THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

2 November 2016

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

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

Newsletter Team
* SA Jeanette Greene
Albuquerque FBI
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
Click **HERE** to request for your employer-provided email address to be added to this product's distribution list

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, Air Force Research Labs, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, MDA, NAG, NCIS, NGA, NRO, Sandia National Labs and the US Attorney's Office

Distribution
Do NOT forward this product to a personal email account (e.g. Hotmail).

You may forward this product to U.S. person co-workers or other U.S. agency / U.S. company email accounts

This product may NOT be altered in any way or copied / pasted into a database system or Internet forum

This Issue's News Articles:

Microsoft: Google-Disclosed Windows Flaw Exploited by Russian Hackers Fancy Bear

Softpedia, 2 Nov 2016: Microsoft has already expressed its frustration with Google's decision to go public with an unpatched vulnerability in Windows, especially because it is already being exploited in the wild, but it turns out that the on-going attacks are connected to a Russian group known for political hacks. The Redmond-based software giant explained in an advisory on its website that the recently-discovered Windows vulnerability is currently being used for attacks launched by a group called STRONTIUM, who is also known as Fancy Bear and is based in Russia. Microsoft claims that the group conducted "a low-volume spear-phishing campaign" against a series of targets, but the company hasn't revealed how many of these attacks were successful or not. Spear phishing attacks generally involve messages submitted to vulnerable targets through different communication channels such as email and which include links or attachments that in the end lead to malicious code used to exploit unpatched flaws. What's interesting is that Fancy Bear has been often linked to political hacks, and the United States government itself accused Russia of launching attacks against several American targets in order to disrupt the local election. According to Reuters, Fancy Bear works for the GRU, Russia's military intelligence agency and which the United States has blamed for the attacks against the Democratic Party. Microsoft hasn't revealed if any political attacks were launched using the newly discovered Windows vulnerability. "We have coordinated with Google and Adobe to investigate this malicious campaign and to create a patch for down-level versions of Windows. Along these lines, patches for all versions of Windows are now being tested by many industry participants, and we plan to release them publicly on the next Update Tuesday, Nov 8," Microsoft says. At the moment, Microsoft says that it's working with Google and Adobe to test the patch, but Windows 10 users with Microsoft Edge are already protected against attacks. To read more click **HERE**

Russian President Vladimir Putin Wants Microsoft Out of the Country

Softpedia, 2 Nov 2016: Russia already has a plan to cut down usage of foreign software by supporting local companies and applications, but President Vladimir Putin is reportedly planning to accelerate the transition by getting rid of Microsoft products as soon as possible. And in his opinion, there's a good reason why this should happen as soon as possible: Microsoft software can be used in the cyber war against other countries, and the United States could turn to products such as Windows and Office to infiltrate in Russia's systems.

NBC News claims it has obtained a document from the US Homeland Security which confirms that Russian hackers used malware injected into a Microsoft Office document to shut down the Ukrainian electrical grid last year, so Vladimir Putin is afraid that a similar tactic can be used by Americans against Russia as well. Putin is now trying to get rid of foreign software in both the government and state-controlled companies, pushing for the adoption of local solutions that can be easily controlled and looked into should any fears of spying occur. A senior US Intelligence source told NBC News that getting rid of Microsoft is a priority for Vladimir Putin, as he thinks the software giant could be directly tied to spying activities launched by the United States. "Not only because they are the most prominent American company in the IT space, but they are also known to the Russian people and businesses as an easily understood collaborator with US Intelligence," the insider said. Microsoft has already explained that it's not involved in any spying activities, and clearly explained that it's not collaborating with the US government, or any other government, to inject backdoor in its software. To read more click **HERE**

FBI offers free online cyber investigation training

GCN, 28 Oct 2016: Law enforcement officers can now learn to properly secure digital evidence from cell phones, laptops and electronic devices at crime scenes with a self-guided online training program from the FBI. The FBI has made its Cyber Investigator Certification Program freely available so that first responders can improve their technical knowledge and follow best practices for cyber investigations. These self-guided courses are now available for all local, state, tribal and federal law enforcement members and are intended to reduce errors in securing digital evidence. The first course was developed in October 2015 specifically for law enforcement first responders. It has nine modules covering software, hardware, the internet and social networks, encryption, legal tools and digital evidence. Specific topics range from cloud and metadata to networks and search warrants for electronic evidence. The course features instructors and cyber experts from the FBI, Carnegie Mellon and other law enforcement agencies who present material on how responders should investigate cases with digital evidence. When the entire training is complete, officers receive a course certificate. The responders' training is the first of four cyber courses that will make up Level 1. The other courses will address specific issues such as digital harassment, online fraud, child enticement and identity theft. Level 2 courses will cover malware, worms and viruses and will be for more advanced officers. Those interested can access it through their Law Enforcement Enterprise Portal account. To read more click **HERE**

Can the phishing epidemic be stopped?

GCN, 26 Oct 2016: Researchers at Germany's Friedrich-Alexander University (FAU) recently conducted two spear-phishing studies. Before the experiment was underway, a questionnaire was sent to all participants asking them to "rate their own awareness of security." Of the 1,700 participants, 78% claimed they were aware of the risks of clicking on unknown links. Astonishingly, despite four-fifths of participants identifying themselves as security conscious, 56% clicked on unknown links in email messages, and 37% clicked on unknown links sent in Facebook messages. In speaking about these results, Zinaida Benenson, FAU's chair of computer science and leader of the study, told Ars Technica, "the overall results surprised us." The results of this study are daunting for both private and public sector organizations, as the most common remedy for phishing attacks to date has centered on human intelligence, or the belief that extensive employee training can transform ordinary workers into hyper-vigilant phishing detectives. Phishing attacks have evolved in sophistication and frequency since they first originated in the 1990s. The first recorded mention of the term 'phishing' was found in AOHell, a tool released in 1995 to hack Windows America Online (AOL) users by allowing the attacker to pose as a company representative and steal passwords and credit card information. AOL influenced many future phishing scams and, over the years, phishers transitioned from amateur to professional cyber criminals. Phishing attacks have evolved from a matter-of-fact nuisance into an epidemic that can cost up to $4 million per event to remediate. Perpetrated by every type of criminal, from nation-state actors and hacktivists to script-kiddies and fraudsters, phishing now accounts for 95% of all successful cyberattacks worldwide. In the first quarter of 2016, phishing attacks surged by 250% -- the highest since 2004, according to the Anti-Phishing Working Group. In commenting on the surge, the APWG's co-founder and Secretary General Peter Cassidy said, "The threat space continues to expand despite the best efforts of industry, government and law enforcement." More effective than traditional phishing scams are spear-phishing attacks. This type of attack carefully targets employees with emails crafted to appear to be from a colleague. Spear-phishing attacks have played a role in

some of the largest cyberattacks to date, including those that hit JPMorgan Chase, Target and Sony. In March 2016, someone posing as Snapchat's CEO targeted the company's payroll department requesting employee information and, because the email's recipient didn't recognize the scam, 700 employees' payroll information was exploited. These types of attacks have also exposed millions of W-2 employee data records in large enterprises like Time Warner Cable, healthcare networks and insurance companies. It's simple: people aren't perfect. In fact, according to a recent IBM Security Officer Assessment, "95% of information security incidents involve human error." Overall, there are numerous reasons why both aware and unaware people click on suspicious links. Everyone from a CEO to a janitor can fall victim to a phishing scam by simply not paying attention, multitasking or giving in to curiosity, confusion, fear, gullibility and implausibility. A 24-year-old junior-level employee will find it hard not to click on a link within an email that looks exactly like it's coming from a superior. Studies show that this type of context-rich phishing attack containing a deadline and feared consequence (loss of access to an email account, for example) is also positively correlated to the click-rate. According to a 2015 study conducted at the University of Buffalo, "the more urgent the message appears, the more likely people are to fall for it." Other analysis concludes that phishing attacks targeting social media accounts have a higher success rate. InfoWorld's Robert A. Grimes suggests that that professionalization of phishing attacks may also play a role: "Today's professional internet criminals work 9-to-5 days, pay taxes, and get weekends and holidays off. The companies they work for often have dozens to hundreds of employees, pay bribes to local law enforcement and politicians, and are often seen as the employer of choice in their region. Working for companies that break into companies in other countries is often proudly worn as a patriotic badge." For public sector organizations in particular, phishing attacks cannot be considered the cost of doing business, which is sometimes the position of the private-sector enterprise. A successful attack can potentially lead to a breach of networks or servers that can compromise the integrity, confidentiality and availability of sensitive information or national security. Employee training is essential; it should remain an important part of an organization's phishing mitigation strategy, despite being costly, only partially effective, time consuming, and difficult to keep up with the latest phishing methods. However, as we've seen with the increase of attacks in 2016, phishing scams will continue to hit inboxes, because no matter how much time, money and resources organizations spend on employee education, a percentage of workers will eventually take the bait. To read more click **HERE**

'Clunky,' low-tech voting system still vulnerable to hacks

GCN, Oct 24, 2016: In the wake of high-profile hacks of Democratic Party systems and attempts to infiltrate state voter databases, intelligence and homeland security officials have been rushing to reassure Americans that the upcoming election cannot be hacked. But one cybersecurity think tank says not only are voting systems vulnerable, they are easy to hack. FBI Director James Comey recently described the U.S. voting system as "clunky as heck," and because it is not a high-tech networked system, "it is hard for an actor to reach our voting processes." Panelists at a discussion sponsored by the Institute for Critical Infrastructure Technology did not dispute the characterization of voting systems as clunky, but they argued that it does not make them immune from hacking or manipulation. The panelists said even machines that are not connected to any network can be corrupted via removable media such as USB drives, and the black-box nature of many voting systems means there is no way for election officials to run diagnostics before or after votes are cast. ICIT recently released a two-part report [**link**], titled "Hacking Elections Is Easy," that outlined a range of vulnerabilities, infiltration points and tactics that could be used to undermine credibility in an election or even manipulate the results. "In all likelihood, cyber-physical attacks against electronic voting systems may continue to go unnoticed due to a lack of cyber-hygiene culture, a lack of verifiable and thoroughly tested security mechanisms, a lack of standardization, and a lack of public attention," the report states. Furthermore, "in 2016, 43 states relied on voting machines that were at least 10 years old and that relied on antiquated proprietary operating systems such as Windows XP, Windows 2000, unsupported versions of Linux, and others," the report states. "Vulnerabilities for these operating systems are widely available for free download on Deepnet." The report also says electronic voting machines are so unsophisticated that an "[18-year-old] high school student could compromise a crucial county election in a pivotal swing state with equipment purchased for less than $100." In addition to manipulating individual machines, the panelists said that when devices are connected to networks to tabulate or transmit results, those results can be intercepted or manipulated. "If you wanted to go influence results on a national scale, you're not going to be successful," said Tony Cole, an ICIT fellow and a vice president at FireEye. "However, if you want to go influence the election in a swing state, in a regional area where it could have a

significant influence, you potentially could." Cole said a concerted effort by a team of individuals, possibly with nation-state backing, could tip a close election one way or the other. "All these voting systems today are in church basements locked up, in elementary schools -- I mean, those are our polling places," he said. "Wherever those systems are stored, it would not be difficult for somebody over a period of four years to work on actually compromising a multitude of those systems...in a swing region in a swing state. It wouldn't difficult at all to have a small, dedicated team focused on that." Most election workers do not have the training or expertise to know whether anyone is trying to tamper with hardware, Cole said. Plus, they are vulnerable to phishing scams and might accept free USB drives that hackers could use to access systems. However, he argued that a more likely and feasible method of manipulating an election is downstream in the tabulation and data transmission process. "Invariably, there are going to be some regions, some states where people have machines that they are interconnecting to the tabulation system, so once you have that, you bridge the air gap and you have the possibility of a tainted result," he said. Cole said an organization such as the National Institute of Standards and Technology should issue mandatory security standards for electronic voting systems to improve election security. But he warned that the approach would not eliminate the problem. "Everything is hackable given enough time and resources, and people need to be aware of that," he said. To read more click **HERE**

DHS working to protect emergency call centers against denial-of-service attacks

GCN, 24 Oct 2016: The distributed denial of service attack on managed DNS provider Dyn that made portions of the internet unreachable on Oct. 21 is just the latest example of the disruption caused by a system that finds itself overwhelmed with requests. Experts are still dialing for dollars when it comes to ideas for how to mitigate the risk, or even the impact, of a potential telephony denial-of-service attack on the 911 emergency services system. Read more. Is an attack on emergency services just one call away? A recent study revealed how easy it would be for bad actors to overload and disable infrastructure for the 911 emergency services in the United States. Read more. Similar to DDoS attacks, telephony denial-of-service attacks – where bad actors flood the system with illegitimate calls to knock out access to emergency services or other critical communication -- are reportedly on the rise. Tech-savvy criminals, hacktivists and even malicious nation-states see the phone system as a critical way to strong-arm federal or local authorities to pay them ransom, pay attention to their cause or just wreak havoc. With more government services facing potential cyber threats by telephone as well as online, the Department of Homeland Security has a cluster of efforts underway to lower the risk and the impact of potential telephone system-based attacks. Such attacks can swamp a 911 call center, causing a potentially life-threatening risk. In a TDoS attack an overwhelming number of calls are sent to the 911 system, and "the high number of bogus calls effectively ties up system resources so that actual 911 calls may not get through," DHS Science and Technology Directorate Program Manager Daniel Massey said. "As attacks become larger and more sophisticated, it is very important that systems for defense also improve to meet this threat," he added. "Our project can play a significant role in helping defend against future attacks." In fact, DHS has a number of efforts underway to try and stem the tide of TDoS attacks, according to Mark D. Collier, CTO of SecureLogix Corp., a San Antonio, Texas-based telephony technology vendor working with DHS. Their core project together seeks ways to detect spoofing -- or differentiating fake calls from legitimate ones -- and aims to apply this to potential TDoS attacks, Colliers said. In another project, in conjunction with the University of Houston, SecureLogix and DHS are investigating how the move to Next Generation 911 might impact TDoS attacks, particularly in relation to emergency services. "When you're dealing with 911, this could be a real emergency situation," Collier said. "We want to make sure that we are never dropping the right call." Collier said the pilots his company is working on include at least two city 911 call centers and a major dispatch line for police and fire fighters. Larry Shi, principal investigator for the University of Houston, said that different government agencies including the FBI and DHS have noticed the "growing number of TDoS attacks against both commercial call centers and emergency communication systems. Without proprietary protection, these attacks against 911 call centers can easily make the service unavailable which may cause serious consequences, like loss of lives." The results of the pilot deployments should help demonstrate the effectiveness of the solution identify issues that may still need to be resolved and show how the results can be widely applicable to 911 systems around the country, as well as other critical systems that are vulnerable to telephony attacks. To read more click **HERE**

Continuous risk mandates continuous protections

GCN, 21 Oct 2016: After more than 16 years, the Office of Management and Budget released the long-awaited revision of its Circular A-130, "Managing Information as a Strategic Resource," [**link**] the governing document for the management of all federal IT systems. This circular has been updated to better reflect the challenges associated with IT systems management as well as an evolving information security threat landscape. Ordinarily, an update to a regulatory document like A-130 would not garner much attention around the Beltway, especially during an election season. But after the Office of Personnel Management data breach in June of 2015, the revised A-130 could not have come at a better time, especially for agency officials tasked with modernizing legacy IT systems and safeguarding information assets against persistent cyber threats. The new document reflects contemporary challenges associated with federal IT systems management in the landscape of ever-growing concerns around cyberattacks, data breaches and sensitive data exposure -- the grim reality born from the OPM breach. In particular, A-130 solidifies the link between information security and privacy, and it establishes legal responsibilities for executive agencies to continually monitor, safeguard and dispose of personally identifiable information (PII). Continuous privacy and vulnerability monitoring are now necessary responsibilities of every agency, especially as more employees and contractors access agency-owned information through a variety of mobile and enterprise content management (ECM) systems. By adhering to the guidelines below, agencies will have the fundamentals to secure their systems in accordance with the requirements and best practices laid out by OMB. "Agencies' privacy programs shall maintain an inventory of PII, regularly review all PII maintained by the agency, and comply with applicable requirements regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII." -- OMB, A-130 Circular, Appendix II: Considerations for Managing PII A-130 strikes new ground with updated language surrounding the protection of PII within agency IT systems. Agency heads bear "ultimate responsibility" for ensuring proper compliance with the requirements of the circular, including the foundational responsibility of inventorying all PII within agency systems. Indeed, understanding what data an organization holds is necessary for any information security strategy to be successful. Agencies can't expect to mitigate against data breach threats without being able to properly catalog all of the sensitive data they hold -- across databases, network drives and ECM systems. Accordingly, agencies should incorporate solutions that can properly discover and classify content containing PII across those systems, especially in legacy applications that are no longer in use. "Agencies shall… implement access control policies for information resources that ensure individuals have appropriate authorization and need, and that the appropriate level of identity proofing or background investigation is conducted prior to granting access." -- OMB, A-130 Circular, Appendix I: Responsibilities for Protecting and Managing Federal Information Resources End users are the weakest link in any security chain, and the vast majority of incidents implicating data privacy occur as a result of inadvertent user error. A-130 establishes the position of a senior agency official for privacy (SAOP) within every federal agency, who bears responsibility and accountability for defining information governance strategies consistent with these new privacy and security mandates. Successful A-130 compliance means that agencies must develop and adhere to strict information governance programs that incorporate defined guidelines around the lifecycle of PII content -- from the moment of data creation to its dissemination and disposition. Employees and contractors, in particular, need comprehensive and continuous training and must comply with governance rules designed to regulate how, when, why and where PII should be created, stored and shared. "Agencies shall… implement policies of least privilege at multiple layers -- network, system, application, and data so that users have role-based access to only the information and resources that are necessary for a legitimate purpose." -- OMB, A-130 Circular, Appendix I: Responsibilities for Protecting and Managing Federal Information Resources A well-defined information governance strategy will always be designed around the concept of 'least privilege,' which holds that end users should be granted only minimal access to IT systems and applications that are necessary for the execution of their job responsibilities. Most leading studies, including research from the 2016 Verizon Data Breach Investigations Report and the Ponemon Institute surveys, conclude that the vast majority of data breaches result from compromised user credentials. In such instances, a threat actor need only determine which users have the most privilege within a system (such as an agency head or IT administrator) in order to access the most sensitive data. Ensuring that the least-privilege principle is followed is a good way to mitigate the risk of sensitive data theft via stolen user names and passwords. While this concept is understood within IT security teams, end users often gain access to sensitive business documents and files that don't pertain to their job functions. This is especially true within ECM systems designed for document storage and collaboration. As SAOPs and agency heads develop information governance

strategies at large, they should also look to deploy solutions that can automate the management and auditing of user privileges across systems and applications. Solutions that can proactively respond to changes in user permissions or detect and alert on suspicious activities (such as excessive document downloads) go a step further in automating security functions and enabling a more refined security process. "Agencies shall... continuously monitor, log, and audit the execution of information system functions by privileged users… to detect misuse and to help reduce the risk from insider threats." -- OMB, A-130 Circular, Appendix I: Responsibilities for Protecting and Managing Federal Information Resources Auditing gives administrators the ability to review log files around network activity to help respond to past, current and future security threats. Since compromised credentials are the most frequent avenue for a breach, auditing lets administrators examine what their users are doing within the network -- from configuration changes to downloading or sharing sensitive documents. To read more click **HERE**