THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

21 August 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

August 20, The Register – (International) **Cryptolocker flogged on YouTube.** Two researchers reported that cybercriminals have been observed to use purchased ad space on YouTube in order to redirect users to malicious sites serving the Cryptolocker ransomware. The researchers are scheduled to present at the Virus Bulletin 2014 conference detailing how legitimate ad networks could be used to spread malware. Source: http://www.theregister.co.uk/2014/08/20/cryptolocker_flogged_on_youtube/

August 20, Securityweek – (International) **Vulnerability in WordPress Mobile Pack exposes password-protected posts.** Researchers with dxw Security identified and reported a vulnerability in the Mobile Pack plugin for WordPress that could allow access to password-protected posts. The vulnerability was reported July 24 and closed August 19 with the release of Mobile Pack version 2.0.2. Source: http://www.securityweek.com/vulnerability-wordpress-mobile-pack-exposes-password-protected-posts

August 19, IDG News Service – (International) **'Reveton' ransomware upgraded with powerful password stealer.** Avast researchers analyzed a new variant of the Reveton ransomware that now includes the Pony password and virtual currency stealer and a Papras family password stealer that can also disable security programs. The new variant was also programmed to check if an infected user had visited the Web sites of 17 German banks. Source: http://www.networkworld.com/article/2466981/reveton-ransomware-upgraded-with-powerful-password-stealer.html

August 19, SC Magazine – (International) **Bug in iOS Instagram app fixed, impacts Facebook accounts.** IOActive researchers reported that an issue in the Instagram app for iOS could leave users open to having their Facebook access token intercepted over public Wi-Fi due to the app sending the token in plain text. The issue was fixed in Instagram version 6.0.4 and users were advised to update to the latest version. Source: http://www.scmagazine.com/bug-in-ios-instagram-app-fixed-impacts-facebook-accounts/article/367039/

August 19, New Orleans Times-Picayune – (Louisiana) **Restaurant Mizado Cocina says customer credit card data breached by hacker.** The New Orleans restaurant Mizado Cocina notified about 8,000 customers that their payment card information, including names, card numbers, and CVV security codes, may have been breached after the business discovered that a hacker installed malware known as Backoff on the restaurant's point of sale system May 9. The restaurant's IT company replaced affected computer hardware and the business's point of sale system was secured July 18. Source: http://www.nola.com/business/index.ssf/2014/08/restaurant_mizado_cocina_says.html

This Is Not a Flash Drive, It's an ADATA Disk on Module SATA SSD

Softpedia, 21 Aug 2014: Some PCs just don't have a lot of space inside, if any at all for 2.5-inch or smaller storage devices. Still, no computer can work without some storage capacity. Knowing this, ADATA has created what essentially amounts to flash drives which have SATA ports instead of USB. The company calls it Disk on Module SATA SSD, since SSDs are, technically, what all NAND Flash-based storage devices are, in a sense. The newcomer has SATA III 6.0 Gbps support and is made from MLC NAND Flash chips. Its read and write speeds aren't that high, at 250 MB/s and 40 MB/s, respectively, but it's not like the things are expected to be used in servers or PCs. No, they're made for industrial computers, network infrastructure hubs, even medical systems. That said, the endurance is pretty high at 1 million hours, the power consumption is a tiny 1.15W, and the temperature support is of -40°C and 85°C / -40 °F to 185 °F. Essentially, the ADATA SATA III 6 Gbps 7-pin Disk-On-Module (DOM) can work in any machine that is expected to be used in unfriendly environments. Both horizontal and vertical pin orientations exist, in 8 GB, 16 GB and 32 GB. Prices, alas, are unknown. To read more click HERE **[NOTE: These drives could potentially be used for cyber espionage, since they don't communicate via more commonly monitored USB ports]**

Microsoft: This Month's Updates Can Lead to a "Horrible User Experience"

SoftPedia, 21 Aug 2014: The Windows updates released by Microsoft this month as part of the Patch Tuesday cycle caused quite a lot of trouble for those running the company's operating system, with many revealing that in some cases they're getting a BSOD every time they reboot their PCs. Microsoft hasn't talked too much about this issue, but the company has said that a fix is on its way, although no timing has been provided as to when this eagerly awaited patch could be shipped. A Microsoft employee has however taken to the Community forums to provide more information about the botched updates, explaining that if something goes wrong with this month's patches, it would all lead to a "horrible user experience." That's the reason Microsoft decided to pull the updates, Kurt Phillips says, but the company is working hard to provide a fix. "Everyone else - please be aware that the reason we pulled this patch was that IF you ran into the problem specified, it's a horrible user experience," the Microsoft employee explains. "We made a fairly invasive change in font handling as part of a security patch and thought we had it tested properly, but there are definitely problems in our test coverage and design process that we need to address. We definitely have lessons to learn from this and we will." As compared to what people think, only 1 in 10,000 computers are affected by the botched updates, Phillips says, but Microsoft is taking the issues seriously anyway. And still, he adds, in case you haven't received a BSOD until now, it doesn't necessarily mean that you're perfectly secure. "If you installed and haven't seen a Stop 0x50, there's no guarantee you won't see one before we fix it, but look at the odds. I think it would be irresponsible to say in the security bulletin to not uninstall due to the severity of the problem IF you hit it, but I'm not uninstalling. You need to make your own decision on that of course," he explains. Everyone experiencing this issue should contact Microsoft support as soon as possible, as no details regarding the release date of the fix are available right now. As far as Kurt Phillips' job at Microsoft is concerned, he says that he's "not the official Microsoft spokesperson on this, just an engineer on a very busy graphics team trying to fix our problem." You can read his message in full after the jump, and in case you're experiencing these issues already, you can have a look at this workaround to try fix them. To read more click HERE

Microsoft Rolls Out Major Skype Update to Fix Critical Notification Bug

Softpedia, 21 Aug 2014: If you're using Skype on multiple devices, you most likely know that, in some cases, when talking to a friend on a laptop, both the phone and smartphone are buzzing every time you receive a new message. The same is happening on pretty much every device where you are logged in with your Skype username and password. Contrary to what some people believed, this is actually a critical bug, and although plenty of users had reported it already, Microsoft apparently needed quite a lot of time to repair it. Today the company has introduced what it calls active endpoint, a new feature "designed to only deliver chat notifications to the device that you're currently using." While Microsoft doesn't call it a

bug fix, but rather a new feature, active endpoint finally solves a problem that has been extremely annoying for avid Skype users, especially when chatting with friends on a regular basis. Microsoft says that, when you stop chatting with someone on Skype, all the other devices will start buzzing again when receiving a new message "to make sure you never miss anything important." Of course, once you read the message on one of the devices where you're logged in, all the others are automatically switched to silent mode. "If you are signed in to Skype on multiple devices (a laptop, tablet and a smartphone) and you are sending chat messages to a group of friends from your tablet," the company explains. "Skype will only send new message notifications to your tablet and not to any of your other devices. All of your other devices will remain blissfully silent. You can continue to focus on the most important thing, your conversations, without being disturbed by the bleeping and buzzing from all of your other devices." This feature does not affect chat history, as the whole conversation that you have on one device is automatically synchronized to all the other devices where Skype is logged in. This way, you can continue from where you left off, as long as the latest version of Skype is installed. And speaking of versions, Microsoft says that it's absolutely mandatory to run the very latest update to make sure that you're benefitting from these improvements, so go ahead and download Skype right now to get active endpoint too. "To make sure that you get the full active endpoint experience, please make sure that all of your devices are running the most up-to-date versions of Skype," it says. To read more click **HERE**

51 UPS Locations Hit by Point-of-Sale Malware

SoftPedia, 21 Aug 2014: On Wednesday, UPS announced its customers that the systems of 51 of their franchised center locations, in 24 states, have been compromised by malware stealing credit and debit card details. The company received a government bulletin that informed of a point-of-sale (PoS) threat affecting multiple retailer across the US, and which went undetected by antivirus solutions. After analyzing their systems, the company determined that multiple locations were infected by the malware described in the government bulletin. They asserted that details about credit and debit cards useds at one of the 51 affected locations between January 20, 2014 and August 11, 2014 has been exposed to unauthorized individuals. The information exposed consisted in names, postal addresses, email addresses and payment card details, but not all of them were attached to each affected customer. However, in the announcement of the incident, UPS says that in most cases "the period of exposure to this malware began after March 26, 2014." On August 11, the malware, which is believed to be the recently discovered Backoff, has been removed from all impacted UPS locations and customers were able to make purchases securely from then on. "As soon as we became aware of the potential malware intrusion, we deployed extensive resources to quickly address and eliminate this issue. Our customers can be assured that we have identified and fully contained the incident," says Tim Davis, president of The UPS Store, Inc in a communication. The network of UPS stores comprises a total 4,470 franchised center locations throughout the United States, the 51 stores involved in the incident representing about one per cent. According to the company, franchised centers run on independent private networks, separate from other centers of the same kind. "Same as with the recent Community Health System breach, this is another example of how persistent attackers were able to successfully plant their attack tool. Enterprises are now coming to a conclusion that they are either already compromised, or will soon be. It's not a matter of 'if', it's a matter of 'when'," Aviv Raff, chief researcher at Seculert, told us via email. Ars Technica was tipped off by a reader that sent them a copy of the government bulletin received by UPS. It is dated July 31, a date that coincides with an alert issued by US CERT (Computer Emergency Readiness Team) about Backoff PoS malware infecting on various US retailers' payment devices. The bulletin includes an analysis of the malware, performed by security resarchers from Trustwave Spiderlabs, also consistent with the CERT announcement at the end of July. Backoff and its variations have been detected since at least October 2013 and it is equipped with memory scraping capabilities, which allows extraction of sensitive information available in the memory of the system. The report says that threat actors scan the systems for the presence of a remote desktop protocol and then abuse its log-in with brute-force attacks in order to find the credentials. Apart from scraping memory for track data, the malware can also record key strokes and communicate with a command and control server. US CERT's advisory notes that "at the time

of discovery and analysis, the malware variants had low to zero percent anti-virus detection rates, which means that fully updated anti-virus engines on fully patched computers could not identify the malware as malicious." However, after the publication of the report, more and more antivirus vendors updated their malware detection mechanisms to catch this type of threat and its variants. To read more click **HERE**

38-Day Long DDoS Siege Amounts to Over 50 Petabits in Bad Traffic

SoftPedia, 21 Aug 2014: A massive DDoS attack directed at an undisclosed video game company due to an alleged business feud, lasted no less than 38 days and spewed over 50 petabits of malicious traffic at the target. The perpetrators used extremely large DNS floods for the entire duration of the attack that started on June 21 and ended on July 28, channeling several tens of millions of requests per second, according to Incapsula, who mitigated the incident from start to end. The company said in a blog post that the offenders "tried everything from massive network layer DDoS attacks to focused application layer (HTTP) floods, followed by dozens of SQLI and XSS attempts." On a regular basis, they relied on at least two of these attack vectors but they often ramped things up with five-vector attacks. Incapsula says that the largest amount of packets was over 90 million per second, totaling a bombardment of more than 110 Gbps. Their DNS infrastructure was also hit with large SYN floods, in an attempt to disrupt the protection of the targeted service. Suspicion of a business feud being at the root of the incident is supported by the fact that the attackers had sufficient firepower in their hands and were extremely determined in their activity. "The 'business feud' theory is reinforced by the resources used during the attack. Looking at source IP data, Incapsula noticed the majority of malicious packets were originating from the same IP ranges. We knew that 20% of C-classes are typically responsible for ~80% of all DDoS traffic," Incapsula says. The resources leveraged in the incident were far from being consistent with an off-the-shelf botnet for hire capable of short-lived 20 Gbps blasts, which could be purchased on underground forums for a few hundred US dollars. An offensive lasting this long with capability to generate 90+ Gbps of unamplified DDoS traffic is clearly the work of professionals who DDoS for a living. The long-lasting event was handled by Incapsula using a single "Behemoth" scrubbing server, which is capable of processing up to 170Gbps or 100Mpps worth of traffic. The company under attack had contracted the DDoS mitigation services from Incapsula just a day before the incident started. At the time of the event Behemoth had spent a month being tested internally. It goes without saying that Incapsula is mighty proud of their technology, especially after proving itself in an incident of this magnitude. To read more click **HERE**

Stanford University Webpage Defaced

Softpedia, 21 Aug 2014: The webpage of the Stanford University portal has been defaced by a hacker in an attempt to draw attention on the lax security in some parts of the website. The deed is claimed by a hacker going under the online alias of SaHoo, the same one that modified the looks of the personal agenda page of a professor at MIT. This time, the target was the page of Bonnie McLindon, a Stanford graduate (B.S. Computer Science) class of 2014, currently working at US-based data analysis company Palantir Technologies. SaHoo told us via email that he is not affiliated with any hacker group and that the stunt on the MIT portal was pulled just as a friendly hack, to demonstrate that security needs to be enforced in some areas. It appears that in the case of the Stanford page there was the same goal, as he informed us that no files have been damaged in any way. The defacement is nothing dirty, just a message informing that SaHoo managed to break in, with the same audio background. Originally, the page would present some details about a project on programmable shading, presenting the results of two experiments: Eggcrate Mattress and Tea and Donuts. All the information on the page seems to be from two years ago. To read more click **HERE**

Critical Delphi and C++Builder VCL library bug found

Heise Security, 21 Aug 2014: A buffer overflow vulnerability that could be exploited to execute malicious code has been discovered in the Visual Component Library (VCL) library of Embarcadero's Delphi and C++Builder application development environments, and could, therefore, also affect applications that were built by using the software and that use the affected library. The issue was first discovered by a Core

Security researcher. "Marcos Accossatto from our Exploit Writing team detected the vulnerability on an affected application by manually changing some values in the BMP header of a sample image, later confirming the finding on a set of image handling applications," explained Flavio De Cristofaro, the company's VP of Engineering for Professional Products. "While manipulating the BMP file, it was observed that some applications of the set would crash. That led us to assume a software library common to all the applications was probably responsible for the crash, which led us to the culprit." "C++Builder and Delphi have been used in software development for many years. Financial institutions, healthcare organizations and companies in several other industries have developed homegrown applications using these products," he noted, and said that it's difficult to say which specific software is affected. The vulnerability can be exploited locally, if a user is made to open a malformed BMP file on the affected application. "Even when a Client Side attack seems to be the most likely attack vector, some applications allow a remote user to upload malformed files. In this case, the affected application could be remotely exploitable," De Cristofaro added. Once the vulnerability has been exploited, the attacker has the same permission level of the user running the vulnerable app. This often translates into the capability to execute whatever program he or she wants. The vulnerability has been patched and, depending on the Delphi and C++ Builder versions, users can do several things. To read more click **HERE**

Analysis reveals many malicious Chrome extensions

Heise Security, 20 Aug 2014: An analysis of 48,332 browser extensions from the Chrome web store has revealed 130 outright malicious and 4,712 suspicious extensions, some of which have been downloaded by millions of users. "The amount of critical and private data that web browsers mediate continues to increase, and naturally this data has become a target for criminals. In addition, the web's advertising ecosystem offers opportunities to profit by manipulating a user's everyday browsing behavior," the researchers noted in the paper detailing their findings. "As a result, malicious browser extensions have become a new threat, as criminals realize the potential to monetize a victim's web browsing session and readily access web-related content and private data." To analyze the extensions, the researchers used Hulk, a dynamic analysis system of their own making, which flushes out the extensions' malicious behaviour. "First, Hulk leverages HoneyPages, which are dynamic pages that adapt to an extension's expectations in web page structure and content," they explained. Second, Hulk employs a fuzzer to drive the numerous event handlers that modern extensions heavily rely upon." Among the malicious extensions they found, some perpetrated affiliate fraud and credential theft, others performed ad injection or replacement, and others still abused social networks for spamming. To read more click **HERE**

86% of hackers don't worry about repercussions

Heise Security, 14 August 2014: Thycotic announced the results of a survey of 127 self-identified hackers at Black Hat USA 2014. The survey found that 86% of hackers are confident they will never face repercussions for their activities. In a double-edged sword conundrum, 88% of respondents also believe their own personally identifiable information (PII) is at risk of online theft. Asked which types of employees they would most likely target first in order to gain login credentials for a particular company, 40% of the hackers polled indicated they would start with a contractor. This is especially relevant, given that Edward Snowden was a contractor, and used his privileged access to steal sensitive NSA documents. Additionally, 30% of respondents would first target IT administrators, highlighting the importance of locking down access controls to privileged accounts. Other key findings from the survey include:

- More than half (51%) of hackers say their actions are motivated by fun/thrill seeking, while only 18% say they are motivated by financial gain.
- Meanwhile, 29% claim they are motivated by social consciousness or a moral compass.
- 99% of respondents believe that simplistic hacking tactics such as phishing are still effective.
- 53% of hackers do not believe users are learning to avoid such tactics.

"Understanding why hackers do what they do is the first step as IT security teams take measures to better control and monitor access to company secrets. Organizations need to do a better job of protecting the passwords and privileged login credentials associated with contractors and IT administrators, as these employees are a huge target for cybercriminal activity." To read more click **HERE**

PGP is fundamentally broken, says crypto expert

Heise Security, 15 Aug 2014: "It's time for PGP to die," Matthew Green, noted cryptographer and research professor at Johns Hopkins University, opined in a recent blog post. "Zimmermann's PGP was a revolution. It gave users access to efficient public-key cryptography and fast symmetric ciphers in package you could install on a standard PC. Even better, PGP was compatible with legacy email systems," he noted. "Sure, it sucked badly to use. But in those days, everything sucked badly to use." "While the protocol has evolved technically -- IDEA replaced BassOMatic, and was in turn replaced by better ciphers -- the fundamental concepts of PGP remain depressingly similar to what Zimmermann offered us in 1991," he concluded. There are many problems with PGP, he notes. Its public keys are long, difficult to manually compare, and often times gotten from key servers via untrustworthy data transfer channels. "PGP assumes keys are too big and complicated to be managed by mortals, but then in practice it practically begs users to handle them anyway. This means we manage them through a layer of machinery, and it happens that our machinery is far from infallible," he adds. PGP key management is not transparent and there is no forward secrecy to protect old communications - although there are some experimental systems that are trying to fix both these problems. "The OpenPGP format and defaults suck," says Green. "Poking through a modern OpenPGP implementation is like visiting a museum of 1990s crypto. For legacy compatibility reasons, many clients use old ciphers like CAST5 (a cipher that predates the AES competition). RSA encryption uses padding that looks disturbingly like PKCS#1v1.5 -- a format that's been relentlessly exploited in the past. Key size defaults don't reach the 128-bit security level. MACs are optional. Compression is often on by default. Elliptic curve crypto is (still!) barely supported." To read more click **HERE**

51% of consumers share passwords

Heise Security, 20 August 2014: Consumers are inadvertently leaving back doors open to attackers as they share log in details and sign up for automatic log on to mobile apps and services, according to new research by Intercede. While 52% of respondents stated that security was a top priority when choosing a mobile device, 51% are putting their personal data at risk by sharing usernames and passwords with friends, family and colleagues. The survey of 2,000 consumers also questioned whether these passwords are strong enough to adequately protect consumers' applications and the data they hold. Half of respondents stated that they try and remember passwords rather than writing them down or using password management solutions, suggesting that consumers are relying on easy to remember combinations and using the same password across multiple sites and devices. Richard Parris, CEO of Intercede commented: "As we live more and more of our lives online, all our various digital identities need to be effectively protected – worryingly, it appears that this is not the case at the moment. We need so many passwords today, for social networking, email, online banking and a whole host of other things, that it's not surprising consumers are taking shortcuts with automatic log ins and easy to remember passwords. These solutions are increasingly not fit for purpose though – they do not offer proof of a person's identity and are easily lost, stolen or hacked, leaving consumers at risk of identity theft. It's time for stronger authentication and more sophisticated forms of identity." The research revealed that consumers are not only sharing passwords but also potentially putting their personal and sensitive information at risk by leaving themselves logged in to applications on their mobile devices, with over half of those using social media applications and email admitting that they leave themselves logged in on their mobile device. Worryingly many consumers are also compromising their bank and credit card details by selecting 'Remember me' or 'Keep me signed in' options. Of those that use Amazon and other shopping sites, 21% said they were automatically logged in, while the figures stood at 16% for mobile banking and 12% for PayPal. "Keeping your Facebook, Gmail, shopping and financial accounts automatically logged in

might be convenient for consumers, but it's leaving the back door wide open to hackers," continued Parris. To read more click HERE

US defense contractors still waiting for breach notification rules

Heise Security, 14 August 2014: US Department of Defense contractors will have to wait until September 24 to see what specific rules they will be required to follow when it comes to the reporting of computer breaches to the DoD. This particular requirement has been mandated by the US Congress last year, in an attempt to get clear view of the type and frequency of attacks contractors face. The US Congress will require "cleared defense contractors" - i.e. those who have been granted clearance by the DoD to access, receive, or store classified information - to effect a rapid report in the wake of a successful breach, and to include in it a description of the technique or method used in the penetration, a sample of the malicious software used (if discovered), and a summary of information created for the Department in connection with any Department program that has been potentially compromised due to such penetration. Defense contractors have become preferred targets for cyber spies who, it seems, find their networks easier to breach than those of government departments and agencies. As the companies are waiting for the rules to be punished, they expressed their worry about government agents being allowed to access to their networks so that they can conduct forensic analysis of the attack (in addition to the analysis conducted by the contractor). They are not too happy about the possibility of the Pentagon having access to their trade secrets, commercial, financial, and customer information. Contractors are also eager to see whether the Pentagon will return the favor and share threat information it has with the firms, so that they can be better prepared to fend off attacks. Smaller firms are worried that complying with some of the rules might be too costly and impossible for them, which would ultimately make it impossible to keep and gain new government contracts. What the contractors are really hoping for is some "clear guidance on how to implement whatever requirements the government is looking to put into place," Daniel Stohr, director of communications for the Aerospace Industries Association, said to Bloomberg's Chris Strohm. "We don't want contracting officers giving their personal interpretation of what this rule would or should be," he noted. To read more click HERE