The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

15 May 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

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

May 14, Softpedia – (International) **Adobe fixes Flash Player and Reader vulnerabilities reported at Pwn2Own 2014.** Adobe released a total of 17 security updates for its Adobe Reader, Acrobat, and Flash Player, including 6 vulnerabilities in Flash deemed critical. Users are advised to update their installations as soon as possible. Source: http://news.softpedia.com/news/Adobe-Fixes-Flash-Player-and-Reader-Vulnerabilities-Reported-at-Pwn2Own-2014-442054.shtml

May 14, The Register – (International) **Dogevault praying backups work after confirming attack.** Virtual currency wallet service Dogevault reported that it was compromised by attackers May 11 and had the data on its hosted virtual machines destroyed. The service reported that it was attempting to restore its data from an off-site backup. Source:http://www.theregister.co.uk/2014/05/14/dogevault_praying_backups_work_after_confirming_attack/

May 13, Help Net Security – (International) **Microsoft releases eight security updates.** Microsoft released its monthly Patch Tuesday round of updates, containing eight advisories, two of which were rated as critical. The critical updates close a vulnerability in the Internet Explorer browser and one in SharePoint. Source: http://www.net-security.org/secworld.php?id=16847

May 12, Help Net Security – (International) **Google account passwords stolen in phishing attack.** Researchers at Bitdefender identified a new phishing campaign targeting Chrome and Firefox users that attempts to steal users' Google login credentials. The phishing campaign attempts to use the way Chrome displays data Uniform Resource Identifiers (URIs) to trick users in to logging into a fake Google login page. Source: http://www.net-security.org/secworld.php?id=16835

US retailers set up center for cyber intelligence sharing
Heise Security, 15 May 2014: The US Retail Industry Leaders Association (RILA), along with several of America's most recognized retail brands, launched the Retail Cyber Intelligence Sharing Center (R-CISC). The R-CISC is an independent organization, the centerpiece of which is a Retail Information Sharing and Analysis Center (Retail-ISAC). Among those companies participating with and supportive of the R-CISC are American Eagle Outfitters, Gap, J.C. Penney, Lowe's, Nike, Safeway, Target, VF and Walgreens. Through the R-CISC, retailers are sharing cyber threat information among themselves and, via analysts, with public and private stakeholders, such as the US Department of Homeland Security, US Secret Service and the Federal Bureau of Investigation. The R-CISC will also provide advanced training and education and research resources for retailers. Paul Morrissey, US Secret Service Assistant Director for Investigations said, "The Secret Service actively supports information sharing initiatives such as the Retail Cyber Intelligence Sharing Center (R-CISC) announced today by RILA. The Secret Service also continues its commitment to promote public/private partnerships through its 33 nationwide Electric Crimes Task Forces (ECTFs) and two international ECTF's, which bring together over 6,100 private sector partners, members of academia and local, state and federal law enforcement." "The retail industry is already going to great lengths to minimize risk and stay ahead of cyber criminals. The reality is, cyber-criminals work non-stop and are becoming

increasingly sophisticated in their methods of attack and by sharing information and leading practices and working together, the industry will be better positioned to combat these criminals," states Ken Athanasiou, Global Information Security Director, American Eagle Outfitters. RILA has also consulted with recognized third-party cyber specialists and subject matter experts including CrowdStrike, FS-ISAC and other ISACs, IBM, iSIGHT Partners, Information Security Forum, the National Cybersecurity and Communication Integration Center (NCCIC), National Cyber Security Alliance and Verizon to identify leading practices related to threat information sharing. The R-CISC is open to retailers and merchants of all segments and sizes and aims to become a resource for not only the retail industry, but related merchant industries as well. There are three components of the R-CISC: a Retail Information Sharing and Analysis Center (Retail-ISAC), Education and Training and Research. The Retail-ISAC allows retailers to share cyber threat information among each other and share anonymized information with the US government via a cyber-analyst and a technician embedded at the National Cyber Forensics and Training Alliance (NCFTA). The Retail-ISAC's dedicated cyber-analyst and technician at the NCFTA facility are processing and distilling information about real-time cyber threats, such as new strains of malware, underground criminal forum activity, potential software vulnerabilities, and translating this information into actionable intelligence, in the most usable and timely form for retailers. Education and Training: Through the R-CISC, retailers will be able to learn from key stakeholders and advance leading practices on cybersecurity, cyber risk mitigation and data privacy in a trusted environment. To read more click **HERE**

Dispelling the Myths of Cyber Security

DarkReading, 14 May 2014: Perfect security that focuses on eliminating threats is too expensive and impossible to achieve. Better to think about consequence management. Most of us in the security profession don't have James Bond's 007 licence (or even a smartwatch) to eliminate threats. Instead, we focus on strategies to reduce risk through formulas such as cyberrisk = threats X vulnerabilities X consequences. That practice that assumes we can create near-perfect security by reducing one of these factors to zero. In the real world, it's hard to imagine any CISO worth his or her salt telling the CEO that vulnerabilities have been reduced to zero. A more effective approach might be to focus on consequence management. But to do that, we first need to dispel a few cyber security myths:

- MYTH 1: Prevention, detection, and information-sharing are adequate for protecting systems. The CISO truth is twofold: Intrusions are inevitable, no matter what preventive approaches you use, and your public facing hosts are constantly under attack. There are 86,000 new pieces of malware reported each day. Industry stats show that within a few minutes of going online hosts are under attack.
- MYTH 2: Once a server comes online, we leave it alone until we need to perform maintenance or patching. We have been using this work/time element of security strategy for 15 years. But the CISO truth is that while keeping systems static is a low-work, low-cost strategy, it also creates an opportunity for the criminal. We know that once criminals get into the system they do damage for days, weeks, months, or even years. Target (more than two weeks), New York Times (four months), and Nortel (10 years) are all examples of persistent compromises.
- MYTH 3: All security threats need attention. The CISO truth is that there are ankle biters that are unlikely to cause significant damage, and serious persistent threats to which we must pay attention. The ankle biter causes numerous alarms which overwhelm the security department. The serious persistent threat probably causes one alarm which can be easily missed in the "cacophony of alarms." Turn the alarm "screwdriver" too far to the right and the security team is overloaded. Turn it too far to the left and important alarms are missed. The challenge is to find the alarm level that leads to the persistent threats where serious consequences occur.
- MYTH 4: It's possible to get rid of all vulnerabilities. The CISO truth is that the common vulnerabilities and exposures (CVE) list has more than 50,000 recorded vulnerabilities -- with more added hourly. How are you going to ensure your network (firewalls, IDS, hosts, etc.) can deal with 50,000+ vulnerabilities every day?

- MYTH 5: You can win the cyber security lottery with "predictive systems" that will find the next attack. The CISO truth is that it's probably easier to predict your spouse's mood after many years of marriage than the next attack launched by a criminal you have never met. You know nothing of the person's skills. He or she intentionally uses deceptive techniques and could be 10,000 miles away.

CISOs need to develop strategies that are independent of the attacker, require no prior knowledge to succeed, are easy-to-implement, and keep our servers as secure as they were before they go online. Perfect security is too expensive and impossible to achieve. CISOs are always reflecting and reexamining security myths, and identifying the products and services that make the organization more secure. The uncertainty in the environment has led to general acceptance of defense in depth, with a variety of solutions being included in the mix. To mitigate cyberrisk, CISOs must include consequence management strategies, principally intrusion tolerance, in the solution mix. To read more click **HERE**

Microsoft Rolls Out Windows XP Security Updates for Paying Users

SoftPedia, 15 May 2014: Microsoft yesterday rolled out this month's Patch Tuesday fixes and Windows XP was left out of this rollout for the first time since its release. The software giant says that it's very keen on keeping its promise to let Windows XP unpatched and reminded everyone still running it that it's mandatory to move to another operating system that still gets updates and security fixes as soon as possible. "If you're still on Windows XP, you won't receive any security or non-security updates through Windows Update or Microsoft Update. Support ended for Windows XP April 8. If you continue to use Windows XP without support, your computer will still likely work -- but it will become vulnerable to security risks and over time, its performance will be affected," the company explained in a post on its blog. At the same time, the software giant noted that paying customers are still getting Windows XP fixes and security patches just because they're... well, paying. However, Microsoft emphasizes that this is only happening for a limited period of time, until they manage to upgrade all their computers to Windows 8.1. "There are also specific cases in which some enterprise customers have custom support agreements in place directly with Microsoft. They will temporarily receive security updates for Windows XP to help bridge the gap during their migration process to a more modern operating system like Windows 8.1," it added. Two weeks ago, Microsoft actually broke its promise and released a fix for Windows XP, even though the company retired support for this particular OS version on April 8. The company said that this was only an exception because plenty of Windows XP users are still working to migrate their computers to Windows 8.1, so keeping them secure while doing that is a priority. The flaw affected Internet Explorer on all Windows versions, including XP that is, and allowed an attacker to take control of a vulnerable computer once the user loaded a compromised website. "There was one exception, with the recent release of a security update outside of the normal Update Tuesday cycle. It fixes a critical vulnerability in Internet Explorer for Windows 7, Windows 8 and Windows 8.1 as well as Windows XP," the company said, adding that no other exception would ever be made. At this point, Windows XP is still installed on nearly 26 percent of the desktop computers worldwide, but many expect more users to move to Windows 7 or 8.1 as time passes by. To read more click **HERE**

Foreign Intelligence Agency Suspected of Hacking Belgium's Ministry of Economy

SoftPedia, 15 May 2014: Belgium's Federal Public Service (FPS) Economy has reportedly suffered a data breach. The main suspect is a foreign intelligence agency. According to Belgian publication De Tijd (registration required), Johan Vande Lanotte, the country's deputy prime minister and minister of economic affairs, has confirmed that the department's systems have been breached. A complaint has been filed with the public prosecutor and an investigation has been launched. Officials haven't commented on the incident, but it appears that the attackers, probably a foreign intelligence service, have used a sophisticated piece of malware designed for cyber espionage. Earlier this week, De Tijd reported that Belgium's Ministry of Foreign Affairs was the victim of a sophisticated attack that targeted documents and information related to the crisis in Ukraine. Russia is considered the main suspect. The Belgian government has been the target of numerous cyberattacks over the past months. A different suspect was named each time. Back in

September 2013, when the systems of the Ministry of Foreign Affairs were breached and information on the country's foreign policy was stolen, sources close to the investigation revealed that the United States National Security Agency was the top suspect. That particular attack relied on a piece of malware planted on the ministry's networks since early 2012. Belgium's prime minister was also targeted by hackers on at least two occasions in the past years. To read more click **HERE**

Former NOTW Reporter Hacked Kate Middleton's Phone 155 Times

SoftPedia, 15 May 2014: On Wednesday, a former editor of the now-defunct publication News of the World (NOTW) admitted hacking into the phone of Kate Middleton 155 times. The NOTW phone hacking trial continues. According to the Daily Mail, former royal reporter Clive Goodman took the stand on Wednesday and admitted illegally accessing the voicemails of the Middleton almost every day. The hacks took place between December 2005 and August 2006, when Goodman was arrested. The former reporter also admitted intercepting the voicemails of Prince William, Prince Harry and royal aides. Goodman was sentenced to prison for 4 months in 2007 for hacking the phones of royal aids, but no one has known the full extent of the spying operation until now. He allegedly didn't tell anyone about hacking Middleton, now the Duchess of Cambridge, because no one asked him about it. Interestingly, Andy Coulson, who at the time was the editor of NOTW, denies conspiring to hack into phones, and he denies paying public officials for the phone number of royals. However, Goodman told the court that Coulson knew about what he was doing and even approved weekly payments to him. Rebekah Brooks, another former editor at NOTW, also denied sanctioning phone hacking. She told the court that when she was the editor at the tabloid, between 2000 and 2003, she didn't know phone hacking was illegal, but claimed that she would have considered it a "serious breach of privacy" is she had known what was going on. To read more click **HERE**