THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

18 June 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

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

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

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings. Credit is given to the NMCIWG for the compilation of this open source data

June 17, Softpedia – (International) **Evernote's forum server has been hacked.** Evernote advised certain users to change their passwords for the company's forum after attackers were able to access the forum server, potentially exposing hashed passwords as well as email addresses and birthdays if users provided them. Those affected are users with forum accounts created in 2011 or earlier. Source: http://news.softpedia.com/news/Evernote-s-Forum-Server-Has-Been-Hacked-447035.shtml

June 16, SC Magazine – (International) **Technology sites "riskier" than illegal sites in 2013, according to Symantec data.** Symantec researchers released a post based on Norton Web Safe user data that found that technology Web sites were the riskiest category of site to visit in 2013 based on the amount of malware and fake antivirus attempts utilizing that category of sites to attempt to infect users. Source: http://www.scmagazine.com/technology-sites-riskier-than-illegal-sites-in-2013-according-to-symantec-data/article/355982/

June 16, Softpedia – (International) **Internet Explorer script engine susceptible to attacks.** A researcher with Fortinet reported that the script engine in Microsoft Internet Explorer is potentially vulnerable to attacks via changing a security flag in Jscript or VBScript. Such attacks would require a target machine with escalated privileges. Source: http://news.softpedia.com/news/Internet-Explorer-Script-Engine-Susceptible-to-Attacks-447003.shtml

Windows 8.1 Update Still Impossible to Install on Some PCs, Error Code 8007005
Now Reported SoftPedia, 18 Jun 2014: Windows 8.1 Update is now mandatory for everyone running Windows 8.1, so in case you didn't install it already, your computer is not eligible for more updates and security patches released by Microsoft. But even though Microsoft made it a compulsory update, some users are still struggling to install it due to some errors experienced when starting the deploying process. These issues have been experienced by many more users after April 8, but Microsoft promised to address them until it officially makes Windows 8.1 Update mandatory for everyone. The deadline was reached on June 10, so despite this important milestone, some computers cannot be updated to this new OS version due to reasons that have nothing to do with users. "In the latest suite of Windows updates I was having repeated problems with them failing to install after 'restart'. I finally resorted to selecting and installing 1 at at time and they have now installed except for what appears to be the problem file the KB2800095 file. I have tried over a dozen times and every time encounter the same issue... failure to configure on reboot," one of the users that are still trying to fix the errors said. Microsoft initially announced a May 13 deadline for installing Windows 8.1 Update, but due to the plethora of errors experienced by users, the company decided to push it to June 10. The company did confirm that some Windows 8.1 consumers were experiencing issues when trying to deploy Windows 8.1 Update, but stated that everyone was supposed to complete the upgrade thanks to the 30-day extension. "While we believe the majority of people have received the update, we recognize that not all have. Having our customers running their devices with the latest updates is super important to us. And we're committed to helping ensure their safety. As a result, we've decided to extend the requirement for our consumer customers to update their devices to the Windows 8.1 Update in order to receive security updates another 30 days to June 10th," it said in mid-May. At this point,

Windows 8.1 computers that aren't yet running 8.1 Update cannot receive any other updates and the only patch they can get is the KB2800095 file that actually upgrades their systems. Once this is successfully installed on their computers, Windows Update would also display some other patches, thus helping them keep their systems fully up-to-date and secure. To read more click **HERE**

Linux Kernel 3.14 Breaks Wine for 16-bit Windows Applications

SoftPedia, 18 Jun 2014: Linux kernel 3.14 is one of the latest versions available, but it looks like this particular build has managed to break Wine for all the applications that were running in Windows 9x mode. Linux users need Wine to run applications from the Windows platform, but the bulk of apps accessed in this way is actually quite old. Sure enough, it's possible to run newer software as well, but most users need Wine for much older stuff. One of the latest updates for Linux kernel 3.14.x brought some modifications and users found out that they couldn't run Wine configured as Windows 9x, which is actually an important option. "Recently a security issue was fixed on Linux 3.14 kernel for x86_64 (and is being backported to previous versions as well). The security fix unfortunately caused win16 software to stop working, but 32 bit software is supposed to not be affected. The problem is configuring Wine as Windows 9x causes this error to appear even when trying to run 32 bit Windows applications: if you use a kernel with this security flaw fixed and configure Wine in Windows 9x mode, nothing works anymore, not even winecfg," reads just one of the bug reports for the Wine project. This is actually an upstream problem from the Linux kernel, and the Wine developers can't really do much about it. In fact, Linus Torvalds and the leader of the Wine project are taking about this issue, and a solution might be found eventually. "Are there people actually using 16-bit old windows programs under wine? That's what matters," said Linus Torvalds. The response from Alexandre Julliard was pretty straightforward. "Yes, there is still a significant number of users, and we still regularly get bug reports about specific 16-bit apps. It would be really nice if we could continue to support them on x86-64, particularly since Microsoft doesn't." So far, the problem seems to be contained within Linux Kernel 3.14, which means that only a small number of people have been affected, but it's possible that the change might be backported to older versions of the kernel and more Wine users will be unable to run 16-bit applications. Alexandre Julliard made a very good point about the usefulness of Wine. Microsoft is no longer supporting 16-bit applications that were released for its Windows operating system, but Linux users can run them without any major problems. To read more click **HERE**

Avast Releases Simplocker Removal Tool

SoftPedia, 18 Jun 2014: Avast announced today the availability of Ransomware Removal, an app designed to clean Android devices of Simplocker Trojan, as well as to unlock files affected by the threat. The tool is available for free on Google Play, where the description says that it can remove Cryptolocker/Simplocker threats from the device and decrypt the data encrypted for ransom demands. Detected at the beginning of the month by ESET security firm, Simplocker is a Trojan that runs an AES encryption routine on the affected device, targeting images, video files and documents (JPG, PNG, BMP, GIF, PDF, DOC, DOCX, TXT, AVI, MKV, 3GP, MP4). It can also collect information from the device, which consists of IMEI number, device model, manufacturer of the product/hardware and the version of the operating system, and send it to a remote server. Researchers at Kaspersky Lab discovered a variant of the threat that can take a picture of the victim via the phone's built-in camera and display it in the ransom message. Avast Chief Operating Officer, Ondrej Vlcek, says that, "Simplocker blocks access to files stored on mobile devices. Without our free ransomware-removal tool, infected users have to pay $21 [€15.5] to regain access to their personal files." "Even though we are seeing exponential growth in ransomware on mobile devices, most of the threats to encrypt personal files are fakes. Simplocker is the first ransomware that actually encrypts these files, so we developed a free tool for people to restore them," he adds. Another solution for retrieving files encrypted by Simplocker has been presented by an undergraduate student at the University of Sussex, United Kingdom, by the name of Simon Bell. After reverse-engineering the threat, he found the encryption and decryption method used by the malware, along with the password that protected the operation. The student then built a Java program capable of unlocking the

hostage data. However, the program is not addressed to the regular user because it needs to be packaged as an Android app, a task that requires a special set of tools. According to a press release sent to us by Avast, "Anybody infected by Simplocker or any other type of ransomware can download the free avast! Ransomware Removal tool." Installation of the app on the affected Android can be initiated from any device with an Internet connection, by accessing Google Play Store. After launching the removal tool a scan is started, followed by the elimination of the virus and decryption of the locked files. To read more click HERE

Alleged "NullCrew" Hacker Arrested by the FBI

SoftPedia, 18 Jun 2014: FBI arrested 20-year-old Timothy Justin French from Tennessee on charges of computer hacking. He is believed to be associated with the NullCrew hacking group. The group of hackers is best known for penetrating the systems of the World Health Organization and releasing hundreds of usernames and passwords in plain text, but also for breaching systems managed by the US Department of Homeland Security (DHS). According to the DoJ, Timothy Justin French is also known as "Orbit," "@Orbit," "@Orbit_g1rl," "crysis," "rootcrysis," and "c0rps3," and the complaint charges him with involvement in five hacking attacks conducted by NullCrew in 2013 and 2014 against two universities and three companies. As a result of the hacks, thousands of usernames and passwords were exposed on publicly accessible channels, Pastebin in this case. It appears that the FBI were able to arrest French thanks to a confidential witness that approached various NullCrew members on Skype, Twitter, and CryptoCat messaging services, which provide client-side encryption. After establishing contact with the members of the group and gaining their trust, the witness engaged them in conversations about "past, present, and future computer hacks, shared current computer vulnerabilities and planned target, and discussed releases of their victims' information." "Hackers who think they can anonymously steal private business and personal information from computer systems should be aware that we are determined to find them, to prosecute pernicious online activity, and to protect cyber victims," said Zachary Fardon, United States Attorney for the Northern District of Illinois. Based on the details obtained by the witness, the FBI were able to determine the involvement of computer user "Orbit" in all of the aforementioned attacks. Furthermore, the records from the targeted computers showed they were accessed by a system with the same IP address as the one assigned to French's home. "Cyber crime sometimes involves new-age technology but age-old criminal activity ? unlawful intrusion, theft of confidential information, and financial harm to victims," Fardon added. The maximum sentence faced by Timothy French in this case is 10 years in prison and a $250,000/184,310 EUR fine. The FBI seems to have arrested the right person, as NullCrew recently made an announcement on Pastebin saying that French had been warned that authorities would issue a subpoena for Skype to release details about the conversation between him and the informant. The announcement mentions another arrest, of a member called Dominik who was acting under the handles "thebinkyp", "zer0pwn", "phlex", "nop_nc", "docofcocks" and "theindigator." An arrest of an underage offender, also believed to be part of NullCrew, was made on Friday in Quebec, Canada, for a hacking incident recorded in February 2014 against Bell telecommunications company. This coincides with DoJ's statement, which mentions that French was involved in an attack on "a large Canadian telecommunications company," conducted on February 1, 2014. Both French and Dominik are called "skids" in the Pastebin message, an abbreviation for "script kiddie," a term generally used for someone who is not skilled in deploying computer attacks and relies on ready-made tools. To read more click HERE

Anonymous Launches #OpWorldCup

Softpedia, 17 Jun 2014: Hacktivist group Anonymous has kicked off a set of cyber attacks targeting various government organizations in Brazil, as a form of protest against hosting the 2014 World Cup event in detriment of taking care of their own citizens. Until now, the operation dubbed #OpWorldCup has already made some victims, as the systems of Globo TV Brasil, of the Brazilian government, Cemig Telecommunications and the Regional Electoral Court of the Amazon have been breached and data has been exfiltrated. Data is available on several online clipboard services, Pastebin being among them. In the file dump text for Globo TV Brasil, a message seems to inform that the data has been obtained via

social engineering tactics and consists of IP addresses and over 150 names and email addresses. The original text in Portuguese reads: "Apenas uma engenharia social que fizemos no site da globo onde obtem informações dos possiveis funcionarios que se responsavéis pelo site www.globo.com, essas informações obtem Ip, Endereços, Emails entre outros ... Não é uma coisa que vocês esperariam mas é um bom adianto!" Information pulled from the systems of other organizations seems to also have been retrieved and, apart from names and email addresses, it consists of hashed passwords and telephone numbers. According to a more recent post on Pastebin, the group announced that these breaches have been just "a small demonstration" of the leaks they managed in 4 days. The post also makes available some information that has apparently been stolen. The group says that they took 450 email addresses and passwords of employees of the Brazilian government, 3,4000 emails, full names and telephone numbers from Eletronorte (Centrais Elétricas do Norte do Brasil S.A), a subsidiary of the Brazilian power utility Eletrobrás. Furthermore, a picture of the administration panel of the police portal is included in the Pastebin post. One of the most recent breaches has been announced today on Twitter under the @OpGreenRights, informing that the website for the Ministry of the Environment has also been targeted, and at the moment of writing, the website appears to be down. A full dump of the data extracted has been made public and contains login details, email passwords and phone numbers. Not all the details stolen by the hacktivist group are currently publicly available, as in some cases the information has been taken down. The group does not plan to stop the attacks until the 2014 World Cup competition reaches an end and the activity may increase in intensity and complexity. In a statement made last week, Anonymous said that their actions were meant to persuade the Government of Brazil to "put an immediate end to corruption and stop the use of force and violence against peaceful demonstrators. We cannot stand idly while these injustices are being done. Know that we stand together and united to fight against this oppression." To read more click **HERE**

State-Sponsored Attackers Gained Access to UK Government Intranet

SoftPedia, 17 Jun 2014: UK Government's secure network was breached not too long ago, when hackers managed to gain access to a system administrator account. The information comes from the Minister for the Cabinet Office, Francis Maude, who shared it during the IA14 security conference. He said that the attacker was a state-sponsored hostile group, whose activity was detected and fended off at an early stage, without any damage having been caused. Admitting to a security attack attempt from another state is not something a government shares very frequently, although such activities are known to happen more often than one would think. The Minister said that efficiency of dealing with the incident was thanks to "brilliant people working to keep us safe," who were "drawn from GCHQ and the security services, the armed forces, the police and National Crime Agency, the civil service, and of course the private sector too," with "bucket loads of expertise." He also noted that the responsibility of security should not fall on their shoulders alone and everybody should be able to take the necessary precautions to protect their business and even personal privacy when browsing the Internet. Protecting passwords and sensitive information is a responsibility equally important for both a junior and the chief executive officer. To this purpose, the government launched the new Cyber Essentials Scheme on June 5, a document that covers the basics of cyber security in the corporate IT environment. The paper focuses on five key components that include prevention of unauthorized access to or from private networks through firewalls and Internet gateways, secure configuration of the systems, access control to different resources, malware protection, and applying the latest updates for the applications used. Also, starting October this year, the UK Government will request a Cyber Essentials certification to all suppliers bidding contracts aiming at handling certain personal and sensitive information. In order to protect critical businesses not just from attacks sponsored by other governments but also from criminal organizations that have equally complex hacking skills and technology, GCHQ security agency will start to gradually share classified intelligence with communications service providers. The program will include "suppliers to Government networks" and then move to "the other sectors of critical national infrastructure. This ground-breaking initiative will use GCHQ's unique capabilities and insights gleaned from its intelligence and security work to illuminate the critical threats in cyberspace." Maude concluded that technology led to new opportunities, but threats

also kept the pace and "We can't pause; we can't slow down, even for a minute. There's always something more we can be doing to protect ourselves." To read more click HERE

AT&T confirms data breach for mobile users

GSN, 17 Jun 2014: AT&T has confirmed that attackers have compromised the personal information of some mobile account holders. In a letter mailed to customers, AT&T revealed that three employees of one of its service providers managed to access personal information without authorization. The service provider unlocks cell phones for its customers upon their request. The stolen information includes Social Security numbers and call records, i.e. details about the date, time, duration and other phone number for every phone call customers make, according to AT&T. The number of users affected has not been disclosed. The data accessed during the mobile breach, which occurred from April 9-21, 2014, is believed to have been accessed to unlock phones to sell on second-hand markets. The attackers hacked the AT&T database to get unlock codes in order to disconnect stolen phones from the network and reconnect to other mobile networks. The letter to customers from Brian Woolverton, director of Consumer Centers Sales & Service, stated, "AT&T's commitments to customer privacy and data security are top priorities, and we take those commitments very seriously." The letter continued, "our service provider has notified us that these individuals no longer work for them." AT&T discovered the breach on May 19, but has just recently contacted its customers. According to California state law, businesses are required to issue a security breach notification to more than 500 California residents as a result of a single breach of a security system; they also need to electronically submit a single sample copy of that notification, excluding any personally identifiable information, to the state Attorney General. AT&T has informed the authorities. To read more click HERE

FAA orders Boeing to protect 737s from computer hackers

GCN, 16 Jun 2014: The Federal Aviation Administration (FAA) has ordered Boeing to modify technology found aboard 737 aircrafts that could be vulnerable to computer hackers. The FAA's order, which was released in the Federal Register, is effective immediately, although the agency is allowing a comment period until July 21. The order is issued for Boeing Models 737-700, -700C, -800, -900ER, -7, -8, and -9 series airplanes. These models have a unique digital system composed of several connected networks. The network configuration on these models allows increased connectivity with external networks, such as passenger entertainment and information services, which create possible vulnerabilities that can be exploited by hackers, according to the FAA. The network on these models also may be used for flight safety related control and navigation systems and operation support. Jeffrey Duven, manager of FAA's certification services, released the order calling for Boeing to "ensure that the airplanes' electronic systems are protected from access by unauthorized sources external to the plane, including those possibly caused by maintenance activity." The current applicable airworthiness regulations do not contain adequate or appropriate safety standards for the digital system design feature. The special conditions ordered to Boeing contain the additional safety standards that the FAA considers necessary to establish a level of safety equivalent to that established by the existing airworthiness standards. On January 27, 2012, Boeing had applied for an amendment to Type Certificate No.A16WE to include new models in the 737 series. Upon review of the amendment, the FAA was promoted to release the order for the modification to be made to the digital systems. According to the amendment, the newer 737 series models would be designed to reduce fuel burn and community noise. The 737 aircraft models, Boeing's best-selling jet airliner, are operated by more than 500 airlines. According to Boeing, more than 10,000 orders of the 737 series have been ordered since the program began in 1967. The 737 represents more than 25% of the worldwide fleet of large commercial jet airliners. To read more click HERE

Microsoft patches DoS flaw in its Malware Protection Engine

Heise Security, 18 Jun 2014: Microsoft has released an update for its Malware Protection Engine to fix a privately reported security vulnerability that could allow a denial of service if the Microsoft Malware

Protection Engine scans a specially crafted file. The flaw affects the engine that provides the scanning, detection, and cleaning capabilities for Microsoft antivirus and antispyware software (full list available here). "An attacker who successfully exploited this vulnerability could prevent the Microsoft Malware Protection Engine from monitoring affected systems until the specially crafted file is manually removed and the service is restarted," the company explained in the advisory. "There are many ways that an attacker could place a specially crafted file in a location that is scanned by the Microsoft Malware Protection Engine," they explained. "For example, an attacker could use a website to deliver a specially crafted file to the victim's system that is scanned when the website is viewed by the user. An attacker could also deliver a specially crafted file via an email message or in an Instant Messenger message that is scanned when the file is opened. In addition, an attacker could take advantage of websites that accept or host user-provided content, to upload a specially crafted file to a shared location that is scanned by the Malware Protection Engine running on the hosting server." "If the affected antimalware software has real-time protection turned on, the Microsoft Malware Protection Engine will scan files automatically, leading to exploitation of the vulnerability when the specially crafted file is scanned. If real-time scanning is not enabled, the attacker would need to wait until a scheduled scan occurs in order for the vulnerability to be exploited." The good news is that enterprise administrators or end users do not have to do anything about this - the default configuration in Microsoft antimalware software helps ensure that malware definitions and the engine are kept up to date automatically. To read more click **HERE**

Employees take too many risks with Wi-Fi security

Heise Security, 17 Jun 2014: UK employees are potentially putting their companies at risk of cyber-attack when using mobile devices for work purposes while on holiday or on a short break, new research has found. Cisco found that 77% of UK workers surveyed usually take their work devices with them on holiday, with 72% choosing to spend up to one or two hours per day keeping up with what's going on in the office. Over 80% of directors, mid-managers and senior level employees admitted to taking their work device on holiday, and even the most junior employees are also keen to stay connected while away with 50% unwilling to leave their work device at home. Despite 69% of the study confirming that their employer had informed them about the risks associated with using devices remotely for work purposes, 60% admitted that they did not check the security of a wi-fi network before connecting to it whilst on holiday. Trainees were the worst offenders with three quarters (75%) not checking remote networks. However directors and mid-managers were also guilty with 60% and 59% respectively, also admitting to not checking a wi-fi network's security before signing on. Reading and sending emails were the most common activities (97% and 85% respectively) followed by nearly a third (30% and predominantly director-level employees) stating that they worked on tasks associated with managing people. Other prevalent tasks included working on corporate documents (27%) and spreadsheets (17%). Sean Newman, Field Product Manager at Cisco, said: "The results of our 'Beach to Breach' study show that many workers do want get online and keep abreast of what's going on in the office, while on holiday. While employees generally do not set out to deliberately pose an IT security risk to their employer, our study shows that the majority of workers are likely to be more concerned about getting online than strictly following the IT security policy. As such, security systems have to be designed to take on board the evolving work life patterns of the modern workforce." Newman concluded: "The upshot for companies is that there is no silver bullet when it comes to IT security. In the era of increased mobility of employees, they need to ensure they have full visibility across their network in order to spot unusual activities of behaviour. Cyber criminals are well resourced and professional and recognise that employees are often a company's weakest link so target them to gain access to the corporate network. While businesses must realize that it's not a matter of if they get attacked, but when and need to focus on setting their security accordingly, employees equally have their part to play by avoiding unsecured wi-fi networks, especially for work-related tasks, and ensuring that they adhere to their companies' IT policies at all times." To read more click **HERE**