THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

27 October 2014

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

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

October 24, The Register – (International) **iMessage SPAM floods US mobile networks.** CloudMark researchers reported that China-based designer goods counterfeiters are using the Apple iMessage platform to spam users with advertisements, the largest mobile spam campaign in the U.S. so far this year and accounting for over 80 percent of all reported mobile messages in the U.S. Source: http://www.theregister.co.uk/2014/10/24/chinese_imessage_spam_floods_us/

October 24, Securityweek – (International) **Cisco fixes 3-year-old vulnerability affecting security appliances.** Cisco released patches to close a vulnerability in its AsyncOS used in several of the company's security appliances that could allow a remote, unauthenticated attacker to execute arbitrary code with elevated privileges. The vulnerability affects all models of Cisco Email Security Appliances (ESA), Cisco Web Security Appliances (WES) and Cisco Content Security Management Appliances (SMA) running affected versions of AsyncOS. Source: http://www.securityweek.com/cisco-fixes-3-year-old-vulnerability-affecting-security-appliances

October 24, Softpedia – (International) **Adobe Digital Editions now encrypts data collected from users.** Adobe stated that its Adobe Digital Editions ebook software would begin using encryption to send data on users to Adobe's servers starting October 23. Researchers previously discovered the transmission of user data and found that it was not encrypted, posing a security risk. Source: http://news.softpedia.com/news/Adobe-Digital-Editions-Now-Encrypts-Data-Collected-From-Users-463045.shtml

October 23, IDG News Service – (International) **Akamai sees record-setting spikes in size and volume of DDoS attacks.** Akamai released their Q3 2014 State of the Internet report and found that distributed denial of service (DDoS) attacks increased in average bandwidth by 389 percent over the past year, among other findings. Source: http://www.networkworld.com/article/2838293/security/akamai-sees-recordsetting-spikes-in-size-and-volume-of-ddos-attacks.html

October 24, SC Magazine – (International) **Malware on Breyer Horses website for about 18 months, payment card data at risk.** Breyer Horses notified an undisclosed number of consumers who purchased items from the company's Web site between March 31, 2013 and October 6, 2014 that their personal information, including financial data, may have been compromised after attackers installed malware on the company's network. The company has taken steps to address the breach, including updating the code used to run the Web site. Source: http://www.scmagazine.com/breyer-horses-website-compromised-payment-cards-at-risk/article/379137/

October 24, Softpedia – (International) **Three-month database of customer payment info leaked at ScoreSports.com.** American Soccer Company notified customers of ScoreSports.com October 23 that its systems were breached and customers' personal information, including payment card data, may have been compromised between June 1 and September 4. The breach was detected October 21 and the company has since secured its Web site payment system. Source: http://news.softpedia.com/news/Three-Month-Database-Of-Customer-Payment-Info-Leaked-At-ScoreSports-com-463085.shtml

Cyber skills shortage makes UK a soft target for hackers

Heise Security, 23 Oct 2014: A survey conducted by MWR InfoSecurity at 44Con 2014 has revealed that 75% of the information security professionals in attendance believed that a lack of cyber security skills in the UK makes it a potential easy target for attackers. A similar number (74%) thought that people's lack of education when it comes to cyber security is the most serious threat facing businesses today. This presents a huge opportunity within industry and Government to improve cyber skills for all. "What we have here is a case of not only a shortage in highly skilled professionals to combat cyber crime, but also a lack of general education amongst the public and employees that hackers can take advantage of to compromise our national security in Great Britain," said Martyn Ruks, Group Technical Director at MWR InfoSecurity. "This information combined with the fact that three quarters of the industry think the UK is put in a vulnerable position because there aren't enough skilled cyber professionals should be viewed as an opportunity for the UK government and industry to rise to the challenge," continued Ruks. "We believe that if you want to protect something you need to know why someone would want to acquire or damage it and why," said Ruks. "Only by understanding motivations and drivers can you begin to map out what the solutions need to look like which is why, in conjunction with professional training courses, University degrees, security conferences and Capture the Flag competitions, we need to equip people with the right approach and attitude for solving the difficult problems through real world simulated activities and challenges." As well as corporate schemes to improve skills amongst professionals, Government initiatives, such as Get Safe Online promote individual responsibilities when it comes to online safety. "Each and every one of us has a big role to play when protecting ourselves, and the places we work, from online criminals," said Tony Neate, CEO of Get Safe Online. To read more click **HERE**

100 million cloud file analysis reveals shadow data threat

Heise Security, 24 Oct 2014: Elastica conducted a security analysis of more than 100 million files being shared and stored in leading public-cloud applications. Research revealed that 20 percent of broadly shared files contain compliance-related data, 5 percent of enterprise users are responsible for driving 85 percent of the exposure risk, and employees each store an average of 2,037 corporate files in the cloud. Further analysis revealed that files being stored and shared among insiders and outsiders hold sensitive personal health information (PHI) regulated by HIPAA, personally identifiable information (PHI) such as social security numbers, and customer payment card information regulated by the Payment Card Industry Data Security Standard (PCI DSS). The research uncovered that sensitive data shared broadly within and outside organizations without IT security teams' knowledge, known as "shadow data," is an emerging threat within enterprises that are integrating cloud applications into their infrastructures. The extreme volume of sensitive and regulated data being shared in the shadows is placing global organizations at risk of costly compliance violations and major data breaches that could impact millions of consumer identities and accounts as well as corporate IP. Elastica discovered that enterprise employees are each storing an average of 2,037 files and that these files are being shared directly with other internal users, across companies with select users and with the public at large. Data is being placed at risk primarily via files being shared broadly across entire organizations, externally and publicly. Scans on these high-risk files revealed:

- 68 percent are shared with the whole company, across functional groups
- 19 percent are shared with external users
- 13 percent are shared publicly.

In particular, regulated data is in jeopardy, including personally identifiable information (PII), PHI and consumer payment card information. Of all the files that are broadly shared, the analysis found 20 percent contain compliance related data, with the following breakdown:

- 56 percent contained PII, including social security numbers
- 29 percent contained PHI

- 15 percent contained payment card information.

Research also indicates that the vast majority of risk is associated with a relatively small number of users. Just 5 percent of the users sharing high-risk content are driving 85 percent of the resulting risk exposure. This finding highlights the value of identifying the highest-risk users in an organization. In doing so, IT security teams can hone in on the biggest impact in resolving compliance risks. To read more click **HERE**

Most IT sec pros still rely on perimeter security to stop APTs

Heise Security, 27 Oct 2014: 78 percent of IT security professionals are confident that firewalls and antimalware tools are robust enough to combat today's advanced persistent threats, say the result of a new survey from Lieberman Software Corporation. These findings highlight the fact that while cybercrime is on the rise, many organisations are still dangerously relying on outdated perimeter security solutions to defend against the latest threats. The survey, which was carried out at Black Hat USA in August 2014, also revealed that 22 percent of those surveyed do not think that tools like firewalls and antivirus are able to defend against APTs. However, given the surge in organisations suffering advanced targeted cyber attacks, this number should have been much higher. 58% of the polled IT security pros are not confident that their network has never been breached by a foreign state-sponsored attack or advanced persistent threat, and 59% of respondents think a state-sponsored attack will attempt to breach their organization in the next six months. Of these, 44% are not confident that their IT staff can detect the presence of an attacker who attempts to breach their network or extract private data, and the same number of security pros do not think their organization's security products and processes can keep up with new and emerging security threats. Commenting on the survey findings, Philip Lieberman, CEO of Lieberman Software, said: "Our survey reveals that while the majority of organizations are prepared for amateur hackers and low-level criminals, they are completely ill-equipped to deal with today's advanced attacks. Traditional perimeter security products are effective at spotting and stopping known threats, but they can't keep up with today's rapidly increasing volume of advanced targeted attacks. The most effective methods for securing yourself from these types of attacks are the use of air-gap networks (machines not connected to the internet) that disconnect systems with sensitive data. Assume that others have already penetrated your network and institute multi-factor authentication and adaptive privilege management to assure that a compromised system is not a jumping off point for an organization wide attack." To read more click **HERE**

U.K. Hackers who threaten national security could face life sentences

Sophos Security, 24 Oct 2014: Proposed changes to the Serious Crime Bill in the UK could see British hackers facing lengthy sentences where their actions damage national security, the environment, the economy or human welfare in any country. Where the damage caused to human welfare or national security is deemed to be serious enough, the amendment to the Computer Misuse Act 1990 would allow judges to hand out life sentences - a situation some experts believe could be used to target whistleblowers. The Bill reached the report stage at the House of Lords on 14 October where Baroness Williams of Trafford offered up some amendments in an attempt to clarify some of the computer misuse clauses, especially in regard to locations falling outside of territorial waters, such as oil rigs and ships. Last week, the Joint Committee on Human Rights expressed concern over the ambiguity of the planned new legislation in other areas of its wording. Definitions such as "damage to the environment", "damage to the economy" and "damage to national security" were too vague, they said, considering the length of jail time that could be associated with them. "Legal certainty requires that criminal offences are precisely defined so that individuals know how to avoid such sanctions. Vagueness is not permissible in the definition of criminal offences. The broad and vague definition of the new offence of computer misuse appears to be without precedent, and the Bill therefore appears to cross a significant line by using these unsatisfactory concepts in the definition of a serious criminal offence carrying a lengthy sentence." The group did agree, however, that robust laws were required in the face of computer crimes, especially where attacks against critical infrastructure were concerned. The Joint Committee concluded its review of the computer misuse proposals by suggesting further amendments to the Bill to remove those particular

elements altogether. The government, however, is keen to press ahead with the Bill. A Home Office spokesperson claimed that its implementation would ensure that anyone responsible for a serious computer attack would face an appropriate level of justice, worthy of a crime that "blights lives and causes misery across the UK. It is a threat to our national security and costs hard-working taxpayers at least £24bn a year." To read more click **HERE**

Verizon Wireless injects identifiers that link its users to Web requests

ARS Technica, 24 Oct 2014: Verizon Cellular communications provider Verizon Wireless is adding cookie-like tokens to Web requests traveling over its network. These tokens are being used to build a detailed picture of users' interests and to help clients tailor advertisements, according to researchers and Verizon's own documentation. The profiling, part of Verizon's Precision Market Insights division, kicked off more than two years ago and expanded to cover all Verizon Wireless subscribers as part of the company's Relevant Mobile Advertising service. It appends a per-device token known as the Unique Identifier Header (UIDH) to each Web request sent through its cellular network from a particular mobile device, allowing Verizon to link a website visitor to its own internal profiles. The service aims to allow client websites to target advertising at specific segments of the consumer market. While the company started piloting the service two years ago, privacy experts only began warning of the issue this week, arguing that the service is essentially tracking users and that companies paid for a fundamental service that should not be using the data for secondary purposes. For the past decade, Verizon, Comcast, and other Internet service providers have sought ways to turn their access to their customers' traffic into additional revenue. In 2008, "deep-packet inspection" became a much-maligned term after a handful of Internet service providers were found tracking their users' activities on the Web by peering into network packets. Internet service providers learned to quietly deploy the technology for other applications. The issue stepped into the national spotlight in June 2013, when Edward Snowden, a former contractor for the National Security Agency, leaked classified documents outlining the close cooperation between private companies and the agency. The access given to the NSA underscored the privacy dangers of overreaching data collection. Google, Microsoft, Facebook and other companies that gather data on users often receive subpoenas, search warrants, and national security letters directing them to give up the information. Because of the risk of similar legal actions targeting Internet service providers, the companies' push to gather information on their users has made privacy advocates nervous. "This is even at a more serious level than throttling traffic because ISPs are going in and modifying traffic in transit and that's something that they should not be doing," Hoffman-Andrews said. "They are paid by their customers to be trusted conduit for data, and they should be sending that data through faithfully rather than trying to insert or remove things." The service allows websites to request advertisements along with the UIDH from a participating on-demand advertising network. The network can then request market-segment and geolocation information from Verizon to deliver the most appropriate. To read more click **HERE**

Comparing the hash file is a good precaution

SoftPedia, 27 Oct 2014: An "exit node" for the TOR anonymization network located in Russia has been found to serve a modified version of the legitimate code requested by the user. In order to become anonymous, TOR (The Onion Router) connections pass through multiple servers that relay the message in an encrypted form until an exit node is reached, which communicates directly with the destination. A server of this kind has been used to deliver patched binaries, employed in malicious activities; when the user would issue the download request, a tampered executable would be returned, if the connection had gone through the respective Russian TOR exit node. The bad server was discovered by Josh Pitts, penetration tester at Leviathan Security, who also created a binary patching framework, called BDF (the Backdoor Factory), that he presented this year at DerbyCon. Pitts already knew that a great number of binaries were hosted without benefiting from Transport Layer Security (TLS) encryption, and that most of them were not signed, which would prevent their modification in transit. As such, an attacker could rely on the man-in-the-middle (MitM) technique to intercept the request from the user and return a different file than the original one expected by the recipient, without triggering alarms. The researcher resorted to

TOR to increase the chances of finding traces of this type of malicious activity being leveraged in the wild. It took no more than one hour of waiting to bump into a nefarious exit node. More than 1,110 exit servers have been analyzed, and the one encountered by Pitts to be located in Russia seemed to patch almost all binaries the researcher tried to download; "the node only patched uncompressed PE files," he wrote in a blog post. According to the researcher, the original binary is wrapped with another one, and the attackers managed to preserve the icon on the file. Through this method, the simple self-checking mechanisms are bypassed in the case of Nullsoft Scriptable Install System (NSIS), a system that creates installers for the Windows platform. This is a significant issue, since TOR is employed for browsing anonymously by a large number of users, such as journalists in oppressive countries, activists, or whistle-blowers. To read more click **HERE**

Future Wearables Could Allow You to Transfer Data between Devices by Touching Sensors

Softpedia, 27 Oct 2014: Standard wearables today will help you receive notifications on your wrist or track your calorie consumption or the number of steps you've taken, but if that's not nearly exciting for you, listen to this. A group of interns working in the Intel Collaborators program are developing a system called human body communications (HBC) to share data between two devices by virtue of touching a sensor while having a wearable device on. While most of us have thought of wearables working in concert with smartphones, they might actually prove to be really effective when used with a PC or a laptop too, through HBC. Human body communications has been around for some time, under terms such as body area networks, body coupled communications and intra-body communications. What researchers are trying to do is use the human body as a medium to transfer data between computers, by virtue of the electromagnetic field surrounding us all. The idea behind the whole experiment is said to be simple in itself. Basically, you will perform a copy / paste action using a particular touch interface. Placing two fingers on the sensor will move the files through the magnetic field via an electrical signal to the wearable device (in this case it's a ring). Once the info is stored in the ring, one can go to a similarly enabled device and perform the same action (placing two fingers on the sensor) in order to copy the info into the laptop. You can see how this is easily achieved in the video demonstration below. As you can spot in the clip, the ring is a prototype, but there's a catch to the whole situation. For the time being, one can't transfer more than a few bytes of information. But if the technology will be refined in the future, the implications are quite huge. Imagine being able to print from your smartphone or tablet by virtue of a few touch gestures. Another application might be picking up geo coordinates from a mapping application and touching a GPS device to swiftly transmit the location. The team said it had to face challenges related to finding ways of dealing with power loss that goes through the human body. To that end, they fine-tuned electric circuits made up of capacitors and inductors so they could build up a stable connection to transfer the data. This has to happen quite quickly and users will not have to press their fingers on the touchpad longer than a second. Current smart ring products aren't all that creative. Basically, they are just tiny, shrunken smartwatches that can buzz when you have received a notification, but smart rings capable of sending info by virtue of touching a sensor would certainly be something. To read more click **HERE**