The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

16 May 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

May 15, Softpedia – (International) **Three security fixes included in Chrome 34.0.1847.137.** Google released the latest stable version of its Chrome browser, including three security fixes. Source: http://news.softpedia.com/news/Three-Security-Fixes-Included-in-Chrome-34-0-1847-137-442377.shtml

May 15, Softpedia – (International) **Fake Kaspersky apps discovered on Windows Phone Store and Google Play.** Kaspersky Labs researchers identified fake Kaspersky mobile security apps in the Windows Phone Store and Google Play store. The fake apps appear similar to previous fake antivirus apps that ask users for payment but contain no actual functionality. Source: http://news.softpedia.com/news/Fake-Kaspersky-Apps-Discovered-on-Windows-Phone-Store-and-Google-Play-442358.shtml

May 14, Threatpost – (International) **Buffer overflows patched in Yokogawa control system products.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported May 14 that Yokogawa Electric Corporation made patches available for three vulnerabilities identified in its Yokogawa Centrum CS3000 production control system. The Centrum CS line is used for several industrial uses such as in oil refineries, steel manufacturing, public utilities, and other manufacturing industries. Source: http://threatpost.com/buffer-overflows-patched-in-yokogawa-control-system-products/106074

DOD extends IT worker exchange program

Washington Business Journal, 15 May 2014 The Pentagon issued final regulations Wednesday that extend a pilot program that help exchange IT workers from the Department of Defense with their counterparts in the private sector, Nextgov reports. The regulations, published in the Federal Register, extend DOD's Information Technology Exchange Program pilot, originally scheduled to expire in 2013, to Sept. 30, 2018. The extension was previously approved by Congress. "Given the changing workforce dynamics in the IT field, DoD needs to take advantage of these types of professional development programs to proactively position itself to keep pace with the changes in technology," the regulations state. "The ITEP pilot will serve the public good by enhancing the DoD IT workforce skills to protect and defend our nation." Launched in 2012, the program authorizes the temporary assignment of Pentagon IT employees to private sector organizations and also gives DOD the authority to accept private sector IT employees. To read more click **HERE**

Filenames Used by VOBFUS Malware Change Depending on Victim's Language

SoftPedia, 16 May 2014: Security researchers have come across a new variant of the worm known as VOBFUS. The latest version can "speak" 21 different languages. Similar to older versions, WORM_VOBFUS.JDN spreads by copying itself to removable drives as executable files. However, unlike previous variants, the latest VOBFUS names the files depending on the operating system language of the targeted computer. Uses who speak English will see files named something like "I love you.exe," "Naked.exe," "Password.exe," "Sexy.exe," and "Webcam.exe." If the operating system is set to another language, these names are translated. The worm is designed to target speakers of the following languages: English, Indonesian, Arabic, Chinese, Bosnian, Czech, Croatian, German, French, Hungarian, Korean, Italian, polish, Persian,

threat response engineer at Trend Micro. "Seeing a file or a notification written in their language might pique users' interest more than seeing one written in English. Users may also find a false sense of security in these 'localized' files and notifications as they might view these as less suspicious than other files." Such tactics are usually utilized for police and file-encrypting ransomware, but obviously they're efficient for other types of malware as well. To read more click **HERE**

Saudi Government to Recruit Ethical Hackers

Softpedia, 16 May 2014: The Saudi Arabian Ministry of Interior's National Information Center wants to recruit hackers to help protect the country's networks. According to the Saudi Gazette, the National Information Center's representatives say recruits will be trained to "transform their abilities into productive energy." Dr. Zaidan Al-Enezi, the center's external affairs coordinator, highlights the fact that some hackers only know how to breach websites, and they're not skilled when it comes to networks. Only ethical hackers are being recruited. Hackers who have targeted government systems or websites will not be accepted. Al-Enezi admits that hiring hackers is not a 100% efficient for thwarting cyberattacks. However, he encourages all government agencies and universities to employ security experts to protect their computer systems. He also reveals the fact that the center will work with government organizations to ensure that international standards are respected. The official strongly believes that this could help prevent around 80% of hacker attacks. "The center is continually developing its mechanisms and employing the latest technologies in electronic safety. The center cannot prevent attacks by hackers, but can only plug any holes that hackers may exploit in their attacks," says Al-Enezi. "The center is continually developing its mechanisms and employing the latest technologies in electronic safety. The center cannot prevent attacks by hackers, but can only plug any holes that hackers may exploit in their attacks." To read more click **HERE**

Member of Carder.su Cybercrime Forum Sentenced to 20 Years in Prison

SoftPedia, 16 May 2014: 22-year-old David Ray Camez, aka "Bad Man," has been sentenced to 20 years in prison and three years of supervised release for being a member of Carder.su, the notorious identity theft service. In addition, Camez will also have to pay $20 million (€15 million) in restitution. The man was convicted in December 2013 for participating in a racketeer influenced corrupt organization, and conspiracy to participate in a racketeer influenced corrupt organization. Back in 2008, Camez became a member of Carder.su, a cybercrime forum which in July 2011 had around 5,500 members. During 2009 and 2010, he purchased fake driver's licenses from an undercover agent. Investigators also intercepted counterfeit cards sent to Camez by someone from Pakistan. When his home was raided in May 2010, agents found not only counterfeit payment cards, but also the equipment used to create them. They also discovered fake IDs and counterfeit money. US authorities charged a total of 55 individuals in the Carder.su case, 39 of which were indicted in January 2012. In addition to Camez, 21 people have already pleaded guilty and two face trial in June. However, many of the suspects are still at large. Camez was not a mastermind of the operation, yet he still got 20 years in prison. That's because, as Sophos experts highlighted, he was tried under the Racketeering Influenced Corrupt Organizations (RICO) Act. "The idea of RICO is to make criminal gangs collectively liable for the offences they commit as an organized group," Sophos' Paul Ducklin explained. This means that, while Camez might seem nothing more than a fraudster, he has been convicted as a member of major criminal organization. "Camez was a member of a vast criminal organization that facilitated rampant cyber fraud throughout the world," said Acting Assistant Attorney General David A. O'Neil of the Justice Department's Criminal Division. "This organization is the new face of organized crime – a highly structured cyber network operated like a business to commit fraud on a global scale. Members, like Camez, paid to tap into the network and gain control of highly sensitive information, like compromised credit card numbers and stolen identities. Thanks to sophisticated law enforcement efforts, Camez will now pay for his crimes with decades in prison." Claude Arnold, special agent in charge of Homeland Security Investigations (HSI) in Los Angeles, noted, "As this sentence demonstrates, cyber-criminals who purposely harm innocent Americans and compromise the world's economic stability

will be aggressively pursued, investigated and prosecuted – and ultimately receive the justice they deserve." To read more click **HERE**

Australian Internet Explorer Users under Attack, Security Company Warns

SoftPedia, 16 May 2014: A zero-day flaw in Internet Explorer that was found in April and patched by Microsoft one week after that is still being exploited in Australia, according to security firm FireEye. In a report published on ZDNet, FireEye warns that business computers in resource and mining, financial services, and telecommunications industries are being targeted right now, but more users could be targeted by similar attempts in the near future. FireEye ANZ engineering manager, Rich Costanzo, explained that although Microsoft already released a patch to address this issue, some business computers are yet to be updated, so they might still be vulnerable to attacks. Microsoft's patch was aimed at all OS versions on the market, including Windows XP, which reached end of support on April 8. "This is clear proof that what we're seeing globally in terms of zero days and breaches is happening here in Australia. Not only that, it's happening in record time. In fact, less than 72 hours after the IE vulnerability became known we were detecting it here," Constanzo explained, pointing out that this is the first attack supposed to exploit this vulnerability in Australia. The easiest way to stay on the safe side right now is to update your computer and deploy the latest patches rolled out by Microsoft. Of course, upgrading to a newer OS version could also help, but keep in mind that Windows XP is one of the platforms that actually got patched and is no longer affected by this zero-day flaw. "The idea with a vulnerability like that is even though there is a patch released it potentially takes a while for that patch to take wide spread use and for everyone to have that installed, so a vulnerability does continue even though a patch is available. This particular one also had multiple reiteration. The first was focused on IE versions 9 to 11, and a few days later we saw a second reiteration attack that was was focused on Windows XP and IE 8," Constanzo continued. FireEye's expert also explained that moving off Windows XP should also be a priority for those who are still running this particular OS version, and although Microsoft addressed this flaw with a previous update, new vulnerabilities could actually expose your data and make your system open to attacks. Approximately 26 percent of the desktop computers in the world are still running Windows XP right now, according to third-party statistics. To read more click **HERE**

Blu-Ray Disks Reach 256 GB, Can Clone Full SSDs

SoftPedia, 16 May 2014: The Blu-ray disk standard, though expensive, was amazing enough even when it "only" supported 100 GB or 128 GB storage space (BDXL specification), but Pioneer wasn't satisfied with just that, so it went further. Though by "further" we don't mean to say that the BD association just slapped a new layer to the things. It's not like it would have been all that possible either, since 128 GB disks already have four. Any more than that and the accuracy of the scribed data, or of the beam for that matter, are debatable. Instead, Pioneer created a new Blu-ray standard that allows for up to 512 GB of storage space, though only 256 GB are possible at the moment. They are able to clone or back up your entire solid-state drive, or even your HDD if it's a particularly low-capacity one (unlikely as it is, in these times). The best part is that you don't need a totally new disc writing and reading technology to use them. Sure, new optical drives will have to be made, but they are still based on the Blu-ray standard, so Pioneer is sure to release such a product soon. Previous super-capacity disk storage products relied on specially made reading drives and cost a lot, like the disks themselves for that matter. They never caught on. Then again, it's not exactly certain that this new media will catch on either. At least not in the near future. Perhaps a decade from now we'll really have console games large enough to demand them, but for now, even 128 GB is too much. Also, people are more likely to purchase a USB 3.0 flash drive unit or an external/portable HDD (hard disk drive) or SSD. They're easier to carry around and can connect to a PC on their own, making them much more convenient. Not even 4K films need as much capacity as Pioneer's latest disk offers. All in all, one could argue that it's a bit (or a lot) ahead of its time. On the flip side, since Blu-ray drives are capacious enough now (BDXL ones anyway) to only be "worth it" in backup and other big data applications, demand for it might turn out to be decent after all. That will ultimately hinge on the endurance of the new standard though. We

don't know the data retention on these things, though since they're still Blu-ray drives, we can afford to be optimistic. Pioneer is at least. To read more click **HERE**

BlackShades RAT Users from All Over Europe and Australia Reportedly Raided

SoftPedia, 16 May 2014: Law enforcement authorities in Europe have raided tens or possibly even hundreds of individuals suspected of using the BlackShades remote access Trojan (RAT). According to French publication RTL, over 70 locations were searched on Tuesday in France, including in Paris, Lille and Bordeaux. On a hacker forum, one user from Germany reported being visited by German police because he had purchased the BlackShades RAT. Agents seized a PC, a laptop, an external hard drive, and cryptography-related documents. One individual from the Netherlands also claimed to have been visited by seven agents of the country's cybercrime police. He said that his phone, computer and other electronics were seized. Nu.nl has reached out to Dutch authorities to get confirmation, but the police say that it's an ongoing investigation, so they can't make any statements. Hacker forum members have also reported raids in Belgium, the UK, Denmark, Italy, Sweden and even Australia. However, we haven't been able to confirm these reports. In the summer of 2012, following a 2-year investigation, the FBI announced the arrests of 23 alleged cybercriminals. One of them was then 21-year-old Michael Hogue, aka xVisceral, believed to be one of the creators of BlackShades. xVisceral announced his retirement from the hacking scene in August 2011. However, he remained active on several cybercrime forums, even offering support for BlackShades customers. L'Express reports that after xVisceral's arrest, French police were provided with a list of local BlackShades customers. It's possible that authorities in other countries have been provided with such information as well. BlackShades is a RAT that can be used to take over an infected computer, including for monitoring webcams, logging keystrokes and stealing files. It's currently being sold for between $40 (€30) and $100 (€73) on cybercrime forums. At the time when Hogue was arrested, security experts warned that other members of the cybercriminal group would likely continue working on improving and distributing the RAT, and they were right. In late November 2013, Symantec warned of an increase in the usage of BlackShades. At the time, researchers revealed that cybercriminals were using the Cool Exploit Kit to distribute the threat. Cool EK became the most prevalent exploit kit after the arrest of the author of BlackHole exploit kit. We'll probably find out more about this operation once authorities come forward with a statement to the press. If there have been so many raids in Europe, Europol's EC3 has been most likely involved, so we should expect to hear from them. To read more click **HERE**