THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

29 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

Hackers breach White House computer system, Russia suspected

AFP, 29 Oct 2014 The White House's unclassified computer network was recently breached by intruders, a US official said Tuesday, with The Washington Post newspaper reporting that the Russian government was thought to be behind the act. "In the course of assessing recent threats, we identified activity of concern on the unclassified EOP network," said the White House official, speaking on condition of not being named. "Any such activity is something we take very seriously. In this case, we took immediate measures to evaluate and mitigate the activity." The Washington Post quoted sources as saying hackers believed to be working for the Russian government were believed to be responsible. The hackers entered the US presidential mansion's unclassified computer network in recent weeks, the Post quotes the sources as saying. In a statement, the White House official said the Executive Office of the President receives daily alerts concerning numerous possible cyber threats. In the course of addressing the breach, some White House users were temporarily disconnected from the network. "Our computers and systems have not been damaged, though some elements of the unclassified network have been affected. The temporary outages and loss of connectivity for our users is solely the result of measures we have taken to defend our networks," the official said. To read more click **HERE**

October 24, Washington Post – (National) **With a $10 million fine, the FCC is leaping into data security for the first time.** The Federal Communications Commission issued two phone carriers, TerraCom and its affiliated YourTel America, with a total of $10 million in fines for improperly storing more than 300,000 customers' personally identifiable information such as their Social Security numbers, home addresses, phone numbers, data of birth and other personal data online without firewalls, encryption or password protection, making the information easily accessible to the public. Source: http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/24/with-a-10-million-fine-the-fcc-is-leaping-into-data-security-for-the-first-time/

October 27, Securityweek – (International) **Tor exit node found maliciously modifying files.** A researcher with Leviathan Security Group identified and reported an exit node on the Tor network that wraps binary files with malware as the files move through the node. The Tor Project stated that they set a "BadExit" flag on the node to protect users after it was reported. Source: http://www.securityweek.com/tor-exit-node-found-maliciously-modifying-files

October 24, Dark Reading – (International) **Backoff PoS malware boomed in Q3.** Damballa released a report which found that detections of the Backoff point-of-sale (PoS) malware increased by 57 percent between August and September. Source: http://www.darkreading.com/attacks-breaches/backoff-pos-malware-boomed-in-q3/d/d-id/1316957

October 27, Softpedia – (International) **Banking trojan Dridex delivered through Microsoft Word macros.** Researchers with Palo Alto Networks found that the Dridex banking malware is being distributed via Microsoft Word documents containing malicious macros in a campaign that began October 21. The malicious documents are sent in fake invoice emails and mainly target users in the U.S. Source: http://news.softpedia.com/news/Banking-Trojan-Dridex-Delivered-Through-Microsoft-Word-Macros-463259.shtml

October 28, The Register – (International) **EvilToss and Sourface hacker crew 'likely' backed by Kremlin - FireEye.** FireEye released a report on an advanced persistent threat (APT) actor dubbed APT28 stating that the group used the Sourface downloader and Chopstick and EvilToss malware to attack NATO, Eastern European governments, European defense industry events, the World Bank, and other national and international organizations. The researchers stated that APT28 has been active since 2007 and was likely backed by the Russian government. Source: http://www.theregister.co.uk/2014/10/28/us_mandiant_claims_moscow_sponsoring_apt_28_hacker_group/

October 28, Securityweek – (International) **Attackers exploit ShellShock via SMTP to distribute malware.** Binary Defense Systems researchers reported that attackers are leveraging the ShellShock vulnerability in GNU Bash to target servers by adding the ShellShock payload to email subject, from, and to fields, abusing the Simple Mail Transfer Protocol (SMTP). If a system is compromised, a Perl-based IRC bot is downloaded and the SMTP gateway is added to a botnet designed for distributed denial of service (DDoS) attacks. Source: http://www.securityweek.com/attackers-exploit-shellshock-smtp-distribute-malware

October 28, IDG News Service – (International) **'ScanBox' keylogger targets Uyghurs, US think tank, hospitality industry.** Researchers at PricewaterhouseCoopers found that the ScanBox keylogging framework may be being used by several attacker groups after it was found being used to perform keylogging attacks on a variety of Web sites, including a U.S. think tank and other sites. ScanBox was first discovered in August and uses JavaScript rather than installing malware to collect keystrokes and other information. Source: http://www.networkworld.com/article/2839600/security/scanbox-keylogger-targets-uyghurs-us-think-tank-hospitality-industry.html

October 28, Softpedia – (International) **Sophisticated Chinese espionage group after Western advanced technology.** A group of security and information technology companies coordinated by Novetta released a report into an advanced persistent threat (APT) group dubbed Axiom Group that has used the Hikit malware family and other tools to target government agencies, law enforcement, aerospace, manufacturers, media, communications, pharmaceutical, energy, educational, and other institutions in the U.S. and several other countries since 2008. The researchers stated that the group originates in China and appears to choose targets in line with Chinese government policies. Source: http://news.softpedia.com/news/Sophisticated-Chinese-Espionage-Group-After-Western-Advanced-Technology-463348.shtml

October 27, Securityweek – (International) **Targeted attacks against businesses jump: Kaspersky Lab.** Kaspersky Labs and B2B International released the results of a survey covering 3,900 respondents in 27 countries and found that 94 percent of businesses surveyed reported at least one cybersecurity incident in the past 12 months, with 12 percent of the countries surveyed reporting one or more targeted attack, among other findings. Source: http://www.securityweek.com/targeted-attacks-against-businesses-jump-kaspersky-lab

DHS No Longer Needs Permission Slips to Monitor Other Agencies' Networks for Vulnerabilities
NextGov, 3 Oct 2014: The Department of Homeland Security has spelled out its intentions to proactively monitor civilian agency networks for signs of threats, after agencies arguably dropped the ball this spring in detecting federal websites potentially harboring the Heartbleed superbug. Annual rules for complying with the 2002 Federal Information Security Management Act released Friday require agencies to agree to proactive scanning. The regulations also contain new requirements for notifying DHS when a cyber event occurs. "The federal government's response to the 'Heartbleed' security vulnerability highlighted the need to formalize this process, and ensure that federal agencies are proactively scanning networks for vulnerabilities," Office of Management and Budget Director Shaun Donovan said in an Oct. 3 memo to department heads. "This year's guidance clarifies what is required of DHS and federal agencies in this

area." In April, researchers discovered Heartbleed, a glitch in widely used data encryption software. DHS for years has had the tools to monitor networks government-wide for intrusions. In addition, "Einstein," a mesh of diagnostic hardware and software, detects and helps prevent cyber intrusions. In May, Homeland Security officials told House lawmakers at a hearing that the department planned to expand Einstein's capabilities and deployment. At the time, Einstein's latest iteration, EINSTEIN 3 Accelerated, only covered seven departments and agencies. Extending coverage "has been significantly delayed by the lack of clear authorities for DHS," National Cybersecurity Communications Integration Center Director Larry Zelvin testified. The new formalized process for vulnerability scans pertains only to public-facing civilian agency networks. The procedures involve surveilling Internet-accessible addresses and segments of agency systems for weaknesses on an ongoing basis, "without prior agency authorization on an emergency basis where not prohibited by law." DHS officials Friday told Nextgov that, in the past, the department would have to obtain essentially permission slips from agencies before using Einstein and scanning their systems. Officials added that DHS now has 110 agreements from agencies to scan for vulnerabilities. Beth Cobert, OMB deputy director for management, said in a blog post Friday the arrangement does not replace existing agency network scans, rather, it "will provide a consistent scanning methodology that quickly identifies risks and vulnerabilities that may have government-wide implications." Separately, going forward, if an agency detects any type of data interruption or data breach, the agency must inform DHS -- within one hour -- of the confirmed data loss. Agencies previously had only been required to report incidents involving the compromise of personal information. To read more click **HERE**

Hackers Are Using Gmail Drafts to Update Their Malware and Steal Data

Wired, 29 Oct 2014: In his career-ending extramarital affair that came to light in 2012, General David Petraeus used a stealthy technique to communicate with his lover Paula Broadwell: the pair left messages for each other in the drafts folder of a shared Gmail account. Now hackers have learned the same trick. Only instead of a mistress, they're sharing their love letters with data-stealing malware buried deep on a victim's computer. Researchers at the security startup Shape Security say they've found a strain of malware on a client's network that uses that new, furtive form of "command and control"—the communications channel that connects hackers to their malicious software—allowing them to send the programs updates and instructions and retrieve stolen data. Because the commands are hidden in unassuming Gmail drafts that are never even sent, the hidden communications channel is particularly difficult to detect. "What we're seeing here is command and control that's using a fully allowed service, and that makes it super stealthy and very hard to identify," says Wade Williamson, a security researcher at Shape. "It's stealthily passing messages back and forth without even having to press send. You never see the bullet fired." Here's how the attack worked in the case Shape observed: The hacker first set up an anonymous Gmail account, then infected a computer on the target's network with malware. (Shape declined to name the victim of the attack.) After gaining control of the target machine, the hacker opened their anonymous Gmail account on the victim's computer in an invisible instance of Internet Explorer—IE allows itself to be run by Windows programs so that they can seamlessly query web pages for information, so the user has no idea a web page is even open on the computer. With the Gmail drafts folder open and hidden, the malware is programmed to use a Python script to retrieve commands and code that the hacker enters into that draft field. The malware responds with its own acknowledgments in Gmail draft form, along with the target data it's programmed to exfiltrate from the victim's network. All the communication is encoded to prevent it being spotted by intrusion detection or data-leak prevention. The use of a reputable web service instead of the usual IRC or HTTP protocols that hackers typically use to command their malware also helps keep the hack hidden. Williamson says the new infection is in fact a variant of a remote access trojan (RAT) called Icoscript first found by the German security firm G-Data in August. At the time, G-Data said that Icoscript had been infecting machines since 2012, and that its use of Yahoo Mail emails to obscure its command and control had helped to keep it from being discovered. The switch to Gmail drafts, says Williamson, could make the malware stealthier still. Thanks in part to that stealth, Shape doesn't have any sense of just how many computers might be infected with the Icoscript variant they found. But given its data-stealing intent, they believe it's likely a closely targeted attack

rather than a widespread infection. For victims of the malware, Shape says there's no easy way to detect its surreptitious data theft without blocking Gmail altogether. The responsibility may instead fall on Google to make its webmail less friendly to automated malware. A Google spokesperson responded to an email from WIRED with only a statement that "our systems actively track malicious and programmatic usage of Gmail and we quickly remove abusive accounts we identify." To read more click **HERE**

IT is losing the battle on security in the cloud

Heise Security, 29 Oct 2014: A majority of IT organizations are kept in the dark when it comes to protecting corporate data in the cloud, putting confidential and sensitive information at risk. This is just one of the findings of a recent Ponemon Institute study commissioned by SafeNet. The study, titled "The Challenges of Cloud Information Governance: A Global Data Security Study," surveyed more than 1800 IT and IT security professionals worldwide. The research indicates that while organizations are increasingly using cloud computing resources, IT staff is having trouble controlling the management and security of data in the cloud. The survey found that only 38 percent of organizations have clearly defined roles and accountability for safeguarding confidential or sensitive information in the cloud. Adding to the confusion, 44 percent of corporate data stored in cloud environments is not managed or controlled by the IT department. And more than two-thirds (71 percent) of respondents say it is more difficult to protect sensitive data in the cloud using conventional security practices. Nearly three-quarters (71 percent) of IT professionals confirmed that cloud computing is very important today, and more than three quarters (78 percent) believe it will be over the next two years. The respondents also estimate that 33 percent of their organizations' total IT and data processing requirements are met with cloud resources today, and that is expected to increase to an average of 41 percent within two years. However, the majority of respondents (70 percent) agree that it is more complex to manage privacy and data protection regulations in a cloud environment, and they also agree that the types of corporate data stored in the cloud, such as emails, and consumer, customer, and payment information, are the types of data most at risk. On average, half of all cloud services are deployed by departments other than corporate IT, and an average of 44 percent of corporate data stored in the cloud environment is not managed or controlled by the IT department. As a result, only 19 percent of respondents are very confident that they know about all cloud computing applications, platforms, or infrastructure services in use in their organizations today. Along with this lack of control over the sourcing of cloud services, views on who is actually accountable for cloud data security are mixed. Thirty five percent of respondents say it is a shared responsibility between the cloud user and the cloud provider while 33 percent say it is the responsibility of the cloud user and 32 percent say it is the responsibility of the cloud provider. More than two-thirds (71 percent) of respondents say it is more difficult to protect sensitive data in the cloud using conventional security practices, and nearly half (48 percent) say it's more difficult to control or restrict end-user access to cloud data. As a result, more than one-third (34 percent) of IT professionals surveyed say their organizations already have a policy in place that requires the use of security safeguards such as encryption as a condition for using certain cloud computing resources. Seventy-one (71) percent of respondents say the ability to encrypt or tokenize sensitive or confidential data is important, and 79 percent say it will become more important over the next two years. In terms of what companies are actually doing to secure data in the cloud, 43 percent of respondents say their organization is using private data network connectivity. Nearly two-fifths, or 39 percent, of respondents say their organizations use encryption, tokenization or other cryptographic tools to protect data in the cloud. Thirty-three percent say they don't know what security solutions they use and 29 percent say they use premium security services provided by their cloud provider. Respondents also noted that the management of their encryption keys is important to securing data in the cloud, given the increasing number of key management and encryption platforms their companies use. Fifty-four percent of respondents say their organization controls the encryption keys when data is stored in the cloud. However, 45 percent say they store their encryption keys in the software where they store their data while 27 percent say they store their keys in more secure environments such as hardware devices. Regarding access to data in the cloud, 68 percent of respondents also say that the management of user identities is more difficult in the cloud, and 62 percent of respondents say their organizations have third parties

accessing the cloud. Nearly half (46 percent) say their company uses multi-factor authentication to secure third-party access to data in the cloud environment. About the same percentage (48 percent) of respondents say their organizations use multi-factor authentication for employees' access to the cloud. To read more click **HERE**

Over one-third of all enterprise data leakage policy violations occur on mobile devices

Heise Security, 29 Oct 2014: Nearly half of all cloud app activities and more than one-third of all data leakage policy violations occur on mobile devices, say the results of the October 2014 Netskope Cloud Report. Based on aggregated, anonymised data from the Netskope Active Platform, the report's findings are based on tens of billions of cloud app events seen across millions of users between July and September 2014. Enterprises are continuing to adopt cloud apps at a fast pace, with an average of 579 cloud apps per organisation in Q3, up from 508 the previous quarter. Additionally, 88.7 percent of apps are not enterprise ready, scoring a "medium" or below in the Netskope Cloud Confidence Index. "There's a veritable storm of corporate activity across a wide variety of cloud apps, and it's increasingly happening on mobile devices and often from remote locations," said Sanjay Beri, CEO and founder of Netskope. "This makes it even more difficult for IT to keep tabs on sensitive corporate and customer data on user-owned devices, especially when you consider that the majority of these apps aren't enterprise-ready. The data here indicate that, while IT is increasingly aware of the 'shadow IT' problem, it continues to underestimate actual app usage, and the associated risks, by a considerable margin." Through this report Netskope isolated the cloud app activity data originating from mobile devices. The data validate that users see mobile devices as a viable extension of cloud apps for completing easily accomplished tasks like "send," "share," and "post." Interestingly, the frequency of activities such as "create" and "approve" may be evidence that app vendors' efforts to improve the user experience and streamline workflows on mobile devices are paying off. Beyond the activities themselves, a high number of activity-based policy violations occur on mobile devices, the highest of which is 59 percent of "download" violations. Moreover, more than one-third (34 percent) of all data leakage policy violations occur on mobile devices. This is disproportionately high as compared to total cloud app consumption from mobile devices. Netskope researchers suspect that IT administrators have set stricter policies for mobile devices based on the higher inherent risks associated with mobile access, whether through a device purchased by the company or brought in by the employee through a BYOD program. The report identified the top 20 apps used by enterprises based on distinct app sessions. This reflects all cloud app access points tracked by the Netskope Active Platform, which includes perimeter device (e.g., firewalls, gateways, etc.) log analysis and real-time visibility of campus PC, remote PC, and mobile device (e.g., smartphones, tablets). These apps are: Google Drive, Facebook, Twitter, GMail, YouTube, LinkedIn, Dropbox, Pinterest, Microsoft OneDrive, iCloud, Salesforce, Box, Jive SBS, LiverPerson, Microsoft Office 365, Evernote, WebEx, Amazon CloudDrive, Concur, and Weibo. To read more click **HERE**