THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

6 October 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

October 2, Associated Press – (National) **76M households hit by JPMorgan data breach.** JPMorgan Chase & Co. stated October 2 that a large cyberattack against the company's systems compromised the customer information of around 76 million households and 7 million small businesses. The attack was discovered in August and began as early as June and compromised customers' names, addresses, email addresses, and phone numbers but the bank stated that there was no evidence that the breach included account information. Source: https://finance.yahoo.com/news/jpmorgan-says-data-breach-affected-210556038.html

October 3, Softpedia – (International) **CryptoWall 2.0 available in the wild, has new obfuscator.** A 2.0 version of the CryptoWall ransomware has been spotted in the wild by researchers and includes the use of the Tor network for communicating with command and control servers and a new obfuscator to prevent analysis and debugging. Source: http://news.softpedia.com/news/CryptoWall-2-0-Available-In-the-Wild-Has-New-Obfuscator-460927.shtml

October 3, Help Net Security – (International) **Destructive Android trojan poses as newest Angry Birds game.** Researchers with Doctor Web identified a piece of destructive Android malware detected as Android.Elite.1.origin that poses as an unreleased Angry Birds game app and once installed deletes a device's data, blocks communications programs, and sends out a high volume of messages to all contacts on the device. Source: http://www.net-security.org/malware_news.php?id=2877

October 2, Securityweek – (International) **"BadUSB" code published.** Two researchers presenting at the Derbycon 4.0 conference reverse-engineered USB firmware to launch various attacks and posted the attack code online. The flaw in USB firmware that enables the attack was first revealed at the Black Hat conference but the attack code was not released at that time. Source: http://www.securityweek.com/badusb-code-published

October 2, Threatpost – (International) **Second same-origin policy bypass flaw haunts Android browser.** A researcher identified and reported a same-origin policy bypass vulnerability in the Android browser in versions prior to 4.4 that could allow an attacker to steal data from a user's browser. Google issued a patch for the vulnerability for users of Android 4.1-4.3 in late September. Source: http://threatpost.com/second-same-origin-policy-bypass-flaw-haunts-android-browser

AT&T suffers another insider breach

Heise Security, 6 Oct 2014: US telecom AT&T has lately been having problems with malicious insiders, and the latest incident has resulted in the compromise of account and personal information of a yet unknown number of customers. The breach notification letter sent out to affected users and to the Office of the Vermont Attorney General explains that one of the company's employees violated their policy and security guidelines by accessing users' account information, including the users' social security number and driver's license number. "Additionally, while accessing your account, the employee would also have been able to view your Customer Proprietary Network Information (CPNI) without proper authorization,"the letter says (link). "CPNI is information related to the telecommunications services you purchase from us." The breach happened in August 2014, and it seems that some of the stolen information has been misused in the meantime. "To the extent this activity results in any unauthorized charges or changes to your account, they have been or will be reversed," it says in the letter. They have also urged them to change the passcode on their account (if they have set it up) or to add one if they haven't. According to the updated Vermont data breach notification law (link), notification to the Vermont Attorney General must occur within 14 business days of either the discovery of the breach or notice to the consumers, whichever is sooner, so it seems that they discovered the breach only quite recently. The employee in question no longer works for the company. Earlier this year, AT&T has also suffered a breach by the hands of three employees of one of its vendors, who accessed customers' account and information in order to be able to impersonate them and get codes to unlock phones from AT&T. To read more click HERE

JP Morgan Chase confirms breach, 76 million homes and 7 million businesses affected

Sophos Security, 3 Oct 2014: JP Morgan Chase, the largest bank in the US, informed investors on Thursday that a data breach during the summer had affected around 76 million households and approximately 7 million small businesses. Confirmation of the scale of the breach, one of the largest ever, came in an 8-K filing with the Securities and Exchange Commission (SEC) in which the company revealed that the attackers took off with user information including names, addresses, phone numbers and email addresses as well as "internal JPMorgan Chase information". On a more positive note, the company says it has seen no indication that account numbers, passwords, user IDs, dates of birth and Social Security numbers were compromised and says it has not seen "any unusual customer fraud related to this incident." It also makes clear that customers will not be liable for any unauthorized activity on their accounts as long as they let the bank know "promptly". JP Morgan Chase, which trades as Chase bank, has published a list of frequently asked questions for customers concerned about the breach. In it, the company reiterated how no sensitive financial information was stolen and no unusual activity had been spotted since. The bank warned of the threat of phishing attacks, which is exactly what happened in January 2014, a month after JP Morgan Chase experienced another breach which affected 465,000 prepaid cash card customers. Be wary if you receive an email that appears to come from JP Morgan Chase & Co (or any other bank). Remember that no legitimate financial institution is ever likely to send you an email asking for personal or sensitive financial information. If you wish to visit the official JP Morgan site, type the URL directly into your browser instead of clicking on a link within an email. Of course, email isn’t the only possible means of a follow-up attack - social engineers may attempt to dupe Chase customers by telephone too, especially if they have hold of the phone numbers we now know were snaffled in the breach. If you receive a call which appears to come from JP Morgan Chase, do not give out any information and hang up. If you actually need to speak to the bank or wish to confirm the call was in fact genuine, call back using a phone number found on your credit card statement or other official banking paperwork. To read more click HERE

How A Major Bank Hacked Its Java Security

DarkReading, 30 Sep 2014: Deutsche Bank London helped create a new application self-defense tool to lock down and virtually patch its Java-based enterprise applications -- even the oldest ones.Deutsche Bank AG London has what many large enterprises have: numerous internal applications based on various versions of Java, many of which are older and can't be patched nor updated. So the bank helped develop a tool that sits below the application to detect and prevent attacks and apply virtual patches. The bank, a subsidiary of Deutsche Bank AG, made the move after it inventoried its hundreds of internal applications and discovered a mix of old and new versions of Java, some of which were legacy applications that had become increasingly difficult to patch or update. Oracle's Java infamously has been riddled with security vulnerabilities, and Java client machines have become a favorite target of attackers. "We [had] uncovered a large degree of variance of Java deployed in the bank's infrastructure," Hussein Badakhchani, vice president of Deutsche Bank London, says in an exclusive interview with Dark Reading today. His application group teamed up with IT security to determine how to secure the large number of legacy Java applications running at the bank. The initial goal was to convert its applications -- everything from payments to training apps -- to a new platform-as-a-service the bank had built based on Java Virtual Machine (JVM). "We wanted to move away from DIY to a managed service" for enterprise applications. "The question becomes 'If you can't decommission an application and you can't operate it [or update its Java version], what can you do with it?'" The bank worked with security vendor Waratek to create a tool that runs within JVM and efficiently secures legacy Java applications. Call it application self-defense: The result was a software solution that uses what Gartner analyst Joseph Feiman calls a "self-protecting" application approach, or Runtime Application Self Protection (RASP). According to Feiman, RASP detects and blocks attacks, and it operates in the application's runtime environment. "Modern security fails to test and protect all apps. Therefore, apps must be capable of security self-testing, self-diagnostics and self-protection," he writes in a new Gartner Maverick Research report on RASP. Gartner predicts that 25% of web and cloud applications will become self-protecting by 2020; fewer than 1% operate that way today. It's a natural fit, according to security expert Dan Kaminsky. "The JVM -- and CLR [Common Language Runtime] and even the various JS [JavaScript] engines -- are designed to detect many errors. Why not instrument them for security and see what comes up?" Kaminsky says. "Over time, the languages and platforms we use increasingly support securing the applications we write on top of them. More importantly, the cost of that security diminishes as the platform shoulders more of the burden." Kaminsky, chief scientist at WhiteOps, says it's not so much about Java's security problems as it is about looking at a way to apply security to multiple different applications, at scale. "Traditional WAFs [web application firewalls] can often be somewhat distant from the platforms they're securing" says Kaminsky, who also serves as a technical adviser to Prevoty, a competitor to Waratek in the RASP space. "What if there was deeper integration? What if the WAF didn't have to guess what the end application saw, what if it could ask… or if it was alerted in case of problems?" Deutsche Bank London had battled the headache of off-cycle patching for zero-day vulnerabilities that occur outside its orchestrated, regular quarterly patching cycles. "Problems arise from unscheduled patching events for zero-day exploits," Badakhchani says. The new RASP approach provides virtual patching to the bank's Java-based applications, so the bank doesn't have to deal with out-of-band patching. Even the regular patching cycle can be disruptive. "To try to remedy every vulnerability, when you have 600 business applications, the amount of work you need to do in standard patching is extremely expensive." It involves, among other things, "hiring teams of developers" to decode patches. It works like this: An attack that attempts to exploit or employ a Java process, such as a SQL injection attempt, cannot execute. "If an attack gets past our security, for example, and tries to make a call to a Java process, it won't be allowed to. We'll be alerted to an intrusion," he says. The tool can detect known and unknown attacks. "It's [like] placing a firewall within the application in the JVM itself," Badakhchani says. Like any security layer, there's a convenience or performance tradeoff. He says the RASP tool comes with a performance tradeoff in about 10% of the bank's applications. "It's not that significant… The benefits from the security side outweigh" that, he says. To read more click HERE