THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

11 July 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

July 10, Securityweek – (International) **CryptoLocker infrastructure used for other threats: Bitdefender.** Researchers with Bitdefender found that the infrastructure for the CryptoLocker ransomware remains active even though a takedown operation in June disrupted the ransomware operation. The infrastructure is currently being used for various fraudulent and malicious purposes including fake antivirus scams and the distribution of the Citadel banking trojan. Source: http://www.securityweek.com/cryptolocker-infrastructure-used-other-threats-bitdefender

July 10, Softpedia – (International) **Exploit kit dropped through Akamai content delivery network.** Malwarebytes researchers found and reported that attackers are abusing the Akamai Technologies Akamaihd.net content delivery network (CDN) to trick users with fake software update notifications to bundle pay-per-install programs and use a malicious iframe to redirect users to an exploit kit. The exploit kit used appears to be the Nuclear Pack exploit kit that targets vulnerabilities in Java, Flash, Internet Explorer, and Adobe Reader. Source: http://news.softpedia.com/news/Exploit-Kit-Dropped-Through-Akamai-Content-Delivery-Network-450214.shtml

July 10, The Register – (International) **Crusty API opened Facebook accounts to hijacking.** A security researcher revealed that a legacy API in Facebook allowed attackers to make REST API calls on behalf of Facebook users if their user ID was known, allowing attackers to update statuses, like content, and upload or delete photos. The flaw was reported to Facebook in April and fixed by Facebook, earning the researcher $20,000 through Facebook's bug bounty program. Source: http://www.theregister.co.uk/2014/07/10/crusty_api_opened_facebook_accounts_to_hijacking/

July 10, Help Net Security – (International) **Nearly 70% of critical infrastructure providers suffered a breach.** Unisys released the results of a survey of 599 security executives in the manufacturing, utility, and energy sectors and found that almost 70 percent of respondents reported at least one security breach that led to a disruption in operations or disclosure of confidential information within the last 12 months. The report also found that data breaches were most often attributed to negligent insiders, among other findings. Source: http://www.net-security.org/secworld.php?id=17100

July 9, Threatpost – (International) **Buffer overflow vulnerabilities in Yokogawa ICS gear patched.** Yokogawa Electric Corporation released patches for its CENTUM and Exaopac industrial control system (ICS) software the week of July 7, closing vulnerabilities that could allow an attacker to remotely execute code. Source: http://threatpost.com/buffer-overflow-vulnerabilities-in-yokogawa-ics-gear-patched/107108

$10,000 (€7,350) to Hack a Tesla Model S

SoftPedia, 11 Jul 2014: At the SyScan security conference in Beijing next week, the organizers will offer a $10,000 / €7,350 prize to the hacker who manages to break into the system of a Tesla Model S car. According to Forbes, the organizers are looking for specific types of attacks that could lead to controlling the car from a computer system or direct the user to certain malware-laden pages in the car's web browser. The reason they chose a Tesla is because the company is security-aware and has implemented a vulnerability disclosure program, which has already helped eliminate the more obvious flaws. The company is not involved in the contest in any way. Among the talks hosted by the conference, there is a presentation from Pk001, a researcher with significant experience in reverse engineering in embedded automotive networks and systems. The presentation is focused on the methods that can be used to prevent car-hacking by building a security system for the automotive network that relies on the Controller Area Network (CAN) protocol. CAN is the most popular protocol in the automotive industry. Because it relies on broadcast bus, messages are also sent to the ECU (engine control unit), posing the risk of an attacker to tamper with various functions of the car. To read more click **HERE**

Gmail for iOS Poses Man-in-the-Middle Attack Risk

SoftPedia, 11 Jul 2014: A vulnerability that allows a potential attacker to intercept encrypted communication between the Gmail app for iOS and the server via the man-in-the-middle (MitM) technique has been reported by security researchers. The flaw resides in the fact that the mobile app does not incorporate the legitimate certificate that validates the server receiving the communication, a feature called certificate pinning. Pinning basically consists in the certificate for the intended server being hard-coded into the client, Gmail for iOS in this case, permitting traffic to be initiated only when it encounters a match at the other end of the line. Because Gmail for iOS devices lacks this feature, cybercriminals could use a rogue certificate to impersonate the server and route all traffic through their systems, thus gaining access to the information in unencrypted form. Certificate pinning is available in the Gmail app for Android, though. Researchers from Lacoon mobile security firm present an attack scenario, involving cybercriminals duping the victim into installing a hostile configuration profile, which adds the unauthorized CA certificate. iOS is vulnerable to this form of attack, which can be carried out by luring the victim to visit a webpage from their device. When the victim runs the Gmail app, all traffic is then routed through the server under the control of the cybercriminals, giving them access to all communication in plain text. Google is very sensitive about security issues in their products, but in this case, they delayed the release of a patch. Lacoon says that they reported the issue more than four months ago, on February 24, and the search giant still has not fixed it. "Lacoon's research team informed Google about this problem on February 24. Google had recognized this flaw and validated it. We were told that they were going to fix this issue though to date, this vulnerability still exists," said Avi Bashan in a blog post. Recently, the National Informatics Centre in India, which was authorized to issue intermediate digital certificates trusted by the Indian Controller of Certifying Authorities (India CCA), was compromised and rogue certificates were found. The full extent of the breach is not known at the moment, but Google took the necessary steps to limit India CAA root certificates to a handful of domains. This shows that organizations handling validation documents are vulnerable to outside attacks that can lead to issuing unauthorized certificates trusted by web browsers and applications implicitly, posing a serious risk to the secure communication of sensitive information. Mitigating the risks depends primarily on the developer. "First and foremost, it's up for the mobile app developer to implement certificate pinning. With enough public concern, let's hope that app developers start listening to their customers and placing the necessary security measures," writes Avi Bashan. To read more click **HERE**

Credit Card Details of 10,000 Exposed in Houstonian Hotel Security Breach

SoftPedia, 11 Jul 2014: A security breach carried out on the systems of the Houstonian Hotel, Club and Spa, with a duration of about six months, led to the exposure of the credit card details of at least 10,000 customers. The management of the retreat was informed by the U.S. Secret Service of a potential attack that targeted the payment processing systems on June 10. It appears that the perpetrators managed to

maintain access to the systems with sensitive information for a period of almost six months, from December 28, 2013 through June 20, 2014. Jason Love, information technology director at the Houstonian Hotel, told Houston Chronicle that immediate measures were taken to secure the customer data, as soon as they received the news from the U.S. Secret Service. "As of June 20, we had fully replaced and overhauled the breached systems, further restricted access to all our servers and hired a data forensics firm to help us enhance our digital security," he said in a statement to the publication. Given the large amount of time cybercriminals had access to the payment systems, the total number of affected customers is not known. The 10,000 customers notified of the breach are only those that provided contact details during their stay at the luxury retreat; they are advised to contact Nora Harding at 713-812-6982. Informing the affected customers is generally done with delay because of the forensic investigation that needs to be conducted in order to determine the risk and the parties impacted. "We wanted to make sure we had all the information before we engaged our members," said Love. When the report of the investigation came out on Tuesday, the company filed a criminal report with the Houston Police Department. They also made available credit monitoring services to the affected customers, free of charge, for one year, which can be used to report fraudulent activities on their bank account. Cybercriminals do not always hurry with selling or using the stolen credit card information. In the case of the P.F. Chang's point-of sale systems breach, the investigation determined that the clients had used their credit cards at the restaurant between the beginning of March and May 19, and the details were advertised for sale only on June 9. However, according to Brian Krebs, the company's restaurants had been leaking the credit card data for a period of nine months, since September 18, 2013, and the total amount of cards compromised may have been around 7.2 million. To read more click **HERE**

Microsoft Issues Emergency Security Update for Windows 8.1

SoftPedia, 11 Jul 2014: Redmond-based tech company Microsoft has released an emergency security update for its modern operating system, including Windows 8.1, to fix an issue that would block exploits grounded in recently discovered digital certificates claiming to come from Google and Yahoo. Microsoft says that more such malicious certificates could be out there in the wild, so it recommends users to accept yesterday's out-of-band update, as it's automatically deployed and installed on computers running Windows 8, 8.1, RT, RT 8.1, Server 2012, Server 2012 R2, Windows Phone 8, and Windows Phone 8.1. The new patch was developed to block 45 different SSL certificates obtained by hackers after successfully breaking into systems operated by the National Informatics Center (NIC) of India, whose certificates are automatically accepted by all Windows versions without any message displayed to users. As you could easily guess, such certificates are being used by quite a lot of websites out there, including online banking, stores, and companies providing you with services such as email. Google and Yahoo services are also said to be affected, so users could be exposed when accessing their products which are using a SSL certificate. Microsoft says that at the moment it's not aware of any successful hacking attempt based on this new threat and adds that thanks to this patch, everyone should be completely secure, at least when running newer versions of Windows. "The subordinate CA has been misused to issue SSL certificates for multiple sites, including Google web properties. These SSL certificates could be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks against web properties. The subordinate CAs may also have been used to issue certificates for other, currently unknown sites, which could be subject to similar attacks," the company explains. While customers running Windows 8 and 8.1 are getting the update automatically, Microsoft says that those who are still on older OS versions won't receive the patch, so additional tweaking is needed. "To receive this update, customers must install the automatic updater of revoked certificates. Customers in disconnected environments and who are running Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 can install update 2813430 to receive this update," it continues. If you're wondering, users whose computers are currently powered by other desktop platforms, including Mac OS X and Linux, are perfectly secure because these operating systems do not trust SSL certificate by default, so no additional patching is required. To read more click **HERE**

Microsoft Software Insecure Due to Users Not Installing Patches

SoftPedia, 11 Jul 2014: A report published by security company Secunia for the second quarter of 2014 in the United Kingdom reveals that 40 percent of the programs running on a Briton's computers are developed by Microsoft, but some of them remain vulnerable to attacks because users simply do not install patches released by the company. According to Secunia data, 31 of 76 programs running on a computer in the United Kingdom are developed by the software giant based in Redmond, while 9.7 percent of the consumers in the country are using unpatched operating systems, including Windows Vista, Windows 7, and Windows 8. While it's hard to find a reason why people don't actually care more about their security, Secunia says that the different mechanism of getting the updates is at fault for users keeping their computers unprotected. "On a typical PC, users have to master 26 different update mechanisms to patch the 76 programs on it, in order to remediate vulnerabilities: 1 single update mechanism for the 31 Microsoft programs that make up 40% of the programs on the PC; another 25 different update mechanisms to patch the remaining 45 programs (60%) from the 25 so-called third-party vendors whose products are on the PC, and who each have a unique update mechanism," Secunia said in a report published today (PDF viewer required to open the document). Microsoft XML Core Services (MSXML) 4.x is the software component found on 74 percent of the computers in the United Kingdom, but according to Secunia data, most users are running an older version that's obviously vulnerable to attacks and could expose data. The reason is the same different update system that's not based on Windows Update, which means that users are required to get the new version manually, thus making it harder especially in the case of beginners. "The reason MSXML is topping the list is because of the way updates for the software are being handled: Normally, patches for Microsoft products are offered through Windows Update, but in the case of MSXML, patches are only offered for MSXML Service Pack 3. Since older MSXML Service Packs are considered End-of-Life, users are not being offered patches as they normally would," Kasper Lindgaard, director of research and security at Secunia, said. Internet Explorer 11, .NET Framework 3.x and 2.x are also among the most popular solutions in the United Kingdom, most of which have already been patched several times by Microsoft. This time, however, Redmond rolled out fixes via Windows Update, so consumers have no excuse for running an older version. To read more click **HERE**

Operating Shylock Trojan Was a Full-Time Job

SoftPedia, 11 Jul 2014: The group behind the Shylock/Caphaw banking Trojan showed their business prowess for the full duration of the operation, by carefully selecting their market, protecting the asset from authorities through detection evasion tactics, and optimizing it for a higher rate of success. This week, the U.K. National Crime Agency coordinated an international effort to take control of the domains used for communication with the machines infected by the banking malware. Among the partners in the operation are both law enforcement organizations and security companies in the private sector. According to Symantec, the cybercriminal gang was organized with professional discipline, as they believe that the developers had a typical nine to five work schedule, from Monday to Friday. This conclusion was also supported by evidence that most binary compilations occurred on weekdays. By observing the activity of the malware, which started as early as July 2011, the security researchers managed to create a profile of the group running it. The cybercriminals are believed to be located in Russia or Eastern Europe and they focused on the financial institutions in the U.K., which, besides having a large online banking customer base, also has numerous wealthy citizens. "Symantec estimates that the gang behind Shylock has stolen several million dollars from victims over the past three years and over 60,000 infections were detected in the past year," says a blog post from the company. Over its lifecycle, Shylock went through numerous modifications that allowed it to continue its activity and bypass the security measures taken against it. Also, thanks to its modular design, the malware developers were able to modify its functionality, as well as increase its complexity. One of the most important aspects is the fact that the cybercrime gang did not share the malicious tool with others and kept it under their control at all time. As such, with no code leaked on underground forums, they were able to maintain a low-profile and keep the spoils to themselves. Symantec notes that they started low and perfected the malware in time, to the point that the advanced man-in-the-browser technique was implemented for performing fraudulent transactions.

"Attackers gain control of the victim's browser by exploiting security vulnerabilities to modify the web pages displayed to the victim. Shylock is also capable of defeating two-factor authentication security mechanisms employed as counter measures at some of these banks," says Symantec. Another technique used by Shylock is automated-transaction-service (ATS); this is designed to run transactions in the background when the user is logged in, and lure them through social engineering techniques to authorize the fraudulent activity. By logging into the online bank account from a Shylock-infected machine, the credentials are sent both to the bank and to the cybercriminals. The attackers assume control of the account, but if a second authorization is required for transferring funds, such as that with a physical token, they cannot steal the money. One social engineering tactic is to pop-up a dialog informing the user that security checks need to be performed to ensure the safety of online banking access. At the end of the process, the victim is prompted to enter the authorization code, an action also purported to be part of the verification process. However, the crooks have already set up the fraudulent transaction and the code is all they need to execute it. By Symantec telemetry, most Shylock infections have been detected in the United Kingdom (30%), followed by the U.S. (16%), Italy (11%) and Brazil (7%). It is delivered through exploit kits (researchers detected the use of Blackhole, Cool, Magnitude, Nuclear Pack, and Styx in the past year), but spam is also an attack vector, with messages carrying items posing as important PDF files, while they are actually executables. Users are advised to run the latest Windows updates in order to prevent Shylock from slipping in or eliminate it if the system is already infected. To read more click **HERE**

17-Year-Old Behind Norway DDoS Attacks This Week

SoftPedia, 11 Jul 2014: On Thursday, the Norwegian police have arrested and charged a 17-year-old in connection to the recent massive distributed denial-of-service (DDoS) attacks directed at major financial institutions and other businesses in the country. The teen, from the city of Bergen, on Norway's west coast, claimed to be part of the hacktivist group Anonymous Norway, who, in a Twitter message, dismissed any connection to him or the DDoS incidents. On the day of the attack, the teenager sent a letter to the media, claiming to be part of Anonymous and saying that "the motivation behind the current attacks and the next attacks in the future is to get the community to wake up. The number of major IT security attacks is increasing and there is nothing being done to prevent such events." Evidence that Anonymous Norway was not involved in the incidents is the fact that the boy joined the group's Facebook page on the same day of the attack. Furthermore, the hacker outfit provided a Pastebin link in a new tweet, pointing to the identity of the perpetrator; they did not create the post, just scooped it up. Initially, the youngster was charged with gross vandalism, which carries a maximum prison sentence of six years in Norway. However, since he has no record and is still a minor, this should be greatly reduced. According to News in English, Frode Karlsen of the Bergen police told Norwegian Broadcasting that the authorities are taking the matter seriously because this sort of attack can have significant impacts on society, like individuals not being able to reach emergency services in case they needed help. After his arrest, the teen cooperated in the investigation and clarified the nature of his actions. His defense lawyer stated that "he's sorry for having caused all this and has laid his cards on the table." The DDoS attack, which occurred on Tuesday, was considered among the largest ever seen in Norway and leveraged the vulnerable "pingback" WordPress feature. Its increased significance is due to the fact that it targeted layers three (network) and four (transport) of the OSI model, as well as layer seven (application), at the same time. Mitigating an application layer DDoS attack is not too easy, because the requests are directed at the application interface and mimic legitimate behavior, which makes filtering out the bad traffic more difficult. The attack aimed at disrupting the online services of major financial institutions in Norway (Norges Bank, Sparebank 1, Storebrand, Gjensidige, Nordea, Danske Bank), as well as other business, like Scandinavian Airlines (SAS) and Norwegian Air. The website of the largest telecommunications company in Norway, Telenor, was also affected. To read more click **HERE**