The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

22 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

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

May 21, Softpedia – (International) **Security breach at eBay – change your passwords now.** eBay advised all users to change their passwords after it detected an intrusion that compromised a database containing encrypted passwords and other non-financial data. eBay stated that attackers were able to compromise a small number of employee login credentials between February and March, giving them access to eBay's corporate network. Source: http://news.softpedia.com/news/Security-Breach-at-eBay-Change-Your-Passwords-Now-443257.shtml

May 21, IDG News Service – (International) **Public utility compromised after brute-force attack, DHS says.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) stated in a report that an undisclosed public utility was compromised via a brute-force attack on an Internet-facing host that used a simple password system. ICS-CERT determined that the utility's systems were likely exposed to numerous threats prior to the identified intrusion. Source: http://www.computerworld.com/s/article/9248473/Public_utility_compromised_after_brute_force_attack_DHS_says

May 20, Threatpost – (International) **Chrome 35 fixes 23 security flaws.** Google released version 35 of its Chrome browser, closing 23 security issues, 3 of which were rated as high-risk. Source: http://threatpost.com/chrome-35-fixes-23-security-flaws

May 20, SC Magazine – (International) **Infections increasing with ransomware, Kovter.** Researchers at Damballa reported that infections of the Kovter ransomware doubled during April. The Kovter ransomware attempts to blackmail users into paying a ransom and can generate false browser history content to support its scam. Source: http://www.scmagazineuk.com/infections-increasing-with-ransomware-kovter/article/347801/

May 20, SC Magazine – (National) **Lowe's employee info accessible online for about 10 months.** Officials from Lowe's notified about 35,000 current and former employees May 19 that their personal information, including Social Security numbers, was inadvertently backed up to an unsecured computer by a third-party vendor and made accessible via the Internet between July 2013 and April 2014. The vendor blocked access to the data and initiated an investigation upon learning of the issue. Source: http://www.scmagazine.com/lowes-employee-info-accessible-online-for-about-10-months/article/347676/

GFI Software: eBay Hack Was Opportunistic, Not a Large-Scale Attack
SoftPedia, 22 May 2014: It was the lax employee data security that left the door open for the eBay hack and this means that the company isn't the first and won't be the last to fall prey to hackers. "Hackers are becoming far more opportunistic today and are frequently targeting easier pickings in an effort to gain access to systems and steal valuable data. In the last few years, most of the high-profile data thefts that have made the news have come about not

through complex, large scale attacks that have used distributed or large-scale local networks of machines to breach security," said Sergio Galindo, general manager of the Infrastructure Business unit at GFI Software, a company that develops web and mail security, as well as software for networking, security, archiving and more. He has explained for Softpedia that hackers are more opportunistic these days and choose to simply exploit the "IT equivalent of an open window in an otherwise locked building," weak passwords, staff information that's easy to obtain, and open wireless network connections. Galindo mentions that while reports so far have indicated that the hacking incident was facilitated by the lax employee data security, there could be more to the story, varying from weak and easily discoverable passwords to exploitation of insecure network devices in order to breach a system without raising any red flags. "The potential damage to confidence and reputation is also not helped by the confirmation from eBay that the thefts announced today took place as far back as February. The reasons for the delay are not yet known, but we know from past examples that an early admission of a data loss helps minimize the negative impact on customer confidence," said the GFI Software GM, pointing to the bad PR move from eBay. Unfortunately, eBay won't be the last company to fall prey to hack attacks that exploit the weak employee security practices, but this can serve as a learning point for any business. Regular password changes can be a solution, as well as the reeducation of the staff about the real risks associated with keeping passwords jotted down on a piece of paper that's left around for anyone to find. 145 million accounts have been affected by the eBay hack that took place between late February and early March. Email addresses, passwords, and personal information have been stolen, but the passwords are supposed to be encrypted and there's no indication thus far that the security layer was broken. To read more click **HERE**

New Internet Explorer Zero-Day Flaw Found, Windows XP Users at Risk

SoftPedia, 22 May 2014: Security researchers have found another zero-day flaw in Internet Explorer that basically exposes users and makes their computers vulnerable to attacks unless it's patched as soon as possible. The flaw was discovered by HP's Zero Day Initiative, which claims it first contacted Microsoft in October, but the software giant is yet to release a patch. ZDI, which according to its own policy can publicly disclose a security vulnerability 180 days after it contacted the parent company, claims that the zero-day flaw affects Internet Explorer 8 on the majority of Windows versions, including Windows XP. Microsoft pulled the plug on Windows XP on April 8, so when Microsoft releases a patch to address this flaw, users that are yet to update to a newer OS version could remain vulnerable to attacks. According to the advisory published a few hours ago, it all comes down to the way Internet Explorer works with Cmarkup objects and the vulnerability would allow an attacker to easily run arbitrary code on a target computer. "The allocation initially happens within CMarkup::CreateInitialMarkup. The free happens after the execution of certain JavaScript code followed by a CollectGarbage call. By manipulating a document's elements an attacker can force a dangling pointer to be reused after it has been freed. An attacker can leverage this vulnerability to execute code under the context of the current process," ZDI explains in today's advisory. Just like it usually happens with Internet Explorer vulnerabilities, attackers need a compromised website to break into an affected system that's yet to receive the patch. "These websites could contain specially crafted content that could exploit these vulnerabilities. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by getting them to open an attachment sent through email," ZDI said. Microsoft hasn't yet provided details on the vulnerability, but expects the company to come up with at least a Fix It solution in the coming weeks until a full-time patch is being released. We've also reached out to Microsoft for more information on the new zero-day flaw, so we're still waiting for details to find out exactly which versions of IE are affected and how users can remain protected. To read more click **HERE**

FBI head: Cyber crime posing 'enormous challenge'

AP, 21 May 2014: FBI Director James Comey said Wednesday, days after the Justice Department announced charges against five Chinese military officials accused of hacking into American companies to steal trade secrets. "There are two

kinds of big companies in the United States: those who've been hacked by the Chinese and those who don't yet know that they've been hacked by the Chinese," Comey told the Senate Judiciary Committee. The Justice Department on Monday announced a 31-count indictment against Chinese hackers accused of penetrating computer networks of big-name steel companies and makers of solar and nuclear technology to gain a competitive advantage. China denies the allegations. Comey said the increased focus on cybersecurity has heightened his agency's demand for new, tech-savvy experts. To read more click **HERE**