THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

17 September 2014

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

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

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

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, and Sandia National Labs

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

September 15, IDG News Service – (International) **'Tiny banker' malware targets US financial institutions.** Researchers at Avast analyzed an updated variant of the Tiny Banker (also known as Tinba) financial malware and found that it is now able to target new financial institutions including ones in the U.S. The malware can inject HTML fields into banking Web sites when a user visits them in order to collect personal and login information. Source: http://www.networkworld.com/article/2684113/tiny-banker-malware-targets-us-financial-institutions.html

September 16, WPLG 10 Miami – (Florida) **Aventura Hospital and Medical Center reports data breach.** Valesco Ventures informed 82,601 Aventura Hospital and Medical Center patients in Florida September 9 that an employee may have accessed their personal information, including Social Security numbers, from September 2012 to June 2014. Authorities are investigating the breach. Source: http://www.local10.com/news/aventura-hospital-medical-center-reports-data-breach/28082920

September 16, The Register – (International) **THREE QUARTERS of Android mobes open to web page spy bug.** A Metasploit developer released a Metasploit module for a vulnerability in Android versions 4.2.1 and below that was discovered September 1, which could automate an exploitation of the vulnerability and allow attackers behind a malicious Web page to see users' other open pages and hijack sessions. Source: http://www.theregister.co.uk/2014/09/16/three_quarters_of_droid_phones_open_to_web_page_spy_bug/

September 15, KrebsOnSecurity – (International) **LinkedIn feature exposes email addresses.** Researchers with Rhino Security Labs demonstrated how an attacker could use a 'find connections' feature in LinkedIn and a large number of email contacts generated with likely email addresses to identify the email address of specific individuals for possible use in spear-phishing or other malicious activities. LinkedIn stated that it was planning at least two changes to the way the professional network handles user email addresses to counteract the issue. Source: http://krebsonsecurity.com/2014/09/linkedin-feature-exposes-email-addresses/

September 15, Threatpost – (International) **SNMP DDoS scans spoof Google public DNS server.** The SANS Internet Storm Center reported September 15 that large-scale scans of Simple Network Management Protocol (SNMP) spoofing Google's public DNS server traffic were taking place, indicating a scan being used to identify routers and devices using default SNMP passwords. Vulnerable routers and devices could have their configuration variables changed, creating a denial of service (DoS) situation on the affected devices. Source: http://threatpost.com/snmp-based-ddos-attack-spoofs-google-public-dns-server

September 15, eSecurity Planet – (New York) **Insider credit card breach leads to $400,000 Saks shopping spree.** Authorities arrested six former employees of a New York City Saks Fifth Avenue store September 5 for allegedly stealing the payment card information of at least 22 customers from store computers and using the data to purchase $400,000 in merchandise, some of which was returned to the store for refunds that were delivered to accounts in the suspects' control. Source: http://www.esecurityplanet.com/network-security/insider-credit-card-breach-leads-to-400000-saks-shopping-spree.html

House passes bills targeting IRS' Email Practices

TheHill, 16 Sep 2014: The House late Tuesday passed legislation to highlight congressional committees' investigations of the Internal Revenue Service for its alleged targeting of conservative nonprofits applying for tax-exempt status. All of the measures were passed by voice vote. One bill, H.R. 5418, would prohibit IRS employees from using personal email accounts for official business. Rep. Charles Boustany (R-La.) said it would prevent sensitive taxpayer information from being compromised if IRS employees use non-secured email accounts. "There's no reason for an IRS employee to have confidential taxpayer information on his or her home computer without the necessary safeguards against disclosure," Boustany said. Another measure, H.R. 5170, would establish a process for firing federal employees who falsify or destroy records. The IRS has been under fire since it informed Congress that nearly two years' worth of former IRS official Lois Lerner's emails were lost in a computer crash. Lerner was held in contempt of Congress in a largely party-line vote in the House earlier this year. "Unfortunately, too frequently of late, Congress has heard examples of agencies and individuals failing to comply with the basic provisions of the federal recordkeeping law. The most recent illustration is the IRS. They failed to follow the law by not disclosing the potential loss of federal records relating to Ms. Lerner," said Rep. Mark Meadows (R-N.C.). Rep. Elijah Cummings (D-Md.), the top Democrat on the House Oversight Committee, agreed it would help ensure that government records remain accessible. "This bill would make the federal government's records more transparent," Cummings said. To read more click HERE

Probe: HealthCare.gov website must boost security

AP, 16 Sep 2014: HealthCare.gov, the health insurance website serving more than 5 million Americans, has significant security flaws that put users' personal information at risk, nonpartisan congressional investigators have concluded. The Government Accountability Office said the Obama administration must resolve more than 20 specific security issues related to who can get into the system, who can make changes in it and what to do in case the complex network fails. GAO, the investigative arm of Congress, found that the administration took a major risk going live with HealthCare.gov last fall when the system was still not fully tested. Some testing was incomplete as of June. While the administration "has taken important steps to apply security and privacy safeguards to HealthCare.gov and its supporting systems, significant weaknesses remain that put these systems and the sensitive, personal information they contain at risk of compromise," Gregory Wilshusen, GAO's director of information security, said in testimony prepared for the House Oversight and Government Reform Committee. The committee released his testimony Tuesday. GAO's accompanying 78-page report was released later. The website collects sensitive personal information including names, birth dates, Social Security numbers and family income. Multiple federal and state agencies as well as many contractors have access. Yet the report found there's no common understanding of security requirements among all the players. The agency running HealthCare.gov "had not always required or enforced strong password controls, adequately restricted access to the Internet, consistently implemented software patches and properly configured an administrative network," the report said. Responding for the administration, Health and Human Services spokesman Aaron Albright said that the changing nature of threats makes website security an evolving process and that officials have already acted on many of the recommendations. In its public assessment, the GAO outlined six broad areas where more work needs to done. They ranged from basics like following recommended best practices for government agencies, to a comprehensive test of all elements of the system, to establishing a backup site for the HealthCare.gov and its supporting networks. In an accompanying report that was not publicly released, Wilshusen said the agency listed 22 specific technical recommendations to fix security flaws. He said the administration agreed with all the specific recommendations, although not with some of the broader suggestions. One major disagreement is whether security testing should involve the entire system simultaneously — as GAO recommends— or whether each component can be tested and certified separately, as the administration has done. HealthCare.gov was hacked this summer, but no consumer information was stolen. Instead, hackers installed malicious software that could have been used to launch an attack on other websites from the federal insurance portal. Federal computer systems get hundreds of cyberattacks every day, but this was believed to be the first successful one involving HealthCare.gov. The health care site had numerous technical problems when it was launched last fall and was initially unworkable for most consumers. Among the issues that concerned the administration's own technical experts at the time was that security testing could not be completed because the system was undergoing so many last-minute changes. The part of HealthCare.gov that serves as the entry way for consumers eventually passed security certification, but the GAO revealed that security testing continued well into this year on other important components that deal with health plan information and financial management. The administration said that's because those components were still in stages of development. The report also confirmed security problems in state computer systems linking to the federal network, reported earlier this year by The Associated Press. Vermont announced Tuesday that its technically troubled site has been taken down to fix numerous issues, including several security problems. To read more click HERE

Macro based malware is on the rise

Heise Security, 17 Sep 2014: Malware authors have a rediscovered their love for Visual Basic, as the percentage of macro based malware rose from around 6% of all document malware in June to 28% in July, Sophos researchers have found. Gabor Szappanos, principal researcher at SophosLabs, explained in a paper published earlier this year the advantages of Visual Basic code over exploits: "Visual Basic code is easy to write, flexible and easy to refactor. Similar functionality can often be expressed in many different ways which gives malware authors more options for producing distinct, workable versions of their software than they have with exploits." Exploits, on the other hands, are more difficult to modify to evade AV detection and still be able to work as intended. Another advantage of Visual Basic code over exploits is that it will work in all versions of Microsoft Office, not just the ones that are vulnerable to that particular exploit. And even though Microsoft has made it so that all macros from untrusted sources are disabled by default, malware authors have been using social engineering to trick users into enabling them. Learning and writing in Visual Basic for Applications (VBA) is extremely easy, researchers note, but even if malicious actors don't have that knowledge, there are a number of VBA downloader templates that can be bought online. "The samples in question contain Visual Basic code with helpful comments as to where authors should insert a malicious link as well as details of methods for obfuscating the code," the researchers explained. In the example pictured above, once the macros are enabled and the document is reopened, the malware checks for the presence of the PowerShell task automation management framework. If it's present, it is used to execute encoded scripts, and inject the shellcode into memory, which ultimately establishes a reverse shell on the affected computer, meaning that the attacker has gained full remote access to it and is free to tinker around. "If the host machine does not have PowerShell installed the sample simply reverts to injecting shellcode using good old Visual Basic," the researchers pointed out, but noted that, despite its effectiveness, VBA shellcode injection is currently very rarely used, because it improves the chances of the malware being detected by security software. To read more click HERE

Even Biometric Locks Can Be Picked

DFI News, 16 Sep 2014: How can we ensure that someone is who they say they are? How can be sure that the person in our system, both digitally speaking or physically in front of us, is who whom they claim to be? You may think that a good password is the answer, but with so many ways to break into a computer system these methods are clearly not always effective — as can be seen from the unfortunate hacked celebrities whose naked pictures were strewn across the internet recently, or the Oleg Pliss ransomware that locks iPhones until the extortioner is paid. Even a combination of a good username and password may not be enough. What about biometrics? This technology uses human physical attributes as locks and keys, such as fingerprints, iris scans or, as is now suggested, the veins in the human fingertip, making them highly individual ways to identify one user from another. Using biometrics is not especially new. For example, while the likes of iris scanners may be familiar from sci-fi films, they're also (or were until recently) found in real life airports too. Often mistakenly called retinal scanners, they are based on scanning the unique pattern of the iris, the coloured part of the eye. But the technology needed to complete an effective and trusted scan is expensive and can be tricked by technologically capable hackers. These are great for entry control systems on the buildings of large organisations, or for the occasional secret bunker seen in films. But they are extremely costly — prohibitively so if a bank was to insist that every customer had one at home – and false readings become a problem as the number of people using it scales. On the other hand, fingerprint technology has become cheaper and more available – fingerprint scanners are now sufficiently small and accurate that they started appearing in laptops 10 years ago, and are even in small devices like the iPhone 5S. This is one way that banks could allow smartphone and laptop users to access their financial services, with users presenting a finger rather than a passcode. In fact it’s easy to obtain a range of low-cost scanners for all sorts of authentication uses. But that doesn’t mean the users will like doing so – there are ethical issues to consider, as some UK schools discovered in 2012 when their use of fingerprint scanners to monitor pupil attendance led to an outcry and a government ban without explicit consent from parents. Despite our fingerprints all being unique, there is still the possibility to fool the systems used to protect secured buildings, large computer systems or financial institutions. There are well known ways to get around fingerprint biometric authentication, from creating false fingers (with prints) from gelatin, using good quality photographs or even a photocopy of fingerprints to fool scanners, or most upsettingly simply removing a finger from those with access rights. These and others are well known, in real life and in the semi-fictional world of Hollywood. Barclays' recent decision to use a finger vein scanner, which scans and pattern-matches the unique structure of the blood vessels in the finger. This has the benefit of only working when the finger is attached to the rest of the body and blood is flowing, which rules out the most grisly workarounds. Facial recognition has been available for a while, and as the majority of computers now come with webcams included this would seem a logical step. The challenge is that the software making the decisions is very sensitive to environmental conditions such as light and darkness. We don’t all look our best for the camera all of the time, and the need for our real face to match the reference version the system is using means that, while a human would recognise the same person, a computer algorithm often can’t. This is why the killjoys at the UK Home Office and elsewhere refuse to let us smile in passport photos these days. But this same fact means that it’s possible to log into laptops equipped with a face-recognition login by simply putting a picture of the owner in front of the webcam. To read more click HERE