The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

19 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

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, Sandia Labs

Latest OS X Update Contained iTunes Bug

Yahoo, 19 May 2014: If you're a Mac user and you downloaded this week's Mac OS X update (Mavericks 10.9.3), you may have noticed that your computer's Users/ and Users/Shared/ folders have disappeared. It turns out the disappearance is due to a security flaw in iTunes 11.2, which was part of the OS X Mavericks 10.9.3 update. The flaw is only really serious on iMacs and MacBooks with multiple user accounts, as it lets one account compromise the other accounts on the same computer. Apple Apple explained in a support note that the bug had to do with how the computer handles the permissions of separate users on the same machine: "Upon each reboot, the permissions for the /Users and /Users/Shared directories would be set to world-writable, allowing modification of these directories [by any user]." The issue also occurred on some Mavericks computers that had iTunes 11.2 installed separately without upgrading to Mavericks 10.9.3. OS X Mavericks 10.9.3, which contained the buggy iTunes 11.2, also included an update to Safari 7.0.3, improved support for 4K screens, the ability to sync contacts and calendars between a mobile device and a Mac via USB, and a number of security updates that had been previously released. To read more click **HERE**

81 People Arrested in International Operation Against BlackShades RAT Users

SoftPedia, 19 May 2014: Last week, 300 houses were raided and 81 people were arrested as part of an international law enforcement operation targeting people believed to be responsible for selling, creating and using the BlackShades Remote Access Trojan (RAT). First rumors of the operation emerged last week, when the members of various popular hacker forums revealed that they were raided by police. On Monday, Europol confirmed the operation and provided more details. Raids took place in over 10 countries, including Belgium, France, the Netherlands, Germany, the UK, Estonia, Austria, Canada, the US, Denmark, Chile, Italy and Croatia. A total of more than 1,000 computers, laptops, mobile phones, USB sticks, external hard drives and routers were seized by investigators. "This case is yet another example of the critical need for coordinated law enforcement operations against the growing number of cyber criminals operating on an EU and global level," said Troels Oerting, head of the European Cybercrime Centre (EC3). "EC3 will continue - together with Eurojust and other partners - to work tirelessly to support our partners in the fight against fraudsters and other cyber criminals who take advantage of the Internet to commit crime." The BlackShades RAT, which is currently sold for between $40 and $100, is highly popular among cybercriminals. The malware can be used to hijack webcams, steal files, log keystrokes, and launch denial-of-service attacks against a designated target. In a recent case in the Netherlands, an 18-year-old used it to infect over 2,000 computers. The teen hijacked the webcams of infected devices in an effort to capture intimate pictures of women. The FBI arrested Michael Hogue, one of the creators of BlackShades, back in 2012. However, others continued to improve the RAT even after Hogue's arrest. In November 2013, Symantec announced that the use of BlackShades had increased in the previous five months. "This case is a strong reminder that no one is safe while using the internet, and should serve as a warning and deterrent to those involved in the manufacture and use of this software," Koen Hermans, assistant to the National Member for the Netherlands, noted. "This applies not only to victims, but also to the perpetrators of criminal and malicious acts. The number of countries involved in this operation has shown the inherent value in Eurojust's coordination meetings and coordination centres." To read more click **HERE**

Microsoft Confirms Windows 8.1 Update Installation Errors, Promises New Fix

SoftPedia, 19 May 2014: Microsoft has pushed the Windows 8.1 Update installation deadline to June 10 in order to give more time to users who are still struggling to deploy it, but it appears that some are still experiencing issues. Soon after the launch of Windows 8.1 Update, a number of users took to Microsoft's Community forums to complain about errors showing up during the installation process. Microsoft has until now tried to address all these bugs several times, but even though it decided to get more time by delaying the 8.1 Update installation deadline, it appears that many consumers are experiencing the exact same issues as before. 80070020, 80073712, and 0x800f081f are some of the errors users are seeing when trying to deploy Windows 8.1 Update on their computers. The company confirmed in a post on its forums that it's indeed aware of some bugs in the way Windows 8.1 Update is being deployed on specific computers and provided a statement to say that it's looking into the matter right now and a fix should be provided soon. "I want to take a moment to repeat what one of our engineers posted in a separate post that should be of some help," a Microsoft forum moderator said in a short post on the company's forums. "For customers experiencing difficulty updating their systems to Windows 8.1 Update, I want to let you know that we are working to resolve as quickly as we can. Many customers have been helped by following the steps suggested in the beginning of this thread. If following the troubleshooting steps listed in this link does not help, we ask that you contact Customer Support directly by clicking here as this is the only way for us to assess your individual situation. Thank you for your understanding." Microsoft decided to make Windows 8.1 Update installation mandatory for all Windows 8.1 computers, which means that everyone running this particular OS version needs to deploy the new build by June 10. The company claims that all future improvements will be based on 8.1 Update, so making it mandatory is basically the only option. Windows 8.1 Update is being delivered to Windows 8.1 computers via Windows Update, but it's also available as a manual download for those experiencing issues. It remains to be seen, however, if Microsoft indeed manages to address these issues and provide a fix in time for the June deadline. To read more click **HERE**

NIST to revise Industrial Control Systems security guide

Heise Security, 19 May 2014: The National Institute of Standards and Technology (NIST) has issued for public review and comment a proposed major update to its Guide to Industrial Control Systems (ICS) Security (**link**). Most industrial control systems began as proprietary, stand-alone collections of hardware and software that were separated from the rest of the world and isolated from most external threats. Today, widely available software applications, Internet-enabled devices, and other IT offerings have been integrated into many systems, and the data produced in ICS operations are increasingly used to support business decisions. This connectivity has delivered many benefits, but it also has increased the vulnerability of these systems to malicious attacks, equipment failures and many other threats. Downloaded more than 2.5 million times since its initial release in 2006, the NIST guide advises on how to reduce the vulnerability of computer-controlled industrial systems used by industrial plants, public utilities and other major infrastructure operations to malicious attacks, equipment failures, errors, inadequate malware protection and other software-related threats. The new draft (the second revision of the guide) includes updates to sections on ICS threats and vulnerabilities, risk management, recommended practices, security architectures, and security capabilities and tools for ICS. Due to their unique performance, reliability and safety requirements, securing industrial control systems often requires adaptations and extensions to security controls and processes commonly used in traditional IT systems. Recognizing this, a significant addition to the draft is a new appendix offering tailored guidance on how to adapt and apply security controls and control enhancements detailed in the 2013 comprehensive update of Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53, revision 4) to ICS. SP 800-53 contains a baseline set of security controls that can be tailored for specific needs according to an organization's mission, operational environment, and the technologies used. The new draft Guide to Industrial Control Systems (ICS) Security includes an ICS overlay that adapts and refines that baseline to address the specialized security needs of utilities, chemical companies, food manufacturers, automakers and other users of industrial control systems. To read more click **HERE**

Linux gets fix for code-execution flaw that was undetected since 2009

ARS Technica, 12 May 2014: Maintainers of the Linux kernel have patched one of the more serious security bugs to be disclosed in the open source operating system in recent months. The five-year-old code-execution hole leaves computers used in shared Web hosting services particularly vulnerable, so users and administrators should make sure systems are running updated versions that contain a fix. The memory-corruption vulnerability, which was introduced in version 2.6.31-rc3, released no later than 2009, allows unprivileged users to crash or execute malicious code on vulnerable systems, according to the notes accompanying proof-of-concept code available here. The flaw resides in the n_tty_write function controlling the Linux pseudo tty device. "This is the first serious privilege escalation vulnerability since the perf_events issue (CVE-2013-2049) in April 2013 that is potentially reliably exploitable, is not architecture or configuration dependent, and affects a wide range of Linux kernels (since 2.6.31)," Dan Rosenberg, a senior security researcher at Azimuth Security, told Ars in an e-mail. "A bug this serious only comes out once every couple years." As Ars reported in May 2013, the then-two-year-old CVE-2013-2049 continued to imperil users more than a month after Linux maintainers quietly released a patch for the gaping hole. While the vulnerability can be exploited only by someone with an existing account, the requirement may not be hard to satisfy in hosting facilities that provide shared servers, Rosenberg said. It could also come handy in multi-stage attacks that exploit a variety of bugs that, when combined, give the attacker unfettered control over a targeted system. As others have pointed out, the vulnerability also has the potential to affect Google's Android and Chrome OSes. To read more click **HERE**

How to stash secret messages in tweets using point-and-click steganography

ARS Technica, 8 May 2014: Steganography is the ancient practice of stashing secret text, images, or messages inside a different text, image, or message. It dates back to as early as the fifth century BC, when Spartan King Demaratus removed the wax from a writing tablet and wrote a message hidden on the wood underneath warning of an imminent invasion by Xerxes. Steganography was a common technique used by German spies in both World Wars. More recently, it has been used to conceal highly advanced espionage malware inside image files and stash secret al-Qaeda documents inside pornographic images. Now steganography is going mainstream with a service that embeds hidden messages inside more or less ordinary Twitter messages. Users need only type the text they want others to see in one field and the hidden message in a separate field. The service, created by New Zealand-based developer Matthew Holloway, then spits out a tweetable message that fuses the two together in a way that's not noticeable to the human eye. Take the following tweet:

T h e t e X t h i d d e n i n t h i s ° t w e e t i s s o s e c r e t t h a t i t ' s ° i m p o s s i b l e f o r a d V e r s a r i e s t o r e a d o r d e t e c t ° # s t e g a n o g r a p h y r o c k s # s e c u r i t y # p r i v a c y

Embedded in the visible message "The text hidden in this tweet is so secret that it's impossible for adversaries to read or detect #steganographyrocks #security #privacy" are the words "no, it's security through obscurity." The letters making up the secret text are expressed in unicode representations that are included in the public message. The encoding added to the messages explains the unusual spacing and fonts found in the tweet. With a little more work, or in formats not as constrained as Twitter's 140-character limit, it would almost certainly be easier to create messages that appeared less crude. The same service takes finished tweets and ferrets out their hidden cargo. While steganography has long been relied on to safeguard sensitive messages, people should realize the technique is little more than security through obscurity. That's because the embedded secret is ripe for plucking by anyone who takes the time to look for it. By contrast, ciphertext generated using strong and time-tested encryption algorithms is virtually impossible to decode without the underlying key, which can take centuries or millennia to guess using even the fastest computers. So put steganography in the same category as disappearing ink. It may even have useful applications in rare circumstances. For instance, it might be an effective technique for a prisoner of war sending a postcard to family members. If it were to include a random-appearing sequence of letters, it would be clear to captors that it included an encrypted message. If

instead the POW crafted a postcard that used every fifth letter to spell a hidden message, the captors might not notice. That said, steganography is mostly fun to play with. It should never be relied on to protect digital crown jewels without a good reason and with plenty of forethought. To read more click **HERE**

US man gets 20 years for cybercrime role

Heise Security, 16 May 2014: A man has been sentenced to 20 years in federal prison for his role in what authorities say is an unprecedented criminal case involving an international cybercrime syndicate with hundreds of thousands of U.S. victims. A federal judge in Las Vegas imposed the sentence Thursday on David Camez, 22, who already is serving a seven-year term in Arizona for similar crimes. Camez, who was convicted of racketeering charges late last year, is the first of 55 members of the Las Vegas-based "Carder.su" syndicate to go to trial. They were charged in four separate indictments in 2012. About 20 defendants have pleaded guilty. Of the handful who has been sentenced so far, all have drawn only two years in prison. Two dozen defendants, including the group's Russian leaders Roman Zolotarev and Konstantin Lopatin, are still at large, authorities said. The case marks the first time the Justice Department has used federal racketeering statutes to go after a cybercrime syndicate, the Las Vegas Review-Journal reported. "As shown in this case, cybercrime has grown into an industry and is rapidly overtaking traditional crime, such as bank robbery," Nevada U.S. Attorney Daniel Bogden said. "Cybercrime was once viewed as the crime wave of the future, but in reality that threat is here now." The syndicate is accused of victimizing hundreds of thousands of Americans and several financial institutions, and of committing more than $50 million worth of financial fraud. Prosecutors say its scheme revolved largely around the buying and selling of pilfered debit and credit card information on an Internet site called Carder.su. The secretive criminal organization had more than 7,800 members worldwide. Camez became involved at the age of 17. "Camez was a member of a vast criminal organization that facilitated rampant cyberfraud throughout the world," said David O'Neil, acting assistant attorney general 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." Michael Adams, a Secret Service agent who infiltrated the crime ring, testified Thursday that federal agents recovered 210,000 stolen credit and debit account numbers in raids. Camez, whose online nicknames were "Bad Man" and "Doctorsex," had nearly 2,000 compromised account numbers in his possession, Adams said. He also was ordered to share in restitution of nearly $51 million. During sentencing, U.S. District Judge Andrew Gordon said he had sympathy for the victims because he also has experienced identity theft. "You appear to be a pretty smart guy," Gordon told Camez. "It's a shame you used your talents in a bad way. Your history tells me I need to protect the public from you." To read more click **HERE**