THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

7 November 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

November 5, Softpedia – (California) **Palm Springs Federal Credit Union loses hard drive with customer data.** An audit at Palm Springs Federal Credit Union in California found that a hard drive containing an undisclosed number of customers' names, Social Security numbers, account numbers, and addresses was unaccounted for on or about October 20. There was no statement on whether the data was encrypted or unencrypted. Source: http://news.softpedia.com/news/Palm-Springs-Federal-Credit-Union-Loses-Hard-Drive-with-Customer-Data-464078.shtml

November 5, Ars Technica – (International) **Crypto attack that hijacked Windows Update goes mainstream in Amazon Cloud.** A researcher stated that he was able to replicate the MD5 hash collision method used in the Flame cyberespionage attacks using a GPU instance on Amazon Web Service to cause two images to have the same MD5 hash. The method was used in the Flame campaign to cause compromised Windows Update certificates to be recognized as valid on targeted systems, allowing malware to be downloaded undetected. Source: http://arstechnica.com/security/2014/11/crypto-attack-that-hijacked-windows-update-goes-mainstream-in-amazon-cloud/

November 4, Softpedia – (International) **Compromised EDU domain used to send out ZeuS-laden emails.** Researchers with PhishMe detected a spam email campaign distributing the Zeus (also known as Zbot) information-stealing trojan through email addresses belonging to an undisclosed U.S. educational organization with around 25,000-30,000 enrolled students. Source: http://news.softpedia.com/news/Compromised-EDU-Domain-Used-to-Send-Out-ZeuS-Laden-Emails-464072.shtml

November 4, SC Magazine – (International) **Spin.com redirects to Rig Exploit Kit, infects users with malware, Symantec observes.** Symantec researchers stated November 4 that the music news Web site Spin.com was redirecting users to a page hosting the Rig Exploit Kit October 27 and that the issue has been closed. The researchers were unsure of how the compromise occurred but found that the attackers injected an iFrame into the site in order to redirect visitors. Source: http://www.scmagazine.com/the-popular-music-news-site-redirected-visitors-to-the-rig-exploit-kit/article/381364/

November 6, Softpedia – (International) **Australia, UK and US are most affected by Dridex banking trojan.** Trend Micro researchers identified an email campaign attempting to distribute the Dridex banking trojan and targeting users in the U.S., U.K., and Australia. The malware is considered the successor to the Cridex banking trojan and can steal online banking credentials. Source: http://news.softpedia.com/news/Australia-UK-and-US-Are-Most-Affected-by-Dridex-Banking-Trojan-464287.shtml

November 4, KCBS 2 Los Angeles – (California) **Thieves steal over $20,000 in computers from elementary school.** Authorities are searching for two suspects who stole about 30 tablets valued at roughly $25,000 from Bryant Elementary School in Riverside November 2. Source: http://losangeles.cbslocal.com/2014/11/04/thieves-steal-over-20k-in-computers-from-elementary-school/

November 6, Securityweek – (International) **New “WireLurker” malware targets iOS, Mac OS X users via trojanized applications.** Researchers with Palo Alto Networks identified a new piece of malware targeting Apple OS X systems and iOS devices dubbed WireLurker, which can run malicious code in order to steal users’ contacts, Apple IDs, and other data. The malware spreads via trojanized and repackaged OS X applications and can compromise any iOS devices linked to an infected system via USB cable by infecting iOS applications on stock or jailbroken devices. Source: http://www.securityweek.com/new-wirelurker-malware-targets-ios-mac-os-x-users-trojanized-applications

Home Depot says about 53 million email addresses stolen in breach

Reuters, 7 Nov 2014: Home Depot Inc (HD.N), the world's largest home improvement chain, said about 53 million email addresses were stolen during a recent breach of its payment data systems, in addition to some 56 million payment cards previously disclosed by the retailer. The company, which confirmed the theft in September, said the stolen files that contained the email addresses did not include passwords, payment card information or other sensitive personal information. Home Depot, which had estimated that the breach would cost about $62 million, was one of a string of U.S. retailers attacked by hackers over the past year. Criminals used a third-party vendor's user name and password to enter the perimeter of its network, Home Depot said in a statement on Thursday. The hackers then acquired "elevated rights" that allowed them to navigate parts of Home Depot's network and to deploy unique, custom-built malware on its self-checkout systems in the U.S. and Canada, according to the company. Home Depot said the stolen credentials did not alone provide direct access to the company's point-of-sale devices. Since September, the company has implemented enhanced encryption of payment data in all U.S. stores and said the rollout to Canadian stores will be completed by early 2015. This, however, was "really lipstick on a pig" and the proper solution was to add chips and PINs, or EMV technology, to U.S. credit cards, said David Campbell, chief security officer at SendGrid, a cloud-based email delivery service. Home Depot said it was already rolling out the EMV technology. The forecast includes estimates for the cost to investigate the data breach, provide credit monitoring services to its customers as well as legal fees, the company said. The company maintained that it has not yet estimated the impact of "probable losses" related to the breach. "Those costs may have a material adverse effect on The Home Depot's financial results in the fourth quarter of fiscal 2014 and/or future periods," the company said. Target Corp's (TGT.N) unprecedented breach saw hackers steal at least 40 million payment card numbers and 70 million other pieces of customer data in 2013. To read more click HERE

India to Beef Up National Cyber Defense

Softpedia, 5 Nov 2014: The government in India has decided to award the cyber security issue more attention and to turn into reality one of its long-proposed cyber defense projects, the National Cyber Coordination Centre (NCCC). The country has allotted $16.2 million for this purpose. The largest part of the money may be used for implementing the NCCC project, which is estimated to cost about $13 million. NCCC’s purpose would be to help the country deal with malicious cyber-activities; it would act as an Internet traffic monitoring entity that can fend off domestic or international attacks. This could raise a serious issue if abused, because there is the risk of privacy invasion on citizens. As expected, officials say that the entity would not have such attributions. Defense World reports that the department of electronics and information technology seeks approval for two additional projects; one is aimed at making the government’s email system stronger. The other is a more ambitious one and it would be designed to tackle the problem of the botnets. Basically, it would have to determine the extent of a botnet and its infrastructure, and take it down in a manner that would not impact on the end users. To read more click HERE

Encrypted Payment Data of over 3,800 Leaked Along with Decryption Key

Softpedia, 5 Nov 2014: Unauthorized individuals accessed encrypted payment details of customers of a hotel booking website by using the decryption key stored with the data. The company, Worldview Limited, found itself fined by the Information Commissioner’s Office (ICO), UK’s privacy watchdog, for keeping the decryption key with the data, allowing intruders undeterred access to sensitive information of 3,814 clients. Following the incident, ICO slapped the company with a $11,900 punishment. At the root of the breach was improper sanitization of SQL statements, which allowed access to the database via an SQL injection vulnerability. ICO issued a call to organizations to start protecting their websites “against one of the most common forms of online attack – known as SQL injection.” With the decryption key stored with the encrypted information and leveraging one of the most basic forms of attacks over a website, the attackers had no trouble reaching full card details. According to a report from ICO, the security code (CVV or CVV2), a string of numbers required for online payments as a means to validate that the physical card is available, not just its data, was also present in the database. Best practices promoted by the Payment Card Industry strongly recommend merchants not to store the CVV or CVV2 details on their systems. Storing the code is generally done for the comfort of the recurrent shopper, who no longer has to enter all the card details. However, in the event that the online shopping account is compromised, the attacker can initiate purchases as if they were the true owner of the account, since no mechanism for authorizing the payment exists. The Information Commissioner’s Office says that the SQL injection flaw existed on the website since May 2010 and was discovered on June 28, 2013, during a routine security check. It appears that the intruders had access to the sensitive details for a period of ten days. The flaw is no longer present in the website as the company has upgraded its security in order to prevent falling victim to other forms of cyber-attack. “It may come as a surprise to many in the IT security industry that this type of attack is still allowed to occur. SQL injection attacks are preventable but organisations need to spend the necessary time and effort to make sure their website isn’t vulnerable. Worldview Limited failed to do this, allowing the card details of over three thousand customers to be compromised,” said Simon Rice, ICO Group Manager for Technology. “Organisations must act now to avoid one of the oldest hackers' tricks in the book,” urged Rice, suggesting to appeal to outside experts if in-house knowledge was not available. To read more click HERE

The Everykey Smartband Will Remember All the Passwords for You

Softpedia, 6 Nov 2014: We all have different accounts on different websites we seldom use, but when the need strikes, it’s really nerve-wrecking to have to squeeze your brain trying to remember your secret combination. Given the need for more and more complex passwords to help safeguard our private data, maintaining more than one account can become a total drag. But the next Kickstarter project wants you to stop worrying about remembering long and complex streams of letters and numbers. The Everykey looks like a simple bracelet that can be worn around your wrist, but the idea behind it has a pretty big potential. The bracelet uses Bluetooth connectivity to help you access accounts on devices, without you actually having to input the password. So, basically, the Everykey can be thought of as a library for your passwords. One which you wear on your wrist every day. So you can be logged into your computer or smartphone and you can automatically access your accounts on those gadgets without the extra fuss. When you’re standing at a certain distance from the device, the band will go into lock-down so other people don’t have access to the gadget you're using. What if your band gets stolen? Well, once you’re done using it, the Everykey can be disabled via the Internet and you can leave it at home, so you don’t have to worry about losing your information. Everykey can be used to unlock Android smartphones and Mac / Windows PCs or to log in to websites using Chrome. If you still don’t find this wristband impressive enough, we should point out that the Everykey can be used to unlock actual physical locks, but it goes without mention that these should be Bluetooth-enabled. Users of the band will be able to customize their wearable, which bundles a battery that can support a life cycle of up to 30 days. The device is water resistant but not waterproof, so it should be handled with care in the vicinity of water. While the concept of a wearable storing part of your identity is not new, as you might remember the Nymi band that used your unique heartbeat pattern to tell you apart from the rest of the crowd, the Everykey does bring to the table an easier way of doing things. Until November 30, Everykey is gathering up funds on Kickstarter that will help push the band into mass production, and if you want to help, you can go ahead and pre-order one of these wearables for $50. When it goes on sale, the band will be up for grabs for $100. If all goes well, the first smartbands will start shipping out in March 2015. To read more click HERE

Cisco Patches Three Out of Four Buggy Small Business RV Series Routers

Softpedia, 7 Nov 2014: Four Cisco routers from the RV series intended for small businesses have been found vulnerable to attacks that could allow execution of arbitrary commands and uploading files to any location on the device. The affected products are Cisco RV120W Wireless-N VPN Firewall, Cisco RV180 VPN Router, Cisco RV180W Wireless-N Multifunction VPN Router, and Cisco RV220W Command injection, CSRF attack and insecure file upload glitches Cisco issued an advisory on Wednesday detailing a total of three flaws affecting the above mentioned products and released firmware updates for all but one product, RV220W, which is expected to receive a patch by the end of the month. One of the security glitches detected by the company allows a potential attacker to remotely execute arbitrary commands with the highest privileges (root), by delivering a specially crafted HTTP request to the vulnerable device. The flaw can be exploited provided that the attacker is authenticated. Identified as CVE-2014-2177, the glitch resides in the network diagnostics administration pages of the routers and emerged because of improper validation of user-supplied input. Another bug (CVE-2014-2178) enclosed in the latest updates opened the door for a cross-site request forgery (CSRF) attack from a remote, unauthenticated intruder. User intervention is required for carrying out the compromise, as an authenticated victim has to be tricked to launch a maliciously crafted link, thus allowing the attacker to complete unauthorized actions, with the same privileges as the authenticated user. The third vulnerability (CVE-2014-2179) plaguing Cisco RV series routers is in the way file uploads are executed, offering the possibility to a remote, unauthenticated individual to place an item anywhere on the device. According to Securify, the company reporting all three issues to Cisco, a certain cookie handled in an insecure manner allows a potential attacker to set an arbitrary path for the uploaded file, which would overwrite existing items. Researchers say that this is possible because the cookie value is used as the path name and there is no input validation for it. Workarounds for reducing risk until permanent fix is applied Cisco provides firmware update 1.0.4.14 for the RV180 and RV180W devices and 1.0.5.9 for the RV120W. If these cannot be applied right away, the company offers workaround solutions for eliminating the security risks until the update with a permanent fix can be installed; these settings are valid for RV220W, too. The measures consist in disabling remote management for the devices, so that an attacker outside the network would not be able to connect to the router and make modifications; however, if management is done through WAN, this action is not required. This would limit exploitation attempts to users in the LAN and would also prevent Cisco QuickVPN access. Another option is to restrict remote management permission to certain IP addresses. To read more click HERE

Microsoft Announces 16 Security Updates for Windows and Office

Softpedia, 7 Nov 2014: Microsoft and its users will “celebrate” Patch Tuesday next week, so today the company has revealed the number of updates expected to be released as part of this rollout, along with the name of the software solutions to be targeted by these improvements. The upcoming Patch Tuesday cycle is more or less a “one-app show” as Windows gets the majority of improvements, with all versions that are still supported to receive more or less important security fixes. Five of the of 16 security updates that will be released next week are rated as critical and at least four will require a restart, so system administrators must prepare to save the current state of their computers before deploying the fixes. In addition to Windows, Office, Internet Explorer, and .NET Framework are also getting security updates next week, so make sure that you keep an eye on the rollout on Tuesday to get the patches as soon as they're released. All Windows versions will receive security fixes next week, including the Windows 10 Technical Preview that has already been downloaded by 1 million Windows Insider Program members who registered with their accounts in order to give the upcoming operating system a try. A total of four updates will be shipped to Windows 10 machines, all via Windows Update, and reboots will be required, but that shouldn't be a problem since this particular OS version is specifically designed for testing purposes. As Wolfgang Kanded, CTO of Qualys, notes, the upcoming Patch Tuesday will bring quite a lot of work for IT admins, so some efforts in advance of the release are required. “A big release like this month's covers all versions of the Windows operating system, both for servers and workstations, the .NET stack, Microsoft Office, Sharepoint and Exchange. Plenty of work for IT admins on all levels, server, desktop and applications, but the focus should be on the top five," he says. All versions of Microsoft's in-house browser will get patched next week, starting with Internet Explorer 6 on Windows Server 2003 and ending with Internet Explorer 11 on Windows 8.1. Kandek says that this will be the highest priority bulletin because of the risks caused by browser vulnerabilities, so make sure that you deploy this one as soon as possible, especially if you use Internet Explorer to browse the web. All updates will be shipped via Windows Update, as is the case every month, so an Internet connection should be all you need to get them. Hopefully, no botched updates will be shipped this time. To read more click HERE

In 2015, Intel Will Replace Passwords with Your Face

Softpedia, 6 Nov 2014: For the past twenty or so years, computer systems and all related hardware have moved forward at a steady pace, but other than tablets there hasn't been any huge concept redesign for them. Intel wants to change this in the coming years. With conventional desktops losing ground to mobile PCs, and normal laptops making room for 2-in-1 hybrids, Intel is thinking that it may as well lobby for changes in areas other than physical design. One thing we already know is definitely coming is the ability to run entirely free of cables. This will happen by 2020, with 2016 to show the first big signs of transition. Now, Intel is providing some information on another one of its goals: safer login methods for PCs, and better security in general. Passwords have been a thing since forever. Whether in the form of something only you and a friend know, or a really complicated number key on an electronic device, they've been used since time immemorial. Now, though, Intel aims to eliminate them, or rather eliminate the need for their use, at least on computers, by swapping them for biometric login instead. The tactic is two-fold. First, the cables will be eliminated, closing that path forever and handily removing any situation where a password might be needed to regulate link access. Wi-Fi / Bluetooth will be the only ways in or out. The other half of the tactic consists of installing cameras, microphones and other sensors that will determine whether you are the PC's owner or not. Of course, since this system, called "you are the password" or YAP for short, merely turns you into the pass key (by taking a 3D scan of your face, reading your fingerprints and / or recording your voice), a good case can be made for passwords not actually disappearing at all. The concept is just going forward under a different guise. Other applications for face recognition If the YAP system is good enough to recognize you even if you have an identical twin (though it's not sure if this is the case), there is definitely room for other uses. Like new ways of controlling what the system does, track expressions and map them on a virtual avatar (can you say immersive co-op multiplayer games?), and maybe even in the development of AIs that can accurately recognize emotion on humans. To read more click HERE

Alleged Silk Road 2.0 Boss Arrested by the Feds, DarkNet Markets Go Down

Softpedia, 7 Nov 2014: A 26-years-old man by the name of Blake Benthall has been arrested by law enforcement in connection with ownership of Silk Road 2.0, an illegal marketplace operating under the anonymity of Tor network. The market was considered the largest among its competitors on the Darknet, offering a wide selection of drugs along with malicious software and services intended for computer hacking (infostealers, keyloggers, remote access tools) and fake documents. Benthall, known by the online alias "Defcon," is believed to have set up Silk Road 2.0 in order to resurrect the original black-market bazaar with the same name that was seized by the authorities last year. "Those looking to follow in the footsteps of alleged cybercriminals should understand that we will return as many times as necessary to shut down noxious online criminal bazaars. We don't get tired," said Manhattan U.S. Attorney Preet Bharara in a communication from the US Department of Justice. According to FBI Assistant Director-in-Charge George Venizelos, the illicit business was very profitable, generating millions of US dollars in sales on a monthly basis. It is alleged that the 150,000 active users of Silk Road 2.0 generated a money flow of at least $8 / €6.45 million, and the operators earned at least $400,000 / €323,000 in commissions; all transactions were made in digital currency in order to preserve anonymity. The authorities believe that Benthall owned and operated the illegal website since December 2013, turning it into one of the largest online locations for exchanging unlawful goods on the web. The marketplace emerged just five weeks after the owner of its previous version, Ross William Ulbricht (known as "Dread

Pirate Roberts"), was arrested in November 2013. On October 17, 2014, the website's listings included 1,783 entries for psychedelics, 1,697 for Ecstasy, 1,707 for cannabis, and 379 for opioids. Silk Road 2.0 has been taken down by the authorities, together with other Darknet marketplaces, including Cloud 9, Hydra, Pandora, Blue Sky, Topix, Flugsvamp, Cannabis Road, and Black Market. Many of these are smaller markets or relatively new ones established inside Tor. Bringing down the sites is part of an operation law enforcement organizations dubbed "Onymous." The full scope of the action was to remove underground platforms that facilitated the trade of illegal goods. A total of 17 individuals have been arrested in connection with administering the black markets and more than 410 .onion domains (addresses for websites accessed through Tor) have been closed, according to information from EC3 (Europol's European Cybercrime Centre). During Operation Onymous, through its cybercrime fighting units, Europol coordinated the activity of law enforcement agencies in 16 European countries: Bulgaria, Czech Republic, Finland, France, Germany, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Romania, Spain, Sweden, Switzerland, and the United Kingdom. Blake Benthall is facing multiple conspiracy charges, which include narcotics trafficking (mandatory 10 years of jail time, maximum sentence: life in prison), computer hacking (maximum sentence: 5 years in prison), trafficking fraudulent documents (maximum sentence: 15 years in jail) and money laundering (maximum sentence: 20 years in jail). However, any sentence is to be determined by the judge. The full complaint against Benthall contains interesting pieces of information about Silk Road 2.0 activity and the administrator's involvement in the enterprise. To read more click HERE