THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

20 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

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

Vietnamese Government Employees Targeted by Phishing Campaign

SoftPedia, 20 Jun 2014: Malware has been specifically crafted for the systems used by the employees at the Vietnamese Ministry of Natural Resources and Environment (MONRE). Phishing campaigns do not always have clear victims, but in this case it looks that the perpetrators are after government data and have created malicious software that can circumvent the protection on the agency's machines. The attack begins with an email with an infected Microsoft Word document in the attachment, which, once opened, drops an executable file on the computer, called "payload.exe;" this is the Trojan dropper that downloads additional executable files. Oh Sieng Chye from ESET says that the ministry relies on a webmail solution for exchanging email messages, which means that the corrupted file has to be downloaded on the computer for the infection to happen. Evidence that the attack is targeted and may be supported by organizations of a different government lies in the fact that the threat performs a scan to check for the presence of the BKAV (Bach Khoa Anti-Virus), a Vietnamese security tool. The malware contacts a remote location for receiving new files and commands, and the researchers determined that it communicates with two servers, one in the US (31.170.167.168) and one in South Korea (www.google.zzux.com). In both cases port 443 is used, which indicates that the traffic is encrypted. Sieng Chye notes that "a connection to the zzux.com domain was tried only if the IP address for the host is different from the IP address 31.170.167.168." The communication is initiated by "Framework.dll," a backdoor that delivers the local IP address of the infected machine and opens a Windows command shell that redirects the input and the output to the command and control server. If the antivirus is detected, the Trojan dropper unloads "BkavFirewallEngine.dll" from memory using the FreeLibrary functions, thus bypassing its protection. The three items added by the dropper on the system are stored in a temporary directory and, according to ESET, they are quite recent, as the date in the PE header indicates April 24, 2014. All the files downloaded on the system are currently detected by ESET products as Win32/Agent.VXU. The Ministry of Natural Resources and Environment may seem like an odd target for an attack, but it is still a government agency that can handle sensitive information. Furthermore, among the details extracted from the compromised systems there can be information that could prove useful in launching similar attacks on other structures of the government. To read more click **HERE**

BMC Vulnerability Exposes Admin Passwords in Plain Text

SoftPedia, 20 Jun 2014: Plain text passwords for remote log in to servers can be accessed from machines equipped with motherboards built by Supermicro, a company that manufactures and sells computer hardware. The security weakness, found by Zachary Wikholm, senior security engineer with the CARInet Security Incident Response Team, dwells in the BMC (baseboard management controller) component of the motherboard that allows monitoring the health of the machine by providing details on current temperatures, fan speeds, power-supply voltage, along with disk and memory performance data. BMC components are not used just for monitoring the state of the server from afar, though, and also provide remote control functionality. Supermicro released a firmware update that fixes the problem, but many systems remain vulnerable because they cannot be patched due to ensuing technical implications. According to the disclosure, "Supermicro had created the password file PSBlock in plain text and left it open to the world on port 49152." "You can quite literally download the BMC password file from any UPnP enabled Supermicro motherboard running IPMI on a public interface," adds the engineer. Using the Shodan search engine that indexes online devices and allows finding them according to given parameters, Wikholm discovered a total of 31,964 vulnerable systems. Also, it appears that a part of the countersigns retrieved are default combinations, a practice that should be avoided by all means. "This means at the point of this writing, there are 31,964 systems that have their passwords available on the open market. It gets a bit scarier when you review some of the password statistics. Out of those passwords, 3296 are the default combination. Since I'm not comfortable providing too much password information, I will just say that there exists a subset of this data that either contains or just was 'password'." Apart

from flashing the BIOS, Wikholm proposes another workaround, but it appears to be a temporary one because it functions only until the next reboot of the IPMI (Intelligent Platform Management Interface), which can be caused by disconnection from a power supply. The solution consists of connecting to the vulnerable machine through SSH and disabling UpnP (universal plug and play) devices: "Most of the systems affected by this particular issue also have their 'sh' shell accessible from the SMASH command line. If you login to the SMASH via ssh and run the command 'shell sh,' you can drop into a functional SH shell. From there you can actually kill all 'upnp' processes and their related children, which provides a functional fix." A post on the InfoSec community forum confirmed the vulnerability discovered by Wikholm, saying that downloading the password can be done by just connecting to port 49152. To read more click HERE

Linux Kernel 3.14.8 Brings New Hardware Support

SoftPedia, 20 Jun 2014: The latest version of the stable Linux kernel, 3.14.8, has been announced by Greg Kroah-Hartman, marking the release of another update in this branch. 3.14.x is no longer the newest kernel that you can get for your distribution and its place has been taken by the 3.15 branch. Even if that is the case, this is still one of the most advanced releases that you can find and it's still a very popular choice for many Linux distributions. The development for 3.14.x has been winding down now that 3.15 kernel is already out, and there are fewer changes and improvements in this latest update. It's still being maintained, but the focus has shifted to other branches. "I'm announcing the release of the 3.14.8 kernel. All users of the 3.14 kernel series must upgrade." "The updated 3.14.y git tree can be found at: git://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git linux-3.14.y and can be browsed at the normal kernel.org git web browser: http://git.kernel.org/?p=linux/kernel/git/stable/linux-stable.git;a=summary," Greg Kroah-Hartman said in the email announcement. According to the changelog, a memory leak in free_msi_irqs() has been fixed (PCI/MSI), the PCI ID for Marvell 88SE91A0 SATA Controller has been added (ahci), inode_capable has been changed to capable_wrt_inode_uidgid, the audit_krule mask accesses no longer need bounds checking, 1b80:d395 Peak DVB-T USB support has been added, and the USB ID for Genius TVGo DVB-T03 has been implemented. Also, the chipset version comments are now present in the device list, a Device ID for HighPoint RocketRaid 642L has been added, the _TIF_SECCOMP flag is now available, a multi-network portal shutdown regression has been fixed, READ_CAPACITY opcode is now allowed in the ALUA Standby access state, accepting transport connections during stop stage is now properly avoided, the ID TerraTec NOXON DAB Stick has been added, the hw ready reset flow has been fixed, some harmful wait optimizations have been dropped, and H_CSR is now read after asserting a reset. If you are using any of the versions released until now in the Linux kernel 3.14.x branch, you should consider an update to this build. It's also a good idea to try the new 3.15 kernel, which has already received an update. Linux kernel 3.14 features, among other things, better Intel Broadwell graphics support, various Radeon improvements, Nouveau improvements (support for new GPUs from NVIDIA), quite a few Btrfs changes, and even NVIDIA Tegra PRIME support. To read more click HERE

OpenSSL Vulnerability Addressed in Android 4.4.4 Update

SoftPedia, 20 Jun 2014: The latest security flaw in OpenSSL has been addressed on Android with the fresh release of the 4.4.4 KitKat (KTU84P) update, which will roll out to Nexus devices. There isn't too much information about the new build, but Engineering Program Manager at Android Sascha Prüter says that it focuses mostly on addressing the OpenSSL ChangeCipherSpec (CCS) Injection vulnerability in the crypto library, identified as CVE-2014-0224. Other security-related flaws have also been addressed, although not as severe as this one, as the changelog for KTU84P shows. The log lists CTS (Compatibility Test Suite) for the CCS flaw and a fix of a concurrency bug in OpenSSLHeartbleedTest; no reference to Towelroot. CVE-2014-0224 was revealed at the beginning of the month and would allow an attacker to force the negotiation of weak encryption keys between a client and a server by using a man-in-the-middle attack. Both systems have to be vulnerable for the exploitation to be successful. A test scan run by Qualys last week showed that almost half of the verified servers were vulnerable to this weakness and 14% of them were declared as exploitable. The current patch can be applied over Android 4.4.3 KitKat on Nexus 4, Nexus 5, Nexus 7 (2013), and Nexus 10 devices. Factory images are already available for those who do not want to wait for the OTA update. To read more click HERE

LinkedIn Info Can Be Stolen via MitM Attack, Zimperium CEO Says

SoftPedia, 20 Jun 2014: Zuk Avraham, CEO of Zimperium mobile security startup, presented a method that would allow a cybercriminal to gain full control of a LinkedIn user's account by using a man-in-the-middle attack that takes advantage of an SSL stripping technique. SSL stripping consists of the attacker interposing between the user and the service they try to access and to replace HTTPS (HTTP Secure) requests with insecure HTTP ones, allowing reading of the intercepted information in plain text. The demonstration was carried out with a mobile pentesting component developed by the company and showed that an attacker could obtain a LinkedIn user's credentials and hijack his

session. As a result of the attack, Avraham says that the information exposed consists of email address, password, messages that have been read and sent, as well as the entire list of connections. Since the criminal has full control of the account, they can carry out actions such as sending invitations, edit the user profile and job postings, or manage the company pages in case of a corporate account. During the demonstration, he discovered that every user he tested was vulnerable, if they worked with a compromised device. "With LinkedIn, the default login page is using SSL so that users' credentials (i.e., username and password) will be sent securely to the server. Once the user authentication is successful, it will redirect to http:// for the remainder of the time a user is browsing LinkedIn. This means that LinkedIn, one of the largest social networks, still has a significant portion of its website traffic that does not enforce the use of https://," said Avraham in the blog post. According to the announcements made by LinkedIn regarding the transition to HTTPS by default to all pages, the operation began in December 2013 but it is not complete; at the moment, only the traffic for users in the US and Europe is served over an encrypted connection. However, users in other regions of the world benefit from HTTPS only on the log in page and, after the authentication procedure completes, the connection switches to HTTP. They have the possibility to turn on encrypted traffic from the security settings menu of the LinkedIn account, a feature that has been available to all users since 2012. Avraham contacted LinkedIn and disclosed his findings in May 2013. The social network for professionals confirmed the vulnerability but claimed that it did not affect users with the secure connection option turned on. Although Avraham's demonstration is not exactly the disclosure of a zero-day vulnerability, the issue exposed is significant and applicable to users outside the US and Europe. To read more click **HERE**

Hundreds of Phishing Scripts Hosted on a Single Compromised Website

SoftPedia, 20 Jun 2014: Popular online dating services are targeted by phishing campaigns, as anti-phishing company finds compromised website with scripts for stealing usernames and passwords. Out of the 862 PHP malicious scripts discovered, only eight were aimed at banking credentials. Among the dating websites in the cross-hair of the cybercriminals are Match.com, Christian Mingle, PlentyOfFish, eHarmony, Chemistry.com, SeniorPeopleMeet, Zoosk, and Lavalife, says a report from Netcraft, a company that provides Internet security services, which include anti-fraud and anti-phishing. The post says that the reason behind the phishing campaign could be to commit online dating fraud, an activity that can prove to be lucrative once the criminals gain the trust of the victim. "Online dating fraud is often orchestrated by criminal gangs who use fake profiles to trick victims into developing long distance relationships. Once the fraudsters have gathered enough sympathy and trust from a victim, they will exploit this by claiming they need money to pay for travel costs, or to afford medical treatment for a family member," says Paul Mutton of Netcraft. "After the money has been stolen, the criminals will make up further reasons why they need more money. In some cases, the fraudsters blackmail their victim into sending money - if the victim has sent any explicit photos or videos to the criminals, they may threaten to send them to the victim's friends and family," Mutton added. Compromised paid accounts offer the fraudsters protection against being traced, as there is no financial transaction recorded through the website's payment service. The latest attacks detected by the company employ a phishing kit with PHP scripts; when credentials are obtained, they are sent to a number of email addresses, more than half being registered for Yahoo! Mail service. Some of the scripts have been configured to steal log-in information for webmail services, too, the email accounts being used for fraudulent purposes. The scripts in the phishing kits are similar in functionality and "simply collate a set of POST parameters into the body of an email message, and then send it to two or more email addresses. The subject of the email is modified to describe what type of credentials are in the email (e.g. 'MATCH ID & PASSWORD'), and after the emails have been sent, the victim is redirected to an appropriate URL on the target website, such as http://www.match.com/login/login.aspx?lid=2," explains Mutton. The compromised servers hosting them does not display fraudulent content but accepts information from other sources, like a form hosted on a different website and the victim is then redirected to the legitimate location, without noticing the switch. To read more click **HERE**

Microsoft fixes flaw in its own security software

Computerworld, 18 Jun 2014: Microsoft on Tuesday warned customers that its malware detection engine, used in a wide range of its products including Security Essentials and Windows Defender, could be disabled if an attacker sent a malformed file as an email attachment. Along with the security alert, Microsoft issued an update to patch the vulnerability. A successful attack would leave a Microsoft-guarded PC wide open to subsequent exploits, the company warned. "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," Microsoft said in an advisory yesterday. That engine is the foundation of the company's enterprise- and consumer-grade security products, including Windows Intune Endpoint Protection, System Center 2012 Endpoint Protection, Microsoft Security Essentials, Windows Defender and the Microsoft Malicious Software Removal Tool. The latter is a PC-cleaning tool updated monthly that seeks out and destroys selected malware. Windows Defender is the

security software packaged with Windows 8 and Windows 8.1, while the free Security Essentials has been a mainstay for many consumers and even small businesses running Windows 7. Microsoft said it had no received no reports that the vulnerability had been exploited in the wild. But the bug was serious, marked "important" -- Microsoft's second-highest threat label. It wasn't difficult to see why: If the anti-malware software was set to automatically scan every incoming file, as most are, an attacker could cripple defenses simply by attaching a specially-crafted file to an email message. Most customers, especially consumers, would have no idea that their PCs were now unguarded. The update Microsoft released at the same time it published the advisory will be automatically delivered to the malware detection engine in the next 48 hours, Microsoft said. To read more click HERE

How a Hacker Nabbed $600,000 in Two Months by Googling People's Home Networks

Business Insider, 17 Jun 2014: Sometimes a hacker does something so brilliant, we can't help but marvel at it. In this case, a hacker figured out how to control certain home networks to mine for a computer currency called Dogecoin, netting over half a million dollars in a matter of months. The hacker's exploits were documented by Dell's security team, which points out that the hacker used a competitor's computer storage product to do the dirty work. The Dell team traced the likely culprit to a German-speaking person who goes by the code name of "Folio" on GitHub. (GitHub is a cloud service where developers post and share their software projects.). Folio used a security flaw in a computer storage product called Synology, Dell says. Synology's computer storage product is easy to set up, so it has become popular with people who store a lot of songs, movies, and other multimedia files on their home networks. In 2013, a security researcher discovered a flaw with the Synology product that let a hacker find, and ultimately control, these computer storage devices by searching for them on Google. The company fixed the vulnerably and released a patch. But between the time the researcher told the world about the flaw and when the company patched it, the hacker named Folio went to work. Folio discovered vulnerable computer storage boxes and put them to work to "mine" for Dogecoin. Dogecoin is a computer currency like Bitcoin and is created by "mining," which involves getting computers to answer a series of cryptographic questions to unlock new coins. It takes a lot of computing power to answer these questions. People actually buy specially made computers to do it. Or, if you are smart enough, you can string together a bunch of computers owned by other people and put them to work mining for you. Folio was able to nab 500 million Dogecoin, equivalent to $620,496, finding most of the coins in January and February right before the patch was released, the researchers discovered. To read more click HERE

600,000 customer details compromised at Domino's

Heise Security, 16 Jun 2014: Today's news that 600,000 customer records have been stolen from Domino's France and Belgium yet again raises questions about just how seriously large corporations and big brands are taking data protection. It is the second time in less than a month that we have seen customers' personal details compromised after the records of 145 million people were affected by the eBay breach. For a period of time hackers turned their attentions away from big businesses as they were seen as too tough a target and turned their attentions to smaller, less resourced targets. However, it would appear that in this period larger organizations have become complacent in their security practices and hackers have been quick to once again re-focus their efforts onto big, data rich organizations. Although it is not certain exactly what records have been affected, it is staggering that the personal details of so many customers were seemingly left unencrypted and susceptible to this kind of attack – especially when you consider the warning shots that have been issued with previous high profile attacks. The possibility that a large organization could even consider leaving data as plain text on a server is surprising to say the least. As a result of this attack there's an additional risk of phishing attacks. Consumers should be aware that the value of that data to criminals and fraudsters should not be underestimated nor should the potential damage that they could suffer as a result. When these serious ramifications are brought into consideration it is concerning that Domino's took four days to alert customers to the potential risks they faced. People should be very cautious about clicking on links in emails which claim to be from Domino's, no matter how authentic they seem to be. There's a very real risk that attackers will try and exploit this attack to send phishing emails to users, to try and harvest more sensitive data. It will also be interesting to see what response, if any, various industry bodies will take in punishing firms for bad practice. For instance if payment card data has been left unencrypted and has been compromised, will the PCI Council move to fine organizations or stand idly by. Business of all sizes should be reviewing their data handling and storage practices as a matter of urgency in the coming days and weeks to ensure that they are not unwittingly offering an easy target for hackers. This should include ensuring that all sensitive data is strongly encrypted. To read more click HERE

Fake Dot-Gov Webmail Used in Phishing Scam to Hack EPA and Census Staff

NextGov, 12 Jun 2014: A Nigerian man has admitted to compromising the email accounts of federal employees to order agency office products that he then sold on the black market, according to newly filed court papers. Abiodun Adejohn and conspirators cheated government supply vendors out of almost $1 million worth of goods through the

scheme. The hackers broke into the accounts through a series of impersonations targeting Environmental Protection Agency and Census Bureau staff. First, they sent the employees "phishing" emails purporting to be from government agencies that contained links to seemingly legit agency webmail login pages. But the webpages actually stole usernames and passwords the employees entered. Many federal agencies are vulnerable to this type of mimicry because of poor cyber hygiene, according to a report released Wednesday. Analysts at the Online Trust Alliance found that many federal webpages and email addresses are missing encryption and verification protections that could prevent phishing scams. In the office supply racket, Adejohn and accomplices "created fraudulent Web pages ('Phishing Pages') that mirrored the legitimate webmail pages of several government agencies," including EPA and Census pages, according to papers filed Monday with the U.S. District Court for New Jersey. The offenders then sent phishing emails to trick the employees into visiting the bogus pages. The hackers "captured any login credentials that victim employees typed into the phishing pages, which were then transmitted to email accounts that they controlled," the court documents state. The identity theft began as early as 2012 and ended around December 2013, according to authorities. Adejohn and accomplices hijacked the email accounts to buy items in the employees' names, repackaged the products in New Jersey and elsewhere, sent the goods to Nigeria and then sold them to rogue vendors for profit. Adejohn was arrested last September in Arizona. He faces up to 20 years in prison and a $250,000 fine. To read more click **HERE**