The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

17 March 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

March 13, Reuters – (National) **Target says it declined to act on early alert of cyber breach.** Target Corp. stated March 13 that security software detected potentially malicious activity that led to the breach of 40 million payment card records and 70 million customer records but that its staff decided not to take immediate action. The company stated that it is investigating past practices to improve security. Source: http://www.reuters.com/article/2014/03/13/us-target-breach-idUSBREA2C14F20140313

March 13, Detroit News – (Michigan) **Harper University Hospital patient records stolen.** The Detroit Medical Center announced March 13 that the personal information of 1,087 Harper University Hospital patients was stolen after being informed of a security breach by the West Bloomfield Police Department. Personal documents were discovered in the possession of a former employee during an identity theft investigation. Source: http://www.detroitnews.com/article/20140313/BIZ/303130113/Harper-University-Hospital-patient-records-stolen

March 12, University of California, San Francisco – (California) **Computer theft at UC San Francisco.** The University of California, San Francisco (UCSF) notified 9,986 individuals March 12 of a January burglary involving unencrypted desktop computers from the UCSF Family Medicine Center at Lakeshore. Authorities are investigating the theft of the computers which contained personal information including Social Security numbers. Source: https://www.ucsf.edu/news/2014/03/112556/computer-theft-uc-san-francisco

March 14, Help Net Security – (International) **Pwn2Own 2014 ends, $850k distributed to successful hackers.** The second day of the Pwn2Own 2014 security competition March 14 resulted in two vulnerabilities in Chrome being discovered, in addition to vulnerabilities in Internet Explorer, Firefox, Safari, and Adobe Flash that were revealed March 13. A total of $850,000 was awarded to security researchers over the course of the competition. Source: http://www.net-security.org/secworld.php?id=16524

March 13, IDG News Service – (International) **Phishing campaign targets Google Docs, Drive users.** Symantec researchers identified a phishing campaign targeting users of Google Drive that uses a fake login page hosted on Google servers and served over Secure Sockets Layer (SSL), making the campaign potentially more convincing than most phishing attempts. Source:http://www.computerworld.com/s/article/9246950/Phishing_campaign_targets_Google_Docs_Drive_users

March 13, IDG News Service – (International) **Adobe patches a critical flaw in Shockwave Player.** Adobe released a patch March 13 for its Shockwave Player to address a critical memory corruption vulnerability that could lead to arbitrary code execution. Source:http://www.computerworld.com/s/article/9246930/Adobe_patches_a_critical_flaw_in_Shockwave_Player

Iran says sabotage prevented at nuclear facility

AP, 15 Mar 2014: Iranian authorities have prevented attempted sabotage at the country's heavy water nuclear reactor, a senior official said Saturday without giving specifics as to the nature of the attempted disruption or its suspected initiator. Asghar Zarean, who heads security at the Atomic Energy Organization of Iran, said domestic intelligence agencies were instrumental in uncovering the plot, which has not been the first attempt to disrupt the contentious nuclear program. "Several cases of industrial sabotage have been neutralized in the past few months before achieving the intended damage, including sabotage at a part of the IR-40 facility at Arak," he said in a statement issued by his organization Saturday. In the past, computer viruses have attacked Iranian nuclear facilities. While Zarean did not say whether that was the case this time, his comments coincided with the opening of a specialized lab Tehran says will fight industrial sabotage and neutralize cyberattacks. "This specialized lab has been launched to identify, prevent and fight threats including modern software viruses," Zarean said. In 2010, the so-called Stuxnet virus temporarily disrupted operation of thousands of centrifuges, key components in nuclear fuel production, at Iran's Natanz uranium enrichment facility. Iran says it and other computer virus attacks are part of a concerted effort by Israel, the U.S. and their allies to undermine its nuclear program through covert operations. Some Iranian officials have also suggested in the past that specific European companies may have sold faulty equipment to Iran with the knowledge of American intelligence agencies and their own governments, since the sales would have harmed, rather than helped, the country's nuclear program. Since then, Iran has also said that it discovered tiny timed explosives planted on centrifuges but disabled them before they could go off. Authorities now claim the Islamic Republic is immune to cyberattacks. The country has also reported computer virus attacks on its oil facilities, including one in 2012 that disabled Internet connections between the Oil Ministry, oil rigs and a major export facility. To read more click **HERE**

NATO websites hit in cyber-attack linked to Crimea tension

Reuters, 16 Mar 2014 - Hackers brought down several public NATO websites, the alliance said on Sunday, in what appeared to be the latest escalation in cyberspace over growing tensions over Crimea. The Western military alliance's spokeswoman, Oana Lungescu, said on social networking site Twitter that cyber-attacks, which began on Saturday evening, continued on Sunday, although most services had now been restored. "It doesn't impede our ability to command and control our forces. At no time was there any risk to our classified networks," another NATO official said. NATO's main public website (www.nato.int), which carried a statement by Secretary-General Anders Fogh Rasmussen saying that Sunday's referendum on Crimea's status would violate international law and lack legitimacy, worked intermittently. The so-called "distributed denial of service" (DDoS) attack, in which hackers bombard websites with requests causing them to slow down or crash, also hit the site of a NATO-affiliated cyber security center in Estonia. NATO's unclassified e-mail network was also affected. A group calling itself "cyber berkut" said the attack had been carried out by patriotic Ukrainians angry over what they saw as NATO interference in their country. The claim, made at www.cyber-berkut.org, could not be independently verified. "Berkut" is a reference to the feared and since disbanded riot squads used by the government of ousted pro-Russian Ukrainian President Viktor Yanukovich. Cyber warfare expert Jeffrey Carr, in a blog on the attacks, described cyber berkut as staunch supporters of Yanukovich and a "pro-Russia hacktivist group working against Ukrainian independence". Lungescu noted the statement by "a group of hacktivists" but said that, due to the complexities involved in attributing the attacks, NATO would not speculate about who was responsible or their motives. John Bumgarner, chief technology officer at the U.S. Cyber Consequences Unit, a non-profit research institute, said initial evidence strongly suggested that these cyber-attacks were launched by pro-Russian sympathizers. "One could equate these cyber-attacks against NATO as kicking sand into one's face," he said. Cyber-attacks on NATO's computer systems are common, but a NATO official, speaking on condition of anonymity on Sunday, said this was a serious online assault. Ian West, director of NATO's cyber defense nerve center at Mons in southern Belgium, said last year that the alliance's network intrusion detection systems handled around 147 million "suspicious events" every day and around 2,500 confirmed serious attacks on its computers in the previous year. Occupied by Russian forces for two weeks, the largely Russian-speaking Crimea holds a referendum on seceding from Ukraine to join

Russia on Sunday. NATO states have opposed the move, calling it unconstitutional and effectively an annexation of Ukraine's sovereign territory. Tensions between Moscow and the West have been rising steadily since Russia intervened following the ouster of Yanukovich. Ukrainian and Russian websites have both been targets for cyber-attacks in recent weeks but this appeared the first major attack on a Western website since the crisis began. Suspected Russian hackers used DDoS attacks to cripple websites and services in Estonia in 2007 during a dispute over a war memorial and against Georgia during its brief 2008 war with Russia. Moscow denied orchestrating such attacks, saying they were simply carried out by independent patriots. To read more click **HERE**

Windows XP Computers Stuck in Endless Reboot Loop After March 2014 Updates

SoftPedia, 17 Mar 2014: Microsoft rolled out this month's Patch Tuesday updates last week and although no problems have been reported at first, it turns out that some Windows XP machines are actually getting some botched fixes. A number of users who reported the issue on Microsoft's Community forums are revealing that after installing March 2014 Patch Tuesday fixes their computers are stuck in an endless reboot loop which doesn't allow the device to start at all. Booting in Safe Mode doesn't work either, they say, which means that they're stuck with a broken computer which cannot be used at all. "Today, when I powered on the relevant PC, it went through BIOS and XP logo screens OK, but never reached the high-res background color stage of the boot process; instead it auto-rebooted---and repeated this loop endlessly. Booting in Safe Mode made no difference," one user reported. "I was able to load XP only by telling the PC's BIOS to use my backup drive as the boot drive ... this backup drive is a clone of the normal boot drive; I re-clone it to match the primary disk about once a week." As you can see, this isn't quite the kind of resolution that comes in handy to beginners, so unless you're an experienced user, you might not be able to fix the computer. Microsoft hasn't yet released a fix and it's unclear whether this is an issue affecting a bigger number of computers because the botched updates are taking the device offline, so some of those whose devices were broken down might not be able to report the problems. Another user has reported a similar problem, again after installing the updated delivered by Microsoft on this month's Patch Tuesday. "At restart, after BIOS and XP-logo screens, I got a black screen permanently. After hitting several times <ctrl> + <alt> + <delete> keys together, then the hotkey that initiates STANDBY, then again the three keys above, I got a blue screen with the message: 'STOP: d0000144 Unknown Hard Error'" he said. After April 8 2014, no other patches and security updates would be released, which means that users who'll still run Windows XP will basically become vulnerable to attacks based on exploit trying to take advantage of the unpatched security flaws. To read more click **HERE**

AVAST: Windows XP 6 Times More Likely to Get Hacked than Windows 7

SoftPedia, 17 Mar 2014: Windows XP should move to a newer operating system in the next 20 days if they want to remain secure after end of support arrives, and new statistics provided by the security company AVAST come to reveal some of the risks taken by those who decide to stay with this particular platform. The company that makes the popular avast! Free Anti-virus said in a press release today that according to its own figures, Windows XP users are 6 times more likely to get attacked than Windows 7 users. Of course, these figures are only some estimates based on past data, but there's no doubt that an operating system still receiving updates and security patches from the parent manufacturer is a much better choice than a discontinued version. "Our telemetry data shows that XP users are 6 times more likely to get attacked than Windows 7 users and once Microsoft stops issuing patches, this can worsen," AVAST said. What's more, AVAST said, 21.5 percent of the users still on Windows XP are currently running Internet Explorer, while 45.6 percent have already made the switch to Google Chrome. Firefox is installed on 28.5 percent of computers powered by Windows XP. "In addition to Windows XP itself being a security risk, Internet Explorer on Windows XP poses an even larger threat. The latest version of the browser available on Windows XP is version 8, making it outdated and lacking a number of security improvements available in its later versions," the security company pointed out. "Of our existing Windows XP user database, 21.5% run Internet Explorer, leaving themselves open to easy attacks. Microsoft has basically the same view over Windows XP, although the software giant doesn't want users to replace Internet Explorer with Google Chrome

and stick to this platform, but migrate to Windows 8.1 completely and even upgrade their hardware configurations. That's actually one of the main problems for Windows XP users, as upgrading their computers involves pricey investments that some cannot afford right now. As a result, many might actually stick to Windows XP for a few more years, not necessarily until they have the money to move to another operating system, but also until the software giant comes up with a more appealing product than the existing Windows 8 and Windows 8.1 platform which generated so much confusion among beginners. To read more click **HERE**

Syrian Electronic Army Hacks Website of Syrian National Coalition

SoftPedia, 17 Mar 2014: The Syrian Electronic Army has breached and defaced the official website of the National Coalition for Syrian Revolutionary and Opposition Forces (etilaf.org). A number of other sites related to the organization have also been targeted. The National Coalition for Syrian Revolutionary and Opposition Forces, also known as the Syrian National Coalition, is an organization founded in November 2012 in Doha, Qatar. It's comprised of opposition groups in the Syrian civil war and it focuses on replacing the Bashar al-Assad government. Considering that the Syrian Electronic Army supports the al-Assad government, it's no surprise that the group has set sights on the National Coalition. In addition to the organization's main website, hackers have also defaced the sites of the Masarat Syria (masaratsyria.com) and the City Council of Daraya (darayacouncil.org). At the time of writing, all of the targeted websites have been taken offline. A mirror of the National Coalition site defacement is available on zone-h.org. The Syrian Electronic Army appears to be operating on a number of fronts. On one hand, they're targeting Syrian organizations that oppose the current government. On the other hand, they also conduct campaigns against foreign entities. On Saturday, the hacktivists announced successfully penetrating the systems of the US Central Command (CENTCOM). So far, the hackers have only published a screenshot to show that they've gained access to some Army Knowledge Online servers. Experts have noted that the information obtained by the SEA appears to be unclassified and CENTCOM denies that its systems have been breached. However, the group says they'll publish a lot of data that will demonstrate their claims. The hacktivists have decided to focus their efforts on CENTCOM after rumors emerged that the US was considering launching cyber operations against Syria. "SEA advises the terrorist Obama to think very hard before attempting 'cyberattacks' on Syria. We know what Obama is planning and we will soon make him understand that we can respond," the hackers noted in late February. "If his advisors think we will respond with the same kind of attacks we have been using they are mistaken. The next attack will prove that the entire US command structure was a house of cards from the start." To read more click **HERE**

Man Arrested in Connection with Morrisons Data Breach

SoftPedia, 17 Mar 2014: An employee of UK supermarket chain Morrisons has been arrested in connection with the investigation into the data breach suffered by the company last week. The suspect has not been named and his motives are still uncertain. The announcement was made a few hours ago by the West Yorkshire Police. The suspect has been arrested on suspicion of making or supplying an article for use in fraud. "An employee of Morrisons has been arrested in Leeds this morning (Monday, 17 March) in connection with an investigation into the theft of data from the company," said Detective Chief Inspector Gary Hooks, of Protective Services (Crime). "He is currently in custody." Last week, we learned that the payroll data – including names, addresses and bank account details – of as many as 100,000 employees were posted on a website. Someone also sent a copy of the data to the Bradford Telegraph & Argus newspaper. Customer information has not been compromised. The supermarket chain rushed to have the data removed, but cybercriminals had enough time to copy it. Shortly after the incident came to light, Morrisons announced that there wasn't any evidence to suggest that it was an external attack. It appears they were right. It remains to be seen what drove the man to do such a thing. Judging by the comments posted on Facebook after the incident was announced, Morrisons has a number of unhappy employees. The man believed to be behind the data theft could be one of them. The data breach came to light shortly after the supermarket chain announced suffering massive losses last year. Morrisons is working with banks and Experian to assist affected employees and make sure their personal and financial

details are not misused. The company has also set up a call line where employees can obtain clarifications about the incident. To read more click **HERE**

Google's Public DNS Hijacked for 22 Minutes

SoftPedia, 17 Mar 2014: On Sunday, BGPmon, a network monitoring and routing security company that monitors the Internet for Border Gateway Protocol (BGP) attacks, revealed that Google's public DNS service had been hijacked. The attackers hijacked the 8.8.8.8/32 DNS server for approximately 22 minutes. According to BGPmon, networks in Brazil and Venezuela were impacted. A screenshot published by the company shows that the traffic was redirected to BT Latin America's networks. BGPmon has noted that the potential for misuse in the case of such hijackings is "huge," especially since many certificate authorities don't do their job as well as they should. Google Public DNS was introduced back in December 2009 in an effort to make the web faster and more secure. Last year in March, the search engine giant made some improvements to the resolver, adding support for Domain Name System Security Extensions (DNSSEC) validation. The security feature is designed to protect users against DNS-based attacks and it makes DNS more secure overall. However, as IT News' Juha Saarinen highlights, there doesn't appear to be any mechanism in place to protect users against BGP hijacking. Around 70 million IP addresses use Google's public DNS servers for 130-150 billion queries every day. For the time being, it's uncertain who is behind the attack or how this could have happened. To read more click **HERE**

Syrian Electronic Army Targets CENTCOM, Shows It Has Access to US Army Data

SoftPedia, 15 Mar 2014: The Syrian Electronic Army claims to have breached the systems of the United States Central Command (CENTCOM). The attack appears to be in response to the US's intention to use cyber warfare against Syria. "Operation targeting CENTCOM are now in motion due to Obama's decision to attack Syria with electronic warfare," the hackers wrote on Twitter. So far, the hackers have published a screenshot to show that they've gained access to Army Knowledge Online (AKO) servers. The AKO provides enterprise information services to the Army and Department of Defense customers. It provides services on both classified and unclassified networks. The image published by the Syrian Electronic Army on Twitter shows that they've obtained information related to Department of Defense organizations, particularly Air Force operations. Representatives of CENTCOM have told The Tampa Tribune that the hackers' claims are "totally bogus." Bob Gourley, the former CTO of the Defense Intelligence Agency (DIA) and founder of Crucial Point LLC, has told The Tampa Tribune that the files shown in the screenshot published by the hacktivists appear to contain unclassified information. Gourley says that if the SEA's claims are true, they appear to have access to unclassified areas, not SIPRNet, the network used by the Department of Defense and the Department of State to transmit classified information. At this point, it would be more an embarrassment than a security concern. However, the SEA argues that the screenshot it has published is only the beginning, claiming to have successfully penetrated "many central repositories." A lot more data will be published in the upcoming days, which, according to the pro-Assad hacktivists, will demonstrate that the breach is more serious than it appears at this point. In the coming days we will update you with specific details and hundreds of documents that the #SEA has obtained. The Syrian Electronic Army revealed its intention to target CENTCOM back in late February. "SEA advises the terrorist Obama to think very hard before attempting 'cyberattacks' on Syria," the hackers wrote at the time. "We know what Obama is planning and we will soon make him understand that we can respond." The announcement came shortly after a report revealed that the US was considering using cyber tools to attack Syria. The Syrian Electronic Army doesn't usually make false claims, so they probably have access to some of the US Central Commands' servers. It remains to be seen just how deep they've gone. To read more click **HERE**

Cybercriminals Leverage Mass Stabbing in China to Distribute Gh0st RAT

SoftPedia, 14 Mar 2014: Cybercriminals are leveraging the recent incident in which tens of people were stabbed to death at a railway station in Kunming, China, to distribute a piece of malware that can help them take over infected computers. The incident occurred at the beginning of this month. A total of 33 people were reportedly stabbed to death and many others were injured. Trend Micro has spotted malicious emails carrying the subject line "Fw: Kunming train station knife attack leaves 33 dead and more than 130 injudred." The emails describe the incident by citing a number of sources. They instruct recipients to open the attachments to learn more. There are a total of five files attached to the emails – four image files and one document. The image files are harmless, but the document actually hides a Trojan that's designed to exploit an old Microsoft Office vulnerability (CVE-2012-0158) to drop a backdoor. The threat, BKDR_GHOST.LRK or better known as Gh0st RAT, is designed to enable cybercriminals to take control of the infected machine. It can also be used to capture information via keylogging, screen grabs and audio recording. Researchers have found a string in the malware's command and control (C&C) communications that's similar to one spotted in the GhostNet campaign, an old cyber espionage operation conducted by Chinese actors against Tibetan institutions. To read more click **HERE**