carried out by the same attackers responsible for the incident that affected Target. Paula Drakes, spokesperson for Home Depot, has confirmed that the company is currently investigating the security breach claims. "I can confirm we are looking into some unusual activity and we are working with our banking partners and law enforcement to investigate," Drakes told the reporter. Although the incident has not been confirmed, the company is ready to take the necessary measures for protecting the customers. Krebs says that his contacts at the banks reporting the stolen credit card information believe that the hack could go as far back as late April or early May, 2014. If this is true, this incident could be much larger than the one that affected retailer Target towards the end of last year, which lasted for about three weeks and ended with credit and debit card information of 40 million customers being stolen. To read more click HERE

Windows 7 Users Getting BSODs after Installing KB2993651 Update

Softpedia, 3 Sep 2014: One of the updates that Microsoft rolled out in last month's Patch Tuesday cycle was causing really big problems on Windows 7 computers, as many experienced a BSOD after installing the KB2982791 patch. Soon after learning about the issues that hit users' computers, Microsoft decided to remove the download links and request those who had already installed the faulty updates to remove them to temporarily address the BSOD-causing problems. Two weeks later, Microsoft came up with a revised patch, this time named KB2993651, which was said to address all problems and thus install successfully even on computers that were previously getting the infamous Blue Screen of Death. It turns out, however, that despite all these revisions, some users are still getting errors after installing the patches, and removing basically all botched updates is the only way to get the affected systems up and running once again. "I first encountered the blue screen after installed KB2982791. Then uninstalled KB2982791 per Microsoft's suggestion. Now I've install the new patch KB2993651. However, the blue screen issue is reproducible ONLY after applying KB2993651 (uninstall it will let the blue screen go away)," one user explained on the company's Community forums. Another user has already confirmed a similar behavior, explaining that the new patch must be hidden in order to avoid getting it installed after removing it to address these issues. "I have experienced the same thing - although I did not initially install KB2982791. I just did the update Sunday (8/31) - well after MS removed that patch that was included in MS14-045. But KB2993651 was included in the latest update - as soon as it was applied, BSOD. I was able to get into Safe Mode to uninstall the update. This allowed me to start my PC as expected. Note I also turned off the Automatic Updates as it kept installing the patch over and over," another user posted. At this point, it's not yet clear how many users are actually affected by the problem, but it's very likely just an issue that's hitting only a small number of computers. In case you're getting the same errors, it's better to uninstall the recently released updates, including the KB2982791 and KB2993651, to make sure that no BSODs are caused to your computer. Additionally, you can hide both of them in Windows Update to prevent them from being offered in the future, but keep an eye on new Microsoft patches to make sure that your computer is fully updated and secure. To read more click HERE

Stealthy Malware Leaves No File on the System

Softpedia, 3 Sep 2014: A new cyber-attack has been spotted to be launched by Angler exploit kit, a memory-residing malware that creates no file on the victim's computer. The threat is delivered via a drive-by download and the code is injected straight into the web browser process, leaving no trace of infection. French malware researcher Kafeine discovered that the new malware was not picked up by his regular security solutions and evaded detection of a host-based intrusion prevention system (HIPS) he relied on. When the victim lands on a compromised website, they are redirected to a malicious page that serves the exploit kit. The web browser is then scanned for outdated versions of software known to have vulnerabilities; this includes Adobe Reader, Flash Player and Java. Angler exploit kit then exploits the security flaw and adds the malware in the memory of the system (RAM). The next stage of the attack is to inject malicious code into the web browser, offering the possibility to steal sensitive information such as account credentials. According to Kafeine, the malware is not placed on the hard disk, which denies persistence on the system. This means that a computer reboot eliminates the malware. Although it's so easy to be removed, the malicious file may not need to survive a restart to complete its task, as it can act as a one-time stealer to exfiltrate the information. The attackers may also rely on this stealthy tool to collect intelligence about the victimized system (e.g. enumerate running processes) in preparation for a targeted attack with malware specially crafted to evade detection from available security products. The researcher says that catching the malware is difficult, as it has to be pulled from the memory or from the recorded traffic and then be decoded. This is not the first time memory malware has been discovered. The method has been previously used by attackers, but generally such threats are used as droppers for persistent malware. In a recent case, it was discovered that a memory-residing malware dubbed Poweliks by researchers at G Data achieved persistence by creating an autostart entry in the registry, allowing it to be deployed when the OS started. The entry contained two sets of code, one of them being a PowerShell script responsible for decoding and executing shellcode that injected a DLL in the memory. The next step was to contact a remote command and control server for instructions, which could be to download a malicious file. To read more click HERE

How hackers spent months pulling bank data from JPMorgan

ARS Technica, 29 Aug 2014: JPMorgan Chase CEO Jamie Dimon said attacks were "going to be non-stop." It looks like he was right. Steve Jurvetson The electronic attack on JPMorgan Chase's network, now under investigation by federal law enforcement, apparently spanned months, according to a report by Bloomberg News. Starting in June, hackers used multiple custom-crafted bits of malware to infiltrate the bank's infrastructure and slowly shipped bits of bank transaction data back out through computers in several countries before it was sent onward to Russia. The attack, which went on for more than two months before being detected by JPMorgan in a security scan, bears the fingerprints of similar long-game attacks against corporate targets by cybercriminals from Eastern Europe, some of whom have developed capabilities more advanced than state-sponsored hackers. While the details obtained by Bloomberg's Jordan Robertson and Michael Riley are sparse, the information provided by their sources is consistent with attacks on a number of European banks earlier this year. The JPMorgan attackers gained entry by exploiting a security flaw in one of the company's websites. From there, they were able to penetrate the bank's data center and gain access to systems with account data, Bloomberg reports, all the while using tools that indicated they had gained knowledge about the company's internal systems. Using custom-crafted malware, the hackers then moved laterally within JPMorgan's data center to other systems and gained access to systems with data on customer banking transactions. Additional malware began transmitting some of this data back to a command and control network with servers in multiple countries, including Brazil. Those servers then relayed data back to a computer in "a large city in Russia," according to a Bloomberg source. Because of the multiple layers of the attack and the use of custom "zero-day" code in each of them, Bloomberg's sources said that JPMorgan's security team believed it was the target of "something more than ordinary cybercrime." But such sophisticated attacks have already become the hallmark of Eastern European electronic crime rings, which frequently use custom code developed specifically to stay under the radar of target companies for long periods. The recent attacks on Neiman-

Marcus, Target, and other retailers are examples of such long-game hacks that infiltrated corporate networks with malware designed specifically for their systems (in those cases, by attacking point-of-sale systems). The sophistication of these criminal attacks is in some cases superior to hacks undertaken by state-financed hackers. In a discussion with Ars last year, Trend Micro Chief Technology Officer Raimund Genes said that the alleged Chinese government-sponsored attacks on The New York Times and other media outlets had, in his view, been uncovered largely because they lacked the finesse found in Eastern European cybercrime rings. Russian Internet crime rings have for some time been accused of acting as a sort of "cyber-militia" for the Russian government, coordinated loosely through indirect ties to Russian law enforcement, intelligence, and military organizations. There may also be some cross-pollination between the Russian government and criminal hacking communities; researchers at security software provider SentinelOne's Labs in July found "intelligence agency grade" carrier malware designed to target government agencies being used by Russian cybercriminals to deliver crimeware to targets. In April, JPMorgan Chase CEO Jamie Dimon told reporters on an earnings call that while the bank's Web servers were not vulnerable to the Heartbleed encryption bug, JPMorgan was bracing for continuous threats similar to Heartbleed. "This is going to be non-stop," he said. In a letter to shareholders that same month, Dimon said that the company was increasing its investment in network security. "By the end of 2014, we will have spent more than $250 million annually with approximately 1,000 people focused on the effort," Dimon wrote. "This effort will continue to grow exponentially over the years. We're making good progress on these and other efforts, but cyberattacks are growing every day in strength and velocity across the globe." Dimon admitted that there was no end in sight to the threat from determined, well-financed attackers. "It is going to be a continual and likely never-ending battle to stay ahead of it—and, unfortunately, not every battle will be won," he wrote. It would seem that Dimon's prediction was prescient. To read more click **HERE**