The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

29 April 2014

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

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, Sandia 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 open source data

Homeland Security Warns Against Using Internet Explorer

Boston.com, April 28, 2014: The Department of Homeland Security issued an advisory on Sunday warning Americans not to use Internet Explorer after a dangerous bug was exposed, according to USA Today. The bug, discovered over the weekend by research firm FireEye, allows for "watering hole" attacks, according to the report. Instead of hunting down individuals using the buggy browser, hackers instead install malicious code on regular websites. If you use the vulnerable browser to view the site, that code then infects the user's computer. It's a remote code execution vulnerability, which in English means a bad guy can make a target computer run software after a successful attack. "The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user within Internet Explorer," Microsoft's alert reads. The phrase "arbitrary code" means pretty much any software that the attacker chooses to run. The bug affects Internet Explorer versions 6 through 11, according to FireEye. If you must continue using the browser, FireEye suggests disabling all Adobe Flash plugins. To read more click **HERE**

One sector especially at risk for cyber attacks, new report says

inShare.by Insurance Business, 29 Apr 2014: The increasing importance of cyber risk insurance has been well-documented, but new information suggests one industry is more at risk of cyber attacks than any other. According to data from the Department of Homeland Security (DHS), more than 50% of investigated cyber incidents from October 2012 to May 2013 occurred within the energy sector. To help bolster client safety, producers advising energy companies on cyber security need to do more than provide industry-appropriate coverage, advised global broker Marsh, which compiled a report on the DHS statistics. Energy company clients will need advice on proper employee training, system penetration testing and periodic treat assessment reviews. Producers should also work with clients to develop an effective plan of action if attacks do occur. "Definitely have a response plan. It will limit a lot of confusion and costs," said Jake Kouns, chief information security officer at Risk Based Security. Kouns recommended having a forensics team on alert to investigate the attack, as well as a system for notifying "the affected state agencies." That latter piece of advice is something many companies in the energy industry don't follow. Marsh noted that in all of 2012, just 198 cyber attacks were reported to the government. Christine Marciano, president of Cyber Data-Risk Managers and specialist in cyber security, says the attacks on the energy sector represent a growing trend in cyber attackers' motivations—instead of stealing information for financial gain, attackers are now seeking to cause as much havoc as possible. "[Attackers] have political agendas with a political motivation," Marciano said. "Their attacks can impact political structure through the corruption and destruction of our critical infrastructure systems…targeting and potentially harming civilians, causing havoc and property damage and generating fear." If they are successful, the results could be disastrous both for the company and their customers. "A power grid interruption as a result of a cyber attack has the potential to cost utilities and other infrastructure facilities millions of dollars in lost revenue, regulatory fines, and additional expenses to restore operations and to improve cyber securities defenses, not to mention reputational damage," said Matt McCabe, a senior advisory specialist with Marsh's Network Security and Privacy Practice. To read more click **HERE**

Heartbleed: Understanding When We Disclose Cyber Vulnerabilities

TMCnet, 28 Apr 2014: The White House issued the following blog: When President Truman created the National Security Agency in 1952, its very existence was not publicly disclosed. Earlier this month, the NSA sent out a Tweet making clear that it did not know about the recently discovered vulnerability in OpenSSL known as Heartbleed. For an agency whose acronym was once said to stand for "No Such Agency," this step was unusual but consistent with NSA's efforts to appropriately inform the ongoing discussion related to how it conducts its missions. While we had no prior knowledge of the existence of Heartbleed, this case has re-ignited debate about whether the federal government should ever withhold knowledge of a computer vulnerability from the public. As with so many national security issues, the answer may seem clear to some, but the reality is much more complicated. One thing is clear: This administration takes seriously its commitment to an open and interoperable, secure and reliable Internet, and in the majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest. This has been and continues to be the case. This spring, we re-invigorated our efforts to implement existing policy with respect to disclosing vulnerabilities - so that everyone can have confidence in the integrity of the process we use to make these decisions. We rely on the Internet and connected systems for much of our daily lives. Our economy would not function without them. Our ability to project power abroad would be crippled if we could not depend on them. For these reasons, disclosing vulnerabilities usually makes sense. We need these systems to be secure as much as, if not more so, than everyone else. But there are legitimate pros and cons to the decision to disclose, and the trade-offs between prompt disclosure and withholding knowledge of some vulnerabilities for a limited time can have significant consequences. Disclosing a vulnerability can mean that we forego an opportunity to collect crucial intelligence that could thwart a terrorist attack stop the theft of our nation's intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks. Building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our national security interest. But that is not the same as arguing that we should completely forgo this tool as a way to conduct intelligence collection, and better protect our country in the long-run. Weighing these tradeoffs is not easy, and so we have established principles to guide agency decision-making in this area. We have also established a disciplined, rigorous and high-level decision-making process for vulnerability disclosure. This interagency process helps ensure that all of the pros and cons are properly considered and weighed. While there are no hard and fast rules, here are a few things I want to know when an agency proposes temporarily withholding knowledge of a vulnerability: * How much is the vulnerable system used in the core internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems? * Does the vulnerability, if left unpatched, impose significant risk? * How much harm could an adversary nation or criminal group do with knowledge of this vulnerability? * How likely is it that we would know if someone else was exploiting it? * How badly do we need the intelligence we think we can get from exploiting the vulnerability? * Are there other ways we can get it? * Could we utilize the vulnerability for a short period of time before we disclose it? * How likely is it that someone else will discover the vulnerability? * Can the vulnerability be patched or otherwise mitigated? Enabling transparency about the intersection between cybersecurity and intelligence and providing the public with enough information is complicated. Too little transparency and citizens can lose faith in their government and institutions, while exposing too much can make it impossible to collect the intelligence we need to protect the nation. We weigh these considerations through a deliberate process that is biased toward responsibly disclosing the vulnerability, and by sharing this list we want everyone to understand what is at stake. I hope this post will instill some confidence that your government is acting responsibly in the handling of this important issue. To read more click **HERE**

AOL breach confirmed, bigger than initially thought

Heise Security, 29 Apr 2014: Recent spam emails apparently sent from AOL email addresses and hawking diet products are a direct consequence of a breach of the company's networks and systems, AOL has confirmed on Monday. "AOL's investigation began immediately following a significant increase in the amount of spam appearing as "spoofed emails" from AOL Mail addresses," the AOL Mail Team shared. The company is working both with the federal authorities and external forensic experts to get at the bottom of the matter. The investigation is still ongoing, but they have discovered that the attackers have accessed information on about 2 percent of user accounts, belonging to an estimated half a million of users. What information was taken? Users' email addresses, postal addresses, address book contact information, encrypted passwords and encrypted answers to security questions. Certain employee information was also compromised. There is also good news: so far, it seems that this encryption protection has not been broken and, also, no financial information provided by the users has been accessed. AOL has been notifying users of the breach, and is urging them to change their passwords and security question and answer just in case. They are also warning them to be wary of emails claiming to come from AOL and containing links for resetting passwords. "Large-scale breaches like this usually lead to widespread phishing attacks, which prey on people's security concerns in an attempt to trick them into revealing more data," commented Keith Bird, UK managing director of Check Point. "Users should only reset their passwords via the main website, and never from emails, no matter how plausible they appear to be." "If you believe you are a victim of spoofing, consider letting your friends know that your emails may have been spoofed and to avoid clicking the links in suspicious emails," the security team has also added. In the wake of the aforementioned spam run, the company has also changed their DMARC policy "to tell DMARC-compliant email providers like Gmail, Yahoo! Mail, Outlook.com and others (including AOL Mail itself) to reject mail from AOL addresses that are sent from non-AOL servers." "Sending mail on behalf of AOL Mail users from non-AOL servers had been a common and legitimate practice for services like mailing lists and bulk senders. But it also provided the means for spammers to spoof addresses as described above. By switching AOL Mail's policy to 'reject,' we significantly thwart spammers' ability to spoof AOL addresses," the company explained in a breach-related FAQ section. To read more click **HERE**

News Adobe patches actively exploited vulnerability in Flash Player

IDG News Service, April 28, 2014: Adobe Systems released emergency security updates for Flash Player in order to fix a vulnerability that has been exploited in attacks against users since earlier this month. The attacks were discovered by security researchers from Kaspersky Lab and were launched from a website set up by the Syrian Ministry of Justice to receive complaints about law violations. It's not clear who was behind the attack, but the site had been compromised in the past by hackers. "We received a sample of the first exploit on April 14, while a sample of the second came on April 16," Vyacheslav Zakorzhevsky, manager of the vulnerability research group at Kaspersky Lab said in a blog post Monday. "The first exploit was initially recorded by KSN [the Kaspersky Security Network] on April 9, when it was detected by a general heuristic signature." While the two exploits leveraged the same, previously unknown, vulnerability in Flash Player they targeted users in different ways. One exploit could have been used to infect any computer with Flash Player installed, but the second specifically required Adobe Flash Player 10 ActiveX and the Cisco MeetingPlace Express Add-In to be installed on the targeted systems. The Cisco Unified MeetingPlace Express is a Web collaboration and video conferencing product developed by Cisco Systems and the Kaspersky researchers believe the exploit authors were trying to use it to spy on their targets. It's not known what kind of malware the exploits delivered because the payload files that they were designed to download and execute on the victim computers had been removed from the remote server where they were hosted by the time the attacks were discovered. Given the nature of the site used to host the exploits and the fact that all identified victims -- seven unique users -- were based in Syria, "we believe the attack was designed to target Syrian dissidents complaining about the government," Zakorzhevsky said. The vulnerability was fixed Monday in the newly released Flash Player 13.0.0.206 for Windows and Mac and Flash Player 11.2.202.350 for Linux. The Flash Player versions bundled with Google Chrome, Internet Explorer 10 on Windows 8 and Internet Explorer 11 on Windows 8.1, will get the fix automatically through the respective update mechanisms of those browsers. "Although we've only seen a limited number attempts to exploit this vulnerability, we're strongly recommending users to update their versions of Adobe Flash Player software," Zakorzhevsky said via email. "It is possible that once information about this vulnerability becomes known, criminals will try to reproduce these new exploits or somehow get the existing variants and use them in other attacks." It's likely that cybercriminals will try to profit from this vulnerability even with a patch available, because it will take some time for all users to update their Flash Player installations, Zakorzhevsky said. "Unfortunately this vulnerability will be dangerous for a while." To read more click **HERE**