THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

28 August 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

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, and Sandia National Labs

August 25, Softpedia – (International) **FlashPack exploit kit shared through social media buttons add-on.** Researchers with Trend Micro observed the FlashPack exploit kit being distributed to users through social media sharing buttons on Web sites. The exploit kit attempts to exploit vulnerabilities in Adobe Flash and is mostly targeting users in Japan at present. Source: http://news.softpedia.com/news/FlashPack-Exploit-Kit-Shared-Through-Social-Media-Buttons-Add-On-456317.shtml

August 23, Softpedia – (International) **MeetMe social network systems breached.** Social network MeetMe reported that it was compromised by attackers between August 5 and August 7 who were able to obtain an unspecified number of users' encrypted user names, passwords, and email addresses. The company advised users to change their passwords as a precaution. Source: http://news.softpedia.com/news/MeetMe-Social-Network-Systems-Breached-456085.shtml

August 23, Softpedia – (International) **Backoff PoS malware impacts more than 1,000 businesses.** The U.S. Department of Homeland Security issued an advisory August 22 encouraging retailers to evaluate their payment systems to determine if their assets may be vulnerable or compromised by a recently discovered point of sale (PoS) malware dubbed BackOff which is believed to have affected over 1,000 businesses since October 2013. The malware was recently leveraged to attack United Parcel Service (UPS) systems in 51 locations across the U.S. Source: http://news.softpedia.com/news/Backoff-PoS-Malware-Impacts-More-than-1-000-Businesses-456106.shtml

August 22, WCSH 6 Portland – (Maine) **Data breach discovered at OTTO's Portland locations.** OTTO Pizza reported August 22 that about 900 of its customers were notified that the company suffered a point-of-sale attack between May 1 and August 13 at its Portland locations and hackers may have accessed some customers' payment card information. The hard drives of the affected terminals were replaced and additional firewall and monitoring software was installed after the breach was detected. Source: http://www.wcsh6.com/story/news/local/portland/2014/08/22/data-breach-discovered-at-ottos-portland-locations/14450607/

August 26, Softpedia – (International) **Backoff PoS malware has at least eight variants.** Researchers at Symantec conducted an analysis of the Backoff point-of-sale (PoS) malware and identified eight variants, with differences in registry entries and values, command and control servers, and the variants' installation paths. Source: http://news.softpedia.com/news/Backoff-PoS-Malware-Has-At-Least-Eight-Variants-456433.shtml

August 25, WGCL 46 Atlanta – (Georgia) **Crooks swipe nearly 100 laptops worth more than $200k from Atlanta school.** Police in Atlanta are searching for a group of men who broke into Brown Middle School and stole 91 desktop computers and laptops worth over $200,000 August 17. Authorities released security video August 25 showing four young men walking out with several laptops. Source: http://www.cbs46.com/story/26362906/crooks-swipe-100-laptops-from-atlanta-school

August 26, Softpedia – (International) **Hardcoded password in Netis, Netcore routers offers backdoor to devices.** Trend Micro researchers found that some routers sold under the Netis brand in the U.S. and other countries, and under the Netcore brand in China, contain a backdoor that can be accessed if the routers provide external access. The researchers also found a hardcoded password in the devices that can allow anyone with the password to access the router. Source: http://news.softpedia.com/news/Hardcoded-Password-in-Netis-Netcore-Routers-Offers-Backdoor-to-Device-456394.shtml

August 26, Threatpost – (International) **50 security flaws fixed in Google Chrome.** Google released an update for its Chrome browser, addressing 50 security issues, including a series of critical vulnerability that could be exploited to execute arbitrary code outside of the Chrome sandbox. Source: http://threatpost.com/50-security-flaws-fixed-in-google-chrome

August 25, Help Net Security – (International) **Researchers exploit flaw to tie Secret users to their secrets.** Researchers from Rhino Security Labs demonstrated a proof-of-concept attack against the Secret app that could allow a user to deduce the identity behind a posting on the anonymous social network. The attack method was previously reported to Secret and closed before the researchers' demonstration. Source: http://www.net-security.org/secworld.php?id=17291

August 26, Softpedia – (California) **Unlisted Comcast customer details exposed by the thousands.** The personal information of more than 74,000 Comcast customers in California who had paid to have their details remain unlisted, including names, addresses, and phone numbers, was exposed due to a fault in an agreement with a third party that distributes and publishes Comcast residential directories. The company stated that the leak appeared to occur between July 2010 and December 2012, and affected customers were offered refunds and in some cases additional remediation actions. Source: http://news.softpedia.com/news/Unlisted-Comcast-Customer-Details-Exposed-by-the-Thousands-456369.shtml

August 27, Dallas Morning News – (Texas) **Commissioner accuses Xerox of "reckless" misuse of Medicaid data.** The commissioner of the Texas Health and Human Services Commission stated that the agency filed a second lawsuit August 26 against Xerox Corp., for allegedly failing to protect patient confidentiality and for improperly retaining large quantities of medical records. The announcement comes several months after the State announced the first lawsuit against Xerox over allegations that the company paid out hundreds of millions of dollars for unnecessary dental work. Source: http://trailblazersblog.dallasnews.com/2014/08/janek-accuses-xerox-of-reckless-misuse-of-medicaid-data.html/

August 27, Softpedia – (International) **Updated NetTraveler backdoor has encrypted configuration file.** Researchers at Kaspersky Labs identified an updated variant of the NetTraveler (also known as Travnet or Netfile) malware being used in a spearphishing campaign that contains an encrypted configuration file. The NetTraveler malware has been used for as long as 10 years and is frequently used in attacks targeting diplomatic, government, military, and activist groups. Source: http://news.softpedia.com/news/Updated-NetTraveler-Backdoor-Has-Encrypted-Configuration-File-456602.shtml

August 27, Help Net Security – (International) **470 million sites exist for 24 hours, 22% are malicious.** Blue Coat researchers reported the results of an analysis of over 660 million unique hostnames requested by users and found that 71 percent of hostnames were sites that appeared for only 1 day, with around 22 percent found to be malicious sites used in short-lived attacks or botnet management. The largest number of 1-day sites were legitimate sites used by major online organizations. Source: http://www.net-security.org/secworld.php?id=17297

August 26, IDG News Service – (International) **HP recalls 6M laptop power cords that can pose fire hazards.** Hewlett-Packard announced a recall of over 6 million LS-15 AC power cords used with HP and Compaq branded laptops due to the potential for the power cords to overheat, melt, and pose a fire or burn hazard. The recall covers around 5.6 million units in the U.S. and 446,000 in Canada. Source: http://www.computerworld.com/article/2599124/computers-all/hp-recalls-6m-laptop-power-cords-that-can-pose-fire-hazards.html

JPMorgan 'targeted by Russian hackers'
Yahoo, 28 Aug 2014: Bloomberg said two people familiar with the probe confirmed that the Federal Bureau of Investigation was examining the case to see if it is retaliation for US sanctions against Moscow over its support of Ukraine's secessionist rebels. Bloomberg and The Wall Street Journal, which also reported the hacking case but without naming Russians as behind it, said it was not clear what damage the hackers caused or what data they may have stolen. Bloomberg said the hackers showed a high level of skill to get through layers of security in the bank's systems, "a feat several security experts said appeared far beyond the capability of ordinary criminal hackers." It said investigators, who also include the National Security Agency, are also studying whether the attack may have come from criminals in Russia or eastern Europe. They are also examining whether the online break-in is related to similar incidents involving European banks. The FBI said they were investigating the reports without confirming details at this point. "We are working with the United States Secret Service to determine the scope of recently reported cyber attacks against several American financial institutions," said spokesman J. Peter Donald in New York. "Combating cyber threats and criminals remains a top priority for the United States Government, and we are constantly working with American companies to fight cyber attacks." A JPMorgan spokeswoman did not confirm the specific case, but said in a statement that "Companies of our size unfortunately experience cyber attacks nearly every day." To read more click **HERE**

Users Still Reporting BSODs on Windows 7 Despite KB2993651 Launch
Softpedia, 28 Aug 2014: Today, Microsoft has patched the patch it rolled out earlier this month as part of the Update Tuesday cycle, but it turns out that despite this release, some users are still experiencing issues on their Windows 7 computers and getting the same BSODs as before. Posts on Microsoft's Community forums reveal that in some cases, deploying the new KB2993651 update doesn't make any difference and actually leads to the very same BSODs as before. "Can you believe this?! I installed patch KB2993651 today, allegedly fixing the problem. Yet, lo and behold, upon reboot, my Windows just hang! Totally dead (with no disk activity of any kind). Had to reset machine four times to finally get it to start again, and now I'm scared to reboot again," one user wrote. And still, there are many reports pointing out that Microsoft's new patch actually solves all issues, at least on Windows 7 PCs. The company however recommended everyone to uninstall the original patch, but a number of users claimed that doing that was actually causing more harm than good. "Do not, under any circumstances, follow their 'strong recommendation' to uninstall KB2982791. That is what is causing my problems and stopping Windows Update from running now. Note I am running Win 7 x64 SP1, which is what seems to be being impacted," another Windows 7 user posted. Microsoft however has already confirmed that there are a few issues with today's patch, but nothing that could lead to more BSODs or errors which could block the booting process. In most of the cases, KB2993651 works as expected and installs just fine on Windows 7, with no other BSODs experienced after that whatsoever. "On Win 8.1, uninstalling the old one, rebooting, installing the new one, rebooting, and then checking WU all went normally, so no WU error, fortunately. Hopefully any new WU errors as reported by some recent posts are not a widespread problem," one user said. At this point, it appears that the issue persists only on a limited number of computers, but it's not yet clear whether these problems are being caused by today's update or users aren't following Microsoft's instructions when trying to repair the problems. Keep in mind that although the removal of the original patch is not mandatory, Microsoft says that everyone should do it, especially due to compatibility problems that could in the end affect the overall stability and reliability of the operating system. To read more click **HERE**

50X Jump in Daily Average of Compromised Identities within Underground

Softpedia, 28 Aug 2014: Delving into the muck of the underground forums ran by crooks, a risk intelligence company found that the criminal activity regarding the trade of personal individual records has increased from a 13,000 daily average to a 650,000 one. The data is provided by C6 Group and has been recorded with a focus on cities in the United Kingdom, over a period of two months, when researchers observed that the cyber crooks exchanged stolen emails, passwords, addresses, bank account numbers, passport numbers and dates of birth. Cyber gangs across the world have been seen browsing the pages of the online locations that cannot be found through the regular search engines. The price of the details varies from $0.09 to $50, depending on factors like the amount of information provided and the likelihood of successfully leveraging it, which is assessed based on a given score. Darren Innes, CEO of the company, said that passwords and data relating to credit and debit cards is the most valuable on the markets they monitor. These are stolen by the crooks through phishing scams as well as intrusion into computer systems of various organizations. "Main culprits do seem to be south East Asia, Nigeria and former Soviet states, which makes catching the villain difficult," says Innes; moreover, no special computer skills are required for carrying out the crime. According to the company, C6 has a database with more than 421 million compromised identities, collected over four years, and by their information Manchester is the leader as far as the risk of having personal records compromised is concerned. Living in this city poses a 10X greater risk to have personal details stolen than if living in London. The company has launched a website that allows individuals to check if their email address has fallen into the wrong hands. The query is compared to the C6 database. C6 Group does not pay for the user emails in their collection, so it does not engage in trading with the cyber crooks. To read more click **HERE**

Malvertising Hits High-Profile Websites, Java, deviantART, TMZ, Photobucket

Softpedia, 28 Aug 2014: Between August 19 and August 22, visitors of Java.com, Deviantart.com, TMZ.com, Photobucket.com, IBTimes.com, eBay.ie, Kapaza.be and TVgids.nl were exposed to malware delivered through Angler exploit kit in advertisements from AppNexus, researchers at security firm Fox-IT say. Users with outdated versions of Java, Adobe Flash Player or Microsoft Silverlight are targeted by the aforementioned exploit tool, which "would embed an exploit initiating a download of a malicious payload." "Please note, a visitor does not need to click on the malicious advertisements in order to get infected. This all happens silently in the background as the ad is loaded by the user's browser," warn the researchers in a blog post. Fox-IT observed that Angler would drop Rerdom Trojan on the vulnerable systems; the malware is designed to download files from a malicious online location in order to compromise the computer. One of the problems with getting rid of the malicious advertisements is that the exploit is delivered selectively based on metadata from the user: geographical location, browser type, and web browsing history. For better success, advertisers engage in an automatic, real-time bidding process in order to show their ads to users that meet certain criteria. This makes the malicious ads more difficult to track. "In the case of this malvertising campaign the malicious advertisers were the highest bidders," Fox-IT says. On the same note, threat actors leveraged a method called "retargeting," used by ad-networks to rotate the ads shown to the same visitor when they access the website multiple times, thus allowing customization of the service. "The way it works is that a user with an interesting set of tracking cookies and other metadata for a certain adprovider is retargetted from the original advertisement content on the website to the modified or personalized data," say Fox-IT researchers. Among the methods that can be used for safeguarding against malvertising there is turning on the click-to-play feature in the web browser, which blocks the third-party plug-ins from running automatically. Keeping the browser plug-ins up to date, either by using specialized software that alerts when a new security update is available or by performing the update manually, is also a good way to reduce the risk of compromise through malvertising. Additional advice includes turning off unnecessary plug-ins, as well as employing ad-blocking applications, which can stop redirects. To read more click **HERE**

Lost Hard Drive Exposes Organized Crime Details, UK Ministry of Justice Fined

Softpedia, 27 Aug 2014: The Ministry of Justice in the UK has received a $298,500 penalty over the loss of an unencrypted hard drive that contained confidential information on organized crime connected to 2,935 convicts at the Erlestoke prison in Wiltshire, in 2013. The Information Commissioner's Office (ICO) made this decision as a result of similar incidents occurring in the past, one example being the loss of a data storage unit with unencrypted data on it, containing details of 16,000 prisoners from HMP High Down prison in Surrey. In the most recent case, the details exposed included sensitive and confidential details about organized crime, as well as health information, history of drug misuse, and material about victims and visitors. It appears that the risk of exposure is given by the fact that the data was not encrypted, although this is a standard security measure for the storage hardware in the prison system in the UK. This was not due to laziness, but to lack of technical knowledge, as "the ICO's investigation into the latest incident found that the prison service didn't realise that the encryption option on the new hard drives needed to be turned on to work correctly," says the communication from UK's privacy watchdog. The sensitive details were handled this way for more than a year in prisons across England and Wales. Encrypting the information on the storage units would guarantee that no details are exposed to unauthorized individuals; in many cases, the data they store is much more important than the device itself. "If the hard drives in both of these cases had been encrypted, the information would have remained secure despite their loss," said the release. In regards to the incident, ICO head of enforcement, Stephen Eckersley said, "The fact that a government department with security oversight for prisons can supply equipment to 75 prisons throughout England and Wales without properly understanding, let alone telling them, how to use it." "The result was that highly sensitive information about prisoners and vulnerable members of the public, including victims, was insecurely handled for over a year. This failure to provide clear oversight was only addressed when a further serious breach occurred and the devices were finally setup correctly," he added. The monetary penalty served to the Ministry of Justice has to be paid by September 22, 2014, and will flow into the Consolidated Fund, which is the Government's general bank account at the Bank of England. The ministry has the possibility to pay 20% less, $239,000, if the money is delivered by September 19. To read more click **HERE**

220 Million Personal Records Stolen in South Korea in Massive Data Breach

Softpedia, 27 Aug 2014: Details about a massive data breach in South Korea revealed that information on 27 million individuals, which make about 72% of the entire country, has been compromised. The police arrested 16 individuals, who are suspected of trading 220 million records containing personally identifiable information on people aged 15-65. It appears that the data was collected from website registrations for online games and other types of online services. "Online gaming is a huge industry and pastime in South Korea. The country treats its professional gamers like rock stars, on the same level as professional athletes. In turn, some of the best gamers in the world are from South Korea. So it's not a big surprise when one of the biggest attacks against the population is part due to - and a main target of - the attackers," said via email Adam Kujawa, head of malware intelligence at Malwarebytes. The info included in the massive database contains names, account names and passwords, and resident registration numbers. One of the arrested individuals, identified as "Kim," is believed to have obtained the details from a Chinese hacker, during a gaming session, back in 2011. It seems that the crooks would steal in-game currency and tradable game items that can be sold to other gamers. A report from Korea Joongang Daily says the police suspects that Kim used an automatic tool, known as "extractor," to log into users' accounts and commit the digital crimes. After contacting the police, the same publication found out that Kim made about 400 million won ($392,000 / €297,000) by hacking into six major games in Korea, splitting the profit with the Chinese hacker, who received about 130 million won ($127,500 / €96,600). The total damage, however, apparently amounts to 2 billion won ($1.962 / €1.486 million). Kim is also suspected of selling the personal information he obtained to other entities activating in the same fraudulent business; it is unclear if the buyers were from South Korea or from other countries. Despite the large figures for the affected individuals and the profit raked in from the fraud, this is not the largest data leak in South Korea. In 2011, Chinese hackers were accused of stealing information from 35 million

accounts for the social networking service Cyworld, under the umbrella of SK Communications, a major provider of Internet in the country. "This announcement of yet another major breach affecting a huge percentage of the South Korean populace demonstrates both the widespread use of the Internet by virtually an entire population and the impact of accessible vulnerabilities on providers of online services to that population. "In other words, almost everyone uses the Internet and is then vulnerable to an attack they can't prevent. Only the service providers can prevent them. And that prevention requires being able to get your head around an extremely complex system of networks and servers to understand what is possible, what has happened, and how to prevent anything that could cause a breach," Steve Hultquist, an executive at RedSeal said via email. To read more click **HERE**

Cedars-Sinai Health System Announces Patients of Potential Data Loss

Softpedia, 27 Aug 2014: Personal information of patients of Cedars-Sinai Health System may have fallen in the hands of unauthorized individuals after a laptop was stolen from the home of one of its employees, on June 23. The computer was used for troubleshooting software used for clinical laboratory reporting, and it may have contained information about patients. The organization points out that access to the data on the device was protected with a password, but the security protocol was broken because the storage was not encrypted. As soon as the incident became known, the employee announced Cedars-Sinai and the local police of the theft. An investigation was initiated by the medical center, which hired a team of computer forensics experts to determine what files were present on the stolen device. Starting this week, all the individuals affected by the incident will be notified by Cedars-Sinai. The details that could have been exposed are a combination of medical record number, patient identification number, lab testing information, treatment details and diagnostic data. It appears that some of the records contained the patient's social security number, as well as other personal information. "Cedars-Sinai takes the security of our patients' health information very seriously, and has multiple security safeguards in place to protect health information," said David Blake, Cedars-Sinai's chief privacy officer. "Even a potential data security incident on a single computer, as has occurred here, is not acceptable to us. We apologize to the people affected by this incident, and have taken actions to prevent any re-occurrence," he added in an official communication. To read more click **HERE**

Key Israeli Websites Hacked by Anonymous

Softpedia, 27 Aug 2014: Hackers operating under the banners of Anonymous have taken offline important Israeli government websites as a reaction to the alleged shutdown of various social media accounts of the group. The list of websites affected by the attack includes those of Israel Defense Forces, the Bank of Israel and the Israeli Prime Minister. The attackers made the list public on the anonymous publishing platform Pastebin. Some of the online services are still down, including the one for the Israel Defense Forces (idf.gov.il). The actions of the hackers are meant to show their solidarity with the people of Gaza and to try to stop Israel from attacking the region. In the Pastebin post, published on August 24 under the alias AntiSec, the hackers say that even if one individual is stopped, others would continue the work. "You never know what results will come from your action. But if you do nothing, there will be no result," the message adds. IDF's online presence has been affected numerous times, and not only the official website has been taken down, but their Twitter account was also hijacked back in July by the Syrian Electronic Army hacker group; they published a warning about a fake nuclear leak after rockets hit the Dimona nuclear plant. To read more click **HERE**