The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

5 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 2, Softpedia – (International) **XSS vulnerability found in Google Search Appliance.** An update for the Google Search Appliance index and search device was released after a security researcher identified and reported a cross-site scripting (XSS) vulnerability that is present when the dynamic navigation feature is enabled. Source: http://news.softpedia.com/news/XSS-Vulnerability-Found-in-Google-Search-Appliance-440335.shtml

May 1, Help Net Security – (International) **Microsoft updates IE against latest 0-day, updates also XP.** Microsoft released an out-of-band security update for its Internet Explorer browser to close a zero-day vulnerability that is being actively exploited in the wild. The update also covers the recently-discontinued Windows XP operating system. Source: http://www.net-security.org/secworld.php?id=16786

iOS 7.1.1 Siri Flaw Allows Attackers to Go Past Passcode Lock

SoftPedia, 5 May 2014: Apparently Apple can't shake off passcode lock vulnerabilities no matter how hard it tries. In the latest iOS firmware, a new such bug has been discovered that leverages Siri to bypass the four-digit passcode lock and access contacts on the phone. As demoed in the 2-minute clip embedded below, someone with physical access to a handset running iOS 7.1.1 can perform a few gimmicks to enable Siri at just the right moment and summon the phone's list of contacts with ease. The risks are pretty big, considering that a person's contacts list is one of the most personal forms of data residing on a mobile phone. Apple will need to patch this bug in a future iOS update, perhaps in iOS 7.1.2. While they're at it, we'd also suggest they take a look at the code responsible for crippling our battery life. The best thing you can do to avoid having someone exploit this issue on your phone is to disable the option to have Siri accessible from the lock screen. Another security issue in iOS 7.1.1 deals with email attachments. Discovered by security researcher Andreas Kurtz, the issue at heart is that Mail.app lacks a layer of protection for email messages attachments, one that Apple claims to offer. The Cupertino giant has yet to confirm progress on upcoming iOS updates, but it is known to be working hard on the next-generation iOS 8. This is not the first time Apple has to deal with a passcode lock flaw. Far from it, actually - with almost every new iOS release, hackers and amateurs alike have found ways to trick the phone into thinking that the user has entered the passcode and gain access to its contents. In some cases, the security of the OS has been so weak that people were able to access photos, emails, and even text messages. And although Apple prides itself on taking security matters very seriously, the company has always been slow to address such vulnerabilities both on mobile and on desktop platforms. For example, the aforementioned Mail.app flaw was reported to the Mac maker about a month ago, and the company has yet to issue a patch. Similarly, on iOS whenever someone finds and reports a security hole, Apple takes its time in developing a patch. Although it is understandable that it takes time to get things right, working up an update for a couple of bugs shouldn't be such an ordeal. To read more click **HERE**

Twitter Account of British National Party Leader Nick Griffin Hacked

SoftPedia, 5 May 2014: After hijacking the official Twitter account of the British National Party (BNP), the Anonymous hacker who calls himself Anon_0x03 has taken over the account of Nick Griffin, the chairman of the BNP and a Member of the European Parliament (MEP) for North West England. Griffin's Twitter account was hacked on May 3 and it still appears to be controlled by the hacker. He sent messages on the social media network to various users, including British Prime Minister David Cameron. "Hi Dave. Is there any chance we could have a team up next year? We are getting trashed in the daily mail, you could save us!" the hacker tweeted to Cameron. Anon_0x03 has also changed the profile description for Griffin's account, saying that he's chairman and member of the European LGBT community. The hacker claims that he has also breached Griffin's official website, but at the time of writing, the defacement page appears to have been removed. Anon_0x03 says that the same password was used for the website' administration panel, the Twitter account and an email account. Griffin's Facebook page appears to be untouched, but there's no mention of the Twitter account being compromised. Anon_0x03, who's a former member of a Venezuelan hacktivist group, has also hijacked the BNP's Twitter account. The BNP appears to have recovered the account, but the messages posted by the hacker still haven't been removed. To read more click **HERE**

Man Suspected of Hacking Swiss Banks Arrested in Thailand

SoftPedia, 5 May 2014: Mohamed Yassine Gharib, a 26-year-old from Morocco, has been arrested by Thai authorities. The man is suspected of stealing millions of dollars from the customers of Swiss banks after hacking into their accounts. Gharib is said to have entered Thailand four years ago. His Thai girlfriend, Amornrat Hongklad, has also been brought in for questioning. According to the Chiangrai Times, Thai police issued an arrest warrant in late February after being notified by Swiss police of the suspect's whereabouts. Immigration police detained Gharib in the lobby of the hotel he was staying at. Thai PBS reports that the alleged hacker and his pregnant girlfriend have been evading arrest by taking refuge among People's Democratic Reform Committee protesters. They had left the hotel where Gharib was arrested, but the man forgot his passport. Police figured that he would eventually return for it, so they waited for him. When he came back for the passport, the Moroccan was arrested. Authorities in Switzerland believe that Gharib and around 10 others stole around $18 million (€13 million) from the customers of Swiss banks. Representatives of the police say they're contacting the Swiss embassy regarding the suspect's extradition. It appears that it's pretty common for individuals wanted for cybercrimes to seek refuge in Thailand. In March, Thai authorities reported arresting Farid Essebar, a 27-year-old Moroccan with Russian citizenship known on the hacking scene as Diabl0. Essebar is said to have caused damage of around $4 billion (€2.87 billion) by hacking into the computer systems of Swiss banks. Authorities had been tracking him for two years before they made the arrest. He is also awaiting extradition. In January 2013, Thai police arrested 24-year-old Algerian national Hamza Bendelladj. He was detained at an airport while transiting from Malaysia to Egypt. Bendelladj – who is believed to have played a critical role in developing, marketing, distributing and operating SpyEye malware – was extradited to the United States in May 2013. In the US, he has been charged with one count of conspiracy to commit wire fraud and bank fraud, 10 counts of wire fraud, 11 counts of computer fraud, and one count of conspiracy to commit computer fraud. He could spend a lot of time in prison if he's found guilty. At the time of Bendelladj's extradition, FBI representatives highlighted the fact that the agency expanded its international partnerships to ensure that even cybercriminals who hid overseas could be brought to justice. To read more click **HERE**

German Security Expert Finds Vulnerabilities on the NSA's Website

SoftPedia, 5 May 2014: Matthias Ungethüm, a security expert from Germany, has managed to find a couple of vulnerabilities on the official website of the United States National Security Agency. The expert has told German broadcaster MDR that he first found a cross-site scripting (XSS) vulnerability on the NSA website's homepage. The flaw enabled him to alter the website's appearance. To demonstrate how the issue can be exploited, he replaced one of the banners on the site with one that read "Examine your homepage" in German. XSS vulnerabilities can be exploited by cybercriminals for phishing and to lure users to malicious or spam websites. However, the type of XSS found by

Ungethüm can't be leveraged to permanently change the website's appearance. The changed version of the website is only seen by users who click on a link provided by the attacker. While the XSS vulnerability is not critical, the expert also claims to have identified an SQL Injection flaw on the NSA's website. SQL Injection vulnerabilities are usually more serious because they can be leveraged to gain access to information stored in a website's databases. Ungethüm has told MDR that he hasn't exploited the SQL Injection bug for legal reasons. The expert reported the security holes to the intelligence agency one week before making his findings public. He didn't get any response. However, shortly after the existence of the vulnerabilities was revealed, the NSA addressed them. To read more click **HERE**

Everything Can Be Hacked - It's Just a Matter of Time until Things Get More Serious

SoftPedia, 5 May 2014: Everyone who uses the Internet knows by now that websites can be hacked. However, over the past period, security researchers have demonstrated that any device or machine that's powered by a piece of software can also be hacked. Researchers have demonstrated that routers, set-top boxes, security cameras, TVs, and even fridges can be hijacked and abused by cybercriminals for various purposes, including sending spam, mining for crypto-currencies, and spreading malware. Medical devices can also be hijacked, and the consequences can be deadly. On the other hand, experts have also demonstrated that cars, ships, airplanes, satellites and even the sensors used for traffic control systems can be hacked. So far, we've seen the damage that cybercriminals can cause by hacking a website or a company's networks. We've also heard some "spooky" stories about industrial control systems. A perfect example is the Stuxnet worm which reportedly caused serious damage to Iran's nuclear centrifuges. As far as hacking cars, ships, airplanes, satellites and medical devices are concerned, there haven't been any serious incidents so far. We've seen such scenarios in movies, but that's it. While many manufacturers have come to realize that securing their products against cyber threats is important, for many companies, it's far from being a priority. So how long will it take until someone decides that a keyboard is an effective way to commit a serious crime and get away with it? I'm referring to committing murder or causing serious physical damage, because we've already seen that cyberattacks against a company's networks are already considered a serious crime (e.g. the breach suffered by US retailer Target). I think that 2020, the recent mini-series by security company Trend Micro, shows pretty accurately where we're heading. One day in the near future, everything will be dependent on the Internet, and as that period draws near, we'll probably start witnessing all sorts of serious incidents involving cyberattacks. Currently, while many manufacturers have departments whose goal is to ensure that a product is secure, most are still experiencing difficulties in communicating with external security researchers. The contribution of external researchers is critical, because the vulnerabilities they find are the ones missed by internal security teams. The flaws they find are likely the ones that will be exploited by cybercriminals. The attack methods presented by researchers against cars, airplanes, satellites and traffic control systems are mostly theoretical, and they require a lot of resources to be applied in a real-life scenario. However, as technology evolves so do hacking methods. When they're informed of security vulnerabilities in their products, many companies say "this attack is too difficult to pull off" or "our products are more secure than they appear." This is the point where everyone should start making sure that their products – whether it's software for cars, airplanes, or medical devices – are not vulnerable. Security should become a top priority in the development cycle so that we avoid waking up one day to find out that cybercriminals are actively exploiting software vulnerabilities to (directly or indirectly) kill or hurt people. To read more click **HERE**

CISOs Believe Employees and Politicians Are Least Concerned About Preventing Breaches

SoftPedia, 2 May 2014: Courion, a firm that provides intelligent identity and access management solutions, has surveyed IT security executives at companies with 500 or more employees. It turns out that most chief information security officers (CISOs) are anxious about the possibility that their company might suffer a data breach. More precisely, 78% of respondents say they're anxious. Security executives are aware of the fact that they're responsible for protecting customers' privacy and personal data, and maintaining the equity of the brand. Close to 60% have named protecting customers' privacy as a top priority when addressing a serious data breach. The number one goal for 88% of IT security

executives when addressing a significant breach is privilege abuse, followed at a distance by unapproved hardware (18%), bribery (16%) and email misuse (11%). In the eventuality of an incident, 62% fear the negative publicity that affects the company. Only 1% are afraid of personal embarrassment and only 2% fear the loss of employment for others. Almost 7% are afraid they'll lose their job. For 2014, most consider the education of employees and other end users a top priority (29.4%). Other priorities are better management of user access and insider threats, communicating or enforcing company policy, and managing external threats (e.g. phishing scams). Identity management has been named by 14% their organization's top IT security-related project in the next 12 months. Other projects planned by executives are SIEM (13%), firewall management (13%), DLP (12%) and intrusion management (10%). Mobile device management is a top priority only for 9% of respondents. Almost all CISOs believe that their IT security teams take preventing data breaches seriously. Executive management, the organization's board of directors and law enforcement are also believed to be serious about this issue. At the bottom of the chart, we have employees and politicians. "Our recent survey confirmed what we've been hearing from many customers over the past few years, the role of the senior IT security executive is constantly changing," said Christopher Zannetos, president and CEO of Courion. "Not only are they thought of as the front line defense for protecting sensitive company and customer information, they also feel responsible for brand image and customer satisfaction. IT security cannot tackle all this alone, however," Zannetos added. "We believe, and this survey confirmed, that better employee education and management of user access can provide much needed support for the security team." The complete report is available on Courion's website (**registration required**). To read more click **HERE**

57% of Organizations Don't Think They're Protected Against Advanced Cyber Threats

SoftPedia, 2 May 2014: Websense has published the first part of a Ponemon Institute survey called "Exposing the Cybersecurity Cracks: A Global Perspective." The study is based on the responses of almost 5,000 IT security experts from a total of 15 countries from all over the world. The report reveals that many organizations are still unprepared to handle advanced cyber threats. It also shows that many leaders don't realize the fact that a data breach which leads to the loss of confidential data can have a negative impact on revenue. The numbers from the report show that 57% of the respondents don't think their networks and systems are protected against advanced cyber threats. Furthermore, 63% admit that they can't stop cybercriminals from stealing confidential information. 44% of those who took part in the survey admitted that their organizations experienced one or more serious cyberattacks in the past year. Close to 70% of them believe the attackers leveraged "the cracks" in their existing security systems. Unfortunately, over half of the companies still don't have proper intelligence mechanisms in place, and in many cases the security solutions they're using don't inform them of the root causes of an attack. A total of 80% believe their company's executives don't see the loss of confidential data as something that can result in loss of revenue. Almost half of respondents say board-level executives don't understand security issues as well as they should. When it comes to cybercriminal activity, only 41% of organizations feel they have a good understanding of the threats they face. 37% are certain that their companies lost sensitive information as a result of an attack, but 35% of these respondents don't know what the cybercriminals stole. "While there are significant differences among countries for specific questions (such as availability of cyber attack intelligence), the overall analysis indicates that a majority of security professionals do not feel adequately armed to defend their organizations from threats," explained Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "This challenge is further compounded by a perception that company leaders do not believe that data breaches will lead to loss of revenue. Our research has shown this is simply untrue." The complete "Exposing the Cybersecurity Cracks: A Global Perspective" report is available for download on Websense's website (**registration required**). Those who took part in the survey have, on average, 10 years of experience in the field. They're located in Australia, Canada, the US, Mexico, Brazil, France, Germany, Italy, the Netherlands, the UK, Sweden, Singapore, China, India, and Hong Kong. To read more click **HERE**

Target CEO resigns as data breach fallout continues

USA Today, 5 May 2014: Target announced Monday that Chairman, President and CEO Gregg Steinhafel is out nearly five months after the retailer disclosed the breach, which has hurt its reputation among customers and has derailed its business. The nation's third-largest retailer said Steinhafel, a 35-year veteran of the company and CEO since 2008, has agreed to step down, effective immediately. He also resigned from the board of directors. A company spokesman declined to give specifics on when the decision was reached. The departure suggests the company is trying to start with a clean slate as it wrestles with the fallout from hackers' theft of credit and debit card information on tens of millions of customers. The company's sales, profit and stock price have all suffered since the breach was disclosed. Target, based in Minneapolis, said Chief Financial Officer John Mulligan has been appointed interim president and CEO. Roxanne S. Austin, a member of Target's board, has been named as interim nonexecutive chair of the board. Both will serve in those roles until permanent replacements are named. Steinhafel will serve in an advisory capacity during the transition. Jim Johnson remains lead independent director on the board. Steinhafel's tenure has been rocky. The company has struggled with its expansion into Canada, its first foray outside of the U.S. The company, known for its cheap chic clothing and home decor, also has seen uneven sales since the recession ended as it confronts fierce competition. Under Steinhafel's leadership, the company has expanded into fresh groceries and offered a 5 percent discount to customers who use its branded debit and credit cards. But clearly the breach was a big black eye on Steinhafel's term. "The last several months have tested Target in unprecedented ways," Steinhafel wrote in a letter to the board that was made available to The Associated Press. "From the beginning, I have been committed to ensuring Target emerges from the data breach a better company, more focused than ever on delivering for our guests." Steinhafel's departure comes two months after the company announced that Chief Information Officer Beth Jacob resigned and outlined a series of changes it was making to overhaul its security systems and its security department. Last week, Target named Bob DeRodes, who has 40 years of experience in information technology, as its new chief information officer. Target said it is continuing its search for a chief information security officer and a chief compliance officer. Target also said last week that MasterCard Inc. will provide branded credit and debit cards with a more secure chip-and-PIN technology next year. That will make Target the first major U.S. retailer that will have store cards with this technology. Steinhafel has been facing increasing pressure since it was revealed on Dec. 19 that a data breach compromised 40 million credit and debit card accounts between Nov. 27 and Dec. 15. Then on Jan. 10, the company said hackers also stole personal information — including names, phone numbers as well as email and mailing addresses — from as many as 70 million customers. The company's board has been meeting with Steinhafel monthly instead of quarterly to oversee Target's response to the breach. When the final tally is in, Target's breach may eclipse the biggest known data breach at a retailer, one disclosed in 2007 at the parent company of TJ Maxx that affected 90 million records. Target reported in February that its fourth-quarter profit fell 46 percent on a revenue decline of 5.3 percent as the breach scared off customers. Target's sales have been recovering as more time passes, but it expects business to be muted for some time: It issued a profit outlook for the current quarter and full year that missed Wall Street estimates because it faces hefty costs related to the breach. To read more click **HERE**

Department of Defense to study bitcoin as possible terrorist threat

FoxNews, 5 May 2014: A division within the Department of Defense is investigating whether the digital currency bitcoin is a possible terrorist threat. The Combatting Terrorism Technical Support Office is spearheading a program that will help the military understand how modern technologies could pose threats to national security, including bitcoin and other virtual currencies, the International Business Times reported. A memo detailing some of the CTTSO projects states, “The introduction of virtual currency will likely shape threat finance by increasing the opaqueness, transactional velocity, and overall efficiencies of terrorist attacks,” as reported by Bitcoin Magazine, according to IBTimes. One of the greatest concerns reportedly rests with the anonymity afforded bitcoin transactions. The transactions are public, but the people involved in the operations are unnamed. Bitcoins, according to the business site, can allow illegal operations with the speed of the Internet, but with the secrecy of a cash deal. Some high-profile cases have highlighted bitcoin’s

vulnerability, including Silk Road, the digital black market shut down in October by the FBI. Silk Road accepted only bitcoin for payments. The site's founder was charged with drug trafficking and money laundering. A Treasury Department probe found no evidence of bitcoin being used to finance terrorism, but the anonymous nature of the transactions still has many law enforcement officials worried. CTTSO is concerned that anonymous networks are a way to successfully traffic drugs, weapons, people and nuclear tech under the radar. Android, Motorola, social media and virtual reality were also included on the CTTSO's list of topics worth researching regarding terrorism. To read more click **HERE**

Facebook, Google users threatened by new security flaw

Fox News, 5 May 2014: A serious flaw in two widely used security standards could give anyone access to your account information at Google, Microsoft, Facebook, Twitter and many other online services. The flaw, dubbed "Covert Redirect" by its discoverer, exists in two open-source session-authorization protocols, OAuth 2.0 and OpenID. Both standards are employed across the Internet to let users log into websites using their credentials from other sites, such as by logging into a Web forum using a Facebook or Twitter username and password instead of creating a new account just for that forum. Attackers could exploit the flaw to disguise and launch phishing attempts from legitimate websites, said the flaw's finder, Ph.D. student Wang Jing of the Nanyang Technological University in Singapore. Wang believes it's unlikely that this flaw will be patched any time soon. He says neither the authentication companies (those with which users have an account, such as Google, Microsoft, Facebook, Twitter or LinkedIn, among others) nor the client companies are taking responsibility for fixing the issue. "The vulnerability is usually due to the existing weakness in the third-party websites," Wang writes on his own blog. "However, they have little incentive to fix the problem." The biggest danger of Covert Redirect is that it could be used to conduct phishing attacks, in which cybercriminals seize login credentials, by using email messages containing links to malicious websites disguised as something their targets might want to visit. Normal phishing attempts can be easy to spot, because the malicious page's URL will usually be off by a couple of letters from that of the real site. The difference with Covert Redirect is that an attacker could use the real website instead by corrupting the site with a malicious login popup dialogue box. For example, say you regularly visit a given forum (the client company), to which you log in using your credentials from Facebook (the authentication company). Facebook uses OAuth 2.0 to authenticate logins, so an attacker could put a corrupted Facebook login popup box on this forum. If you sign in using that popup box, your Facebook data will be released to the attacker, not to the forum. This means the attacker could possibly gain access to your Facebook account, which he or she could use to spread more socially engineered attacks to your Facebook friends. Covert Redirect could also be used in redirection attacks, which is when a link takes you to a different page than the one expected. Wang told CNET authentication companies should create whitelists — pre-approved lists that block any not on it — of the client companies that are allowed to use OAuth and OpenID to redirect to them. But he said he had contacted a number of these authentication companies, who all shifted blame elsewhere. Wang told CNET Facebook had told him it "understood the risks associated with OAuth 2.0" but that fixing the flaw would be "something that can't be accomplished in the short term." Google and LinkedIn allegedly told Wang they were looking into the issue, while Microsoft said the issue did not exist on its own sites. Covert Redirect appears to exist in the implementations of the OpenID and OAuth standards used on client websites and apps. But because these two standards are open-source and were developed by a group of volunteers, there's no company or dedicated team that could devote itself to fixing the issue. Where does that leave things? "Given the trust users put in Facebook and other major OAuth providers, I think it will be easy for attackers to trick people into giving some access to their personal information stored on those service," Chris Wysopal, chief technology officer of Boston-area security firm Veracode and a member of the legendary 1990s hackerspace the L0pht, told CNET. "It's not easy to fix, and any effective remedies would negatively impact the user experience," Jeremiah Grossman, founder of Santa Clara, Calif.-based WhiteHat Security, told CNET. "Just another example that Web security is fundamentally broken and the powers that be have little incentive to address the inherent flaws." Users should be extra-wary of login popups on Web pages. If you wish to log into a given website, it might be better to use an account specific to that website instead of logging in

with Facebook, Twitter, or another authentication company, which would require the use of OAuth and/or OpenID to do. To read more click **HERE**

Android "Police Locker" ransomware set to attack

Heise Security, 5 May 2014: Android users might soon become victims of "Police Locker" ransomware, if they haven't already, warns the researcher behind the Malware don't need Coffee blog. "The 'Reveton team' has diversified its locking activity," he informs us. "The advert is old (2014-02-18) but i decided to write about it today as I found a Traffic Distribution System (TDS) using almost all features proposed by this affiliate including the Android locker." Other options for malware delivery include system lockers, fake AV, fake codecs, and Browlock ransomware. The researcher discovered a threat actor that uses a TDS that employs almost all features: if you land on a malicious site using Internet Explorer, a variant of the Winlock ransomware is served. If you land with with another browser on Windows, Linux or Mac, you'll get Brownlock. Finally, if you land on it with Android, you will be redirected to a fake adult website that will automatically push the download of a malicious APK file masquerading as a video downloader app (and using the icon of the legitimate BaDoink Video Downloader). The good news is that the user must approve the installation. Another good news is that the malware is already detected by a dozen of AV solutions. The malicious APK can call APIs that provide access to information about the telephony services on the device, in order to determine telephony services and states. Once the malicious app is run or once the device is rebooted, this allows it to show a fake message saying that the device has been blocked and encrypted by the local police (with the apparent help of Mandiant - see the upper left corner of the fake notice). The fine US users are asked to pay in order to get their phones unlocked is $300, payable via Money Pak. Users from other countries (most European countries, Mexico, New Zealand, Canada, Australia, etc.) will see the message in their own language, purportedly shown by their own country's police force. "The locker is kind of effective. You can go on your homescreen but nothing else seems to work," the researcher notes. "Launching Browser, callings Apps, or 'list of active task' will bring the Locker back." The malware is detected by most AV solutions as Trojan Koler, and the researcher has already spotted another threat actor delivering it. In this case, the malicious APK masquerades as the popular BSPlayer video player for Android. To read more click **HERE**