The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

23 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

May 21, IDG News Service – (International) **Point-of-sale attacks accounted for a third of data breaches in 2013, report says.** Trustwave released a report on data breaches that the company investigated in 2013, which found that e-commerce intrusions accounted for 54 percent of investigated data breaches, while point-of-sale (POS) system intrusions constituted 33 percent of data breaches, among other findings. Source: http://www.networkworld.com/news/2014/052114-point-of-sale-attacks-accounted-for-a-281793.html

May 21, The Register – (International) **PayPal Manager bug left web stores wide open to cyber-burglars.** PayPal closed a vulnerability in its PayPal Manager that allowed attackers to change merchants' passwords, hijack accounts, and order merchandise for free. The vulnerability was closed after a researcher at Securatary identified and reported it to PayPal, and the company stated that there was no evidence that customer information had been compromised. Source: http://www.theregister.co.uk/2014/05/21/paypal_account_hijack_vuln_patched/

May 22, Help Net Security – (International) **Sophisticated Google Drive phishing campaign persists.** Researchers at Symantec reported that a persistent phishing campaign targeting Google users is using a Google Drive phishing page that appears more legitimate than most due to it being served over SSL from the Google Drive service itself. Users who fall victim to the phishing page are also redirected to another malicious page and may be exposed to malware infection. Source: http://www.net-security.org/secworld.php?id=16908

May 22, Softpedia – (International) **Hackers bypass iOS 7/iCloud activation lock, free thousands of iPhones (some potentially stolen).** Two researchers created a service which can unlock devices locked by Apple's iCloud Activation Lock system, allowing users to return locked devices to service. The same service could be used by criminals to unlock stolen Apple devices however, and the researchers contacted Apple to inform them of the flaw that allows the unlocking. Source: http://news.softpedia.com/news/Hackers-Bypass-iOS-7-Activation-Lock-Free-Thousands-of-iPhones-443323.shtml

May 21, IDG News Service – (International) **New Internet Explorer zero-day details released after Microsoft fails to patch.** Details of an unpatched zero-day vulnerability in Microsoft's Internet Explorer (IE) 8 browser were released by HP's Zero Day Initiative after the researcher that discovered the flaw reported it 6 months ago. The vulnerability is classified as a use-after-free flaw and could allow an attacker to gain the same user rights as a user who is brought to a malicious Web site. Source: http://www.networkworld.com/news/2014/052214-new-internet-explorer-zero-day-details-281820.html

May 21, SC Magazine – (International) **A billion shortened URLs go down following DoS attack.** Link-shortening service is.gd was disrupted May 18 due to a denial-of-service (DoS) attack that made around a billion links shortened by the service unavailable. Source: http://www.scmagazine.com/a-billion-shortened-urls-go-down-following-dos-attack/article/347958/

eBay Massive Data Theft Gets Investigated

SoftPedia, 23 May 2014: The eBay data breach is being investigated by the European Union. The UK's information commissioner will be working with the European data authorities to look into the incident that affected some 145 million eBay users. According to the BBC, three US states are also investigating the theft of names, email addresses and personal data that occurred between late February and early March. The online marketplace has already started notifying users that they need to change their passwords, although some have been reporting problems when trying to go through the process. Despite this, eBay claims that everything is in perfectly good working order, even though the site is busier than usual these days. "We are sending out millions of emails, and it will take some time. The process is certainly well under way," eBay said. Please mind the fact that the messages sent by the company contain no links. Any other composition of the email should alert you since it could be a phishing attempt. Connecticut, Florida and Illinois have joined forces to investigate the data breach in the United States. The British information commissioner has told Radio 5 live that the incident is very serious, but the ICO couldn't begin an immediate investigation because the data protection laws are outdated and complex. That being said, the UK will have to work with the European Union's data protection office. "There's millions of UK citizens affected by this, and we've been clear that we're monitoring it, but by taking the wrong action under the law now we risk invalidating any investigation," said a spokesperson for the ICO. The data breach that affected eBay involved the theft of email addresses, names, passwords, customer information, while financial details and credit card information remained safe. Even the passwords that were lifted by the hackers should be safe thanks to the level of encryption they're wrapped in. There are concerns about phishing attempts and identity theft, which are quite serious considering that hackers could easily impersonate anyone with the data they got from the eBay accounts. About 145 million users were affected by the breach, the company said, which makes for a really high number of people who could have identity theft problems. The authorities have a long investigation ahead of them and it's likely that eBay could end up in trouble, especially for keeping the secret so long before telling everyone that they needed to change their passwords. To read more click **HERE**

Windows XP Vulnerable Forever Due to Zero-Day Flaw

SoftPedia, 23 May 2014: HP's Zero Day Initiative has recently found a zero-day flaw in Internet Explorer 8, the browser that's currently available on older versions of Windows, including the retired XP, which no longer receives updates and security patches from the software giant Microsoft. While Microsoft has already confirmed the flaw in a statement sent to us today, security experts are warning that, even when the company releases a patch, Windows XP will still be vulnerable to attacks. Wolfgang Kandek, CTO of Qualys, has said in a statement today that replacing Internet Explorer with a different browser is pretty much the fast workaround for those running Windows XP at this point, although he admits that installing a different Windows version is the best possible solution. "Of course, if you still run Windows XP, you will be exposed forever. Switching to a different browser until you can migrate from that OS is probably a good idea," he says. In addition, Kandek explains that Microsoft most likely developed a patch for the zero-day flaw since October 2013, when it was first made aware of the vulnerability in Internet Explorer 8, but the company had to delay its release due to some other publicly disclosed security flaws that affected a wider array of users. The problem in this case is why Microsoft needs so much time to address this new zero-day and why the company delays the release if the patch is already available. "After 6 months Microsoft no doubt has developed a patch for the issue. However, it seems its release was delayed due to the short term nature May's IE patch (MS14-029) which was specifically engineered to address a vulnerability in the use in wild, that was detected by Google's security team. That release took priority over the normal, scheduled release and got Microsoft into this situation with ZDI," Kandek has pointed out. Basically, if your

existing Windows installation can run a newer version of Internet Explorer than 8.0, it would be quite a good idea to update and thus avoid getting your computer hijacked if an exploit is being developed. At the same time, virtually everyone can replace Internet Explorer with a different third-party browser that's obviously not affected by the flaw and keeps you on the safe side. Microsoft has confirmed the existence of the issue but hasn't said anything about the release date of a patch. While the company might opt for an out-of-band patch, it could also very well wait until the next Patch Tuesday on June 10, when some other updates are also planned. To read more click **HERE**