THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

17 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 16, Securityweek – (International) **Oracle patches 13 vulnerabilities, including 20 in Java.** Oracle released its Critical Patch Update for July, which includes patches for 113 security vulnerabilities in various Oracle products, including 20 vulnerabilities in Java SE. The 20 vulnerabilities in Java can all be remotely exploited without authentication and users were advised to apply the updates as soon as possible. Source: http://www.securityweek.com/oracle-patches-113-vulnerabilities-including-20-java

July 16, Softpedia – (International) **vBulletin exploitable through SQL injection.** Members of the Romanian Security Team group identified and reported an SQL injection vulnerability in vBulletin which could be used by attackers to gain access to a forum's administration panel and databases. The group reported the vulnerability to the developers of vBulletin and stated that they would disclose the full details of the issue once a fix is released. Source: http://news.softpedia.com/news/vBulletin-Exploitable-Through-SQL-Injection-450894.shtml

July 16, Securityweek – (International) **OpenBSD downplays PRNG vulnerability in LibreSSL.** A researcher with Opsmate reported finding a flaw in the pseudorandom number generator (PRNG) in LibreSSL for Linux. Representatives of the OpenBSD Project confirmed that the issue exists but stated that the now-fixed problem was unlikely to be exploitable in real world conditions. Source: http://www.securityweek.com/openbsd-downplays-prng-vulnerability-libressl

Microsoft to Fire 18,000 Employees over the Next 12 Months
SoftPedia, 17 Jul 2014: As expected, today Microsoft announced a massive job cut campaign that's supposed to help the company reduce costs following the acquisition of Nokia's devices and services unit. As compared to what people expected, however, Microsoft is not firing 5,000 people, but 18,000, which is clearly the biggest layoff in the history of the software giant. In a press statement this morning, the company explains that this job cut is expected to be completed by June 30, 2015, so it's going to work at full speed to fully accomplish its goals. "Of the total, about 12,500 professional and factory positions will be eliminated through synergies and strategic alignment of the Nokia Devices and Services business acquired by Microsoft on April 25," Microsoft said. "The company expects to incur pre-tax charges of $1.1 billion to $1.6 billion over the next four quarters, including $750 million to $800 million for severance and related benefit costs, and $350 million to $800 million of asset-related charges," it said. As you can see, most of these layoffs come from the recently-purchased Nokia Devices and Services unit, but a number of existing Microsofties are also said to be let go in the next 12 months. Satya Nadella has already announced in a memo sent to employees last week that he worked with the other executives of the company to analyze the internal organization of each department, but there are no details as to how many people from which departments are expected to be fired. Previous reports on the matter indicated that employees of the Xbox marketing department, but also software testers, would be among the ones affected by this decision; but again, Microsoft is yet to provide more info on this. Satya Nadella said in a statement for employees that those getting fired would receive notifications in the coming six months. "It's important to note that while we are eliminating roles in

some areas, we are adding roles in certain other strategic areas. My promise to you is that we will go through this process in the most thoughtful and transparent way possible. We will offer severance to all employees impacted by these changes, as well as job transition help in many locations, and everyone can expect to be treated with the respect they deserve for their contributions to this company," he explained. Stephen Elop, former Nokia CEO now in charge of Microsoft's Devices unit, said in a letter to employees that severance benefits would be offered to those getting fired. "The team transferring from Nokia and the teams that have been part of Microsoft have each experienced a number of remarkable changes these last few years. We operate in a competitive industry that moves rapidly, and change is necessary. As difficult as some of our changes are today, this direction deliberately aligns our work with the cross company efforts that Satya has described in his recent emails," he said. To read more click **HERE**

Cisco Patches Critical Issue in Wireless Residential Gateway Products

SoftPedia, 17 Jul 2014: A security glitch in the web server present in several Cisco Wireless Residential Gateway products could be exploited by an attacker to execute code remotely and has been addressed by the developer. The vulnerability, a buffer overflow, occurred because of incorrect validation of HTTP requests. As such, the intruder had the opportunity to exploit it by sending malicious HTTP requests to the affected device. By doing so, they would cause the web server to crash, which allowed them to inject commands and execute code with elevated privileges. Cisco says that the vulnerability is exploitable regardless if the device is set up to work in router or gateweway mode. So far, Cisco is not aware of the security flaw being leveraged in the wild and urges its customers to install the update as soon as possible. The severity of the issue is high, as the attacker does not need to be authenticated in order to breach the system, and the complexity level is low.
A list with the devices affected includes the following:

- Cisco DPC3212 VoIP Cable Modem
- Cisco DPC3825 8x4 DOCSIS 3.0 Wireless Residential Gateway
- Cisco EPC3212 VoIP Cable Modem
- Cisco EPC3825 8x4 DOCSIS 3.0 Wireless Residential Gateway
- Cisco Model DPC3010 DOCSIS 3.0 8x4 Cable Modem
- Cisco Model DPC3925 8x4 DOCSIS 3.0 with Wireless Residential Gateway with EDVA
- Cisco Model DPQ3925 8x4 DOCSIS 3.0 Wireless Residential Gateway with EDVA
- Cisco Model EPC3010 DOCSIS 3.0 Cable Modem
- Cisco Model EPC3925 8x4 DOCSIS 3.0 with Wireless Residential Gateway with EDVA.

To read more click **HERE**

SQL Injection Risk in vBulletin Receives Prompt Patch

SoftPedia, 17 Jul 2014: vBulletin announced on Wednesday that a security patch was available for the forum software, one that aims at fixing a SQL injection vulnerability. The SQL injection risk was privately disclosed to them earlier this week by the members of the Romanian Security Team (RST). They found it while testing vBulletin 5.x for security issues in order to update their forum. One of the security researchers that found the glitch, who goes by the online alias Nytro, told us that a potential attacker could gain access to the database containing the details of the administrators. This would automatically offer the perp access to the administration panel and, from there, to other databases. Apart from login details and email addresses, some websites have databases with financial information, which would be a treasure trove for an intruder. The current security patch addresses this vulnerability in vBulletin versions 5.0.4, 5.0.5, 5.1.0, 5.1.1, and 5.1.2. Patches for all these releases are available on this page and users are recommended to perform the update as soon as possible. Nytro published a demo video of the exploit, injecting SQL and obtaining access to databases of both RST and vBulletin. The clip clearly shows the database name and version and the MySQL user, which is sufficient proof that details could be exfiltrated. In the clip, RST said that it did not sell the exploit, although zero-days are generously

rewarded by threat actors, the price amounting to thousands of dollars in some cases. The exploit has not been published, but as soon as the freshly-released security fix is applied by more administrators, Nytro said they would present it to the public. vBulletin moved very fast in addressing this glitch, as they actually came up with a solution to the problem a day after the issue had been reported, but delayed its release to the public in order to make sure that everything was okay. In the past, Romanian Security Team found a cross-site scripting (XSS) vulnerability in vBulletin 5.1.1 Alpha 9, which is identified by CVE-2014-3135; it permitted injecting arbitrary web script or HTML code. A post from on the company forum Wayne Luke, technical support lead at vBulletin, says that customers of the cloud service do not need to bother with the patch because it is applied by the maintenance team. The representative also says that the latest security fix is to be incorporated in the next revision of vBulletin 5.1.3 Alpha. Administrators are warned that the alpha release is not considered suitable for production or live servers. To read more click HERE

Japanese Adult Websites Deliver Banking Malware

SoftPedia, 17 Jul 2014: Security researchers found that some online locations with adult content in Japan have been compromised with a new variant of a banking malware that has been used in previous campaigns by threat actors. ESET identifies this malware family as Win32/Aibatook, and they have found a new variant that is no longer written in Delphi; it appears that the malware writers switched to C++ and also implemented some changes regarding the way it was distributed, how the details were stolen and the targeted financial institutions. The researchers say that the threat actors do not rely on entire exploit kits to infect the machines of the victims, and use instead only one exploit at a time. This is delivered through Japanese adult websites and leverages a Java vulnerability (CVE 2013-2465). Researchers' observations show that this distribution method has been used by the cybercriminals since the middle of April. At least four domains have been compromised, all of them containing adult content targeting Japanese. The crooks seem to have prepared the campaign for maximum impact because some of the infected domains are among the most visited 2,000 in Japan. Victims are directed, via a malicious link, from the adult content site to another compromised location that delivers the Java exploit. ESET says that after the malicious file is downloaded, another file, named "counter.php," is requested from another domain. "We believe this last step is related to the conditions under which the HTML snippet will be inserted: only a limited number of users per day will receive the exploit, explaining the need to count the number of tries. This counter script is hosted on what appears to be yet another compromised website, 'ccc.rejec.net'," says the research team in a post. It appears that the cybercriminals have integrated two different methods for stealing the financial credentials from the infected computers of the victims. In the case of a smaller number of targeted banks, Japan Post and SBI Sumishin Net Bank among them, they use a custom method, while for the gross of the financial institutions, about 90 of them, a more generic one is employed. However, according to ESET, both of them are leveraged by manipulating the Internet Explorer web browser through the IHTMLDocument2 interface, which offers read/write permission for web pages with high-level methods. Modification of the web pages is used for the small number of targeted banks, whose addresses are hard-coded in the malware, in order to obtain as much information from the victim as possible. The generic information stealing method has been refined in time and relies on "form-grabbing," a technique that monitors the input fields used by the victim and sends the entered details to the command and control server of the crooks. ESET team said that Win32/Aibatook, an earlier variant also being analyzed by Symantec, has been developed on a constant basis in the past months. They believe that its distribution is very likely to widen in the near future. To read more click HERE

The XPocalypse Begins: Windows XP Hacked to Spread Malware

SoftPedia, 17 Jul 2014: Security company TrapX Security warns that a number of Windows XP devices have been infected to spread malware and help cybercriminals steal documents and other sensitive data. TrapX says that malware was injected into terminal scanners running Windows XP Embedded belonging to a Chinese manufacturer, with the infection then being used to send scanned data, such as origin, destination, contents, value, to, and from details, through an established comprehensive command and

control connection (CnC) to a Chinese botnet that was terminated at the Lanxiang Vocational School located in the "China Unicom Shandong province network." The malware, which is called "Zombie Zero," appears to be exploiting Windows XP systems and is triggered once the scanners are connected to a wireless network. "The problem with legacy security technologies is that they are not able to adapt to defend against emerging threats in real-time," said David Monahan, research director at Enterprise Management Associates. "Today's threat actors are smarter than ever morphing their attacks multiple times to achieve the goal of undermining existing security defenses. The next generation of security solutions must be just as adaptable to counter these modern threats." This security issue isn't necessarily tracked down to Windows XP, but there's no doubt that the old operating system can be easier exploited by cybercriminals and those who are trying to establish large malware networks. Microsoft has been warning about the same thing for months, explaining that without security patches and fixes, it's all just a matter of months until someone finds a vulnerability in the operating system, which can be then used to infect a specific computer and access its data. "While it's true that you can keep using your PC with Windows XP after support ends, we don't recommend it. For starters, it'll become five times more vulnerable to security risks and viruses, which means you could get hacked and have your personal information stolen," Redmond warned. And despite all these risks, 25 percent of the desktop computers worldwide are still running Windows XP, with users claiming that their operating systems still work just fine despite end of support. Of course, security risks are getting bigger and this new malware report is living proof that XP is no longer an operating system that's safe to use, no matter if we're talking about consumers, OEMs, or business users. It remains to be seen, however, how many users would actually decide to upgrade once more cases of such exploits emerge. To read more click **HERE**

20 Java Security Issues Fixed by Oracle

SoftPedia, 17 Jul 2014: Oracle rolled out a new set of updates for its products as part of the company's quarterly Critical Patch Update, and Java received no less than 20 security-related fixes, all allowing a potential attacker to exploit flaws without the need to authenticate. In the case of users with Java 7 on their system, and this includes Windows XP machines, too, applying the latest patch should bring the update number to 65. With Java 8, the update number is 11. Although all 20 Java vulnerabilities present remote exploitation risks, only eight of them have been deemed by the company to be more serious, being assigned a Common Vulnerability Scoring System (CVSS) score greater than 9. Out of these, one vulnerability (CVE-2014-4227) has been labelled with the top severity mark of 10, meaning that exploiting it is far from being complex and the impact is quite significant. It affects Java 8u5, 7 u60 and 6u75. Most of the severe glitches have been given a 9.3 score, as the complexity of leveraging them is not too high. The network is the attack vector in all these cases. The entire Critical Patch Update contains a total of 113 fixes (link), for multiple Oracle product families; this means that they impact hundreds of products. Users are advised to update their Java installation, if available on their systems, as soon as possible in order to mitigate the security risks. To read more click **HERE**

PushDo Trojan Variant Has New Domain Generation Algorithm

SoftPedia, 17 Jul 2014: A fresh version of the PushDo malware component has been detected by security researchers to have changed the encryption keys for the communication across the botnet or with the command and control server. Malware writers have created several variants of the PushDo Trojan, and researchers at Bitdefender have found a new one that relies on the same communication protocol, but switched to different private and public encryption keys. Another modification is the fact that the fresh revision of the malware contains an encrypted overlay for the binaries, which would have a validation purpose. "If the conditions specified in the overlay aren't met, the sample doesn't run properly," explain the researchers in a post on Bitdefender's blog. It seems that the list of the domain names issued through the built-in domain generation algorithm (DGA) now contains about 100 clean entries. The DGA component is designed to hide the details for the real control and command server, making the botnet more difficult to disrupt. Bitdefender informs that a new DGA is in place, maintaining the old structure of the algorithm but with a different pattern for the domain names generated. The security company

managed to sinkhole one of them, and the result was that 2,336 unique IP addresses connected to the server in less than three hours. According to Bitdefender, India, Vietnam, and Turkey are the countries with the largest number of PushDo infections. The investigation is under way at the moment and no additional details have been provided by the security researchers. To read more click **HERE**

22.8 Million Personal Records of New Yorkers Exposed Since 2006

SoftPedia, 17 Jul 2014: A report regarding the impact of security breaches on residents of New York revealed that in 2013 sensitive information of almost 29 million individuals has been exposed, in about 5,000 attacks. Issued by Attorney General Eric T. Schneiderman, the document informs that the total toll of the breaches amounted to more than $1.37 / €1 billion, impacting both the public and the private sector. Schneiderman draws attention to the fact that organizations should take action to prevent this sort of incidents, suggesting that entities that store electronic information should create and implement the necessary security framework, while individuals can protect themselves through frequent monitoring of financial statement and "practicing their own data-minimization techniques." In order to emphasize the need of protective measures for personal information in digital format, the report cites a January 2014 Pew Research poll, which says that one in five Americans had private details stolen; this included Social Security number, credit card or bank account information. A higher percentage said that their email or social networking accounts had been compromised. "Data security breaches are more than simply a privacy concern – they can have harmful consequences," says Schneiderman in the report, bringing information about the fact that all the data lost as a result of intentional security breaches is used for fraudulent purposes. Since 2006, the New York Attorney General's Office has learned that most of the intrusions (40%) occurred as a result of hacking; a smaller amount (24%) were due to lost or stolen equipment or information, while insider wrongdoing was attributed 10% of the incidents. However, the Attorney General admits that these figures may not reflect reality because many of the breaches were not reported. As such, the 22.8 million records may represent only the tip of the iceberg. "For approximately six months between 2008 and 2009, a team of Russian hackers penetrated Heartland Payment Systems, one of the country's largest credit card processing systems. By the time the breach was discovered, an estimated 130 million credit card records were stolen across North America," says the report. Because the company could not estimate the information loss, the data has not been fully enumerated in the breach logs. Despite the large amount of incidents reported by the Attorney General, it appears that only 28 of them were responsible for the 80% of the data loss in the past eight years. To read more click **HERE**

SSL Blacklist Reveals Certificates Used by Cybercriminals

SoftPedia, 17 Jul 2014: A new project has been deployed, aiming at presenting a collection of SSL certificates employed by threat actors to secure communication between the infected machines and the servers under their control. Cryptographic protocols have been implemented as a safe way for a computer user to navigate to certain web pages, giving them access to sensitive information without third-parties being able to intercept the messages. However, cybercriminals also started to adopt this method for exchanging messages with compromised computers in a botnet. The reason behind this is to avoid being spotted by intrusion detection/prevention systems (IDS/IPS). Security researchers at Abuse.ch from Switzerland initiated a project (SSLBL) that publishes a SSL blacklist with the SHA1 cryptographic fingerprints of the SSL/TLS certificates employed in malicious activities, such as communication between command and control servers and the systems in a botnet. "The goal of SSLBL is to provide a list of bad SHA1 fingerprints of SSL certificates that are associated with malware and botnet activities," say the maintainers of the SSLBL in a blog post. The idea of the project came when working with Suricata, an open-source IDS, IPS and Network Secure Monitoring (NSM) tool, which integrates a SSL/TLS module that can fingerprint the secure certificates. The Swiss researcher is known for tracking high-profile banking Trojan families and botnets, and their portfolio includes malicious software, like Zeus, SpyEye, Palevo and Feodo. As such, starting SSLBL is a continuation of their fight against the threat actors attempting to steal financial information from computer users around the world. At the moment, the list includes a number of 127 digital certificates associated with different malware campaigns. Some of them have been

generated by the cybercriminals themselves, while others have been bought from trusted certificate authorities (CA). "The goal of SSLBL is to provide a list of bad SHA1 fingerprints of SSL certificates that are associated with malware and botnet activities. Currently, SSLBL provides an IP based and a SHA1 fingerprint based blacklist in CSV and Suricata rule format," says the researcher. The list is useful for detecting command and control traffic relying on SSL, and it contains important details, such as the MD5 hash of the malware binary, the destination address, and the SSL version used. So far, the entries show the fingerprints for certificates used by KINS, Vawtrack and Shylock. However, the database is likely to grow and add more malware families, considering the general communication encryption trend used by cybercrooks. To read more click **HERE**