The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

21 February 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

February 19, Washington Post – (Maryland) **U-Md computer security attack exposes 300,000 records.** Officials from the University of Maryland reported that the university's secure records database was breached February 18 when an outside source gained access to 309,079 personal records for faculty, staff, and students who have received identification cards at the school dating back to 1998. Authorities are investigating the breach, which included Social Security numbers, dates of birth, and names. Source: http://www.washingtonpost.com/local/college-park-shady-grove-campuses-affected-by-university-of-maryland-security-breach/2014/02/19/ce438108-99bd-11e3-80ac-63a8ba7f7942_story.html

February 20, Help Net Security – (International) **Microsoft issues Fix it for critical IE 0-day exploited in attacks.** Microsoft released a security advisory and a Fix it tool temporarily mitigating the IE zero-day vulnerability actively exploited in attacks in the wild until a patch is released. Source: http://www.net-security.org/secworld.php?id=16392

February 20, IDG News Service – (International) **Cisco fixes flaws in several products.** Cisco Systems released security updates addressing serious vulnerabilities in a range of products including its Unified Computing System (UCS) Director, Intrusion Prevention System, Unified SIP Phone 3905, and Firewall Services module products. Source: http://www.computerworld.com/s/article/9246466/Cisco_fixes_flaws_in_several_products

Two Romanians Sentenced to 57 Months in Prison for Role in ATM Skimming Scheme
SoftPedia, 21 Feb 2014: Two Romanian nationals living in Queens, New York, have each been sentenced to 57 months in prison for their roles in an ATM skimming scheme. According to authorities, 30-year-old Ioan Leusca (a.k.a. Ionel Spinu) and 29-year-old Dezso Gyapias (a.k.a. Valentin Folea) pleaded guilty to conspiracy to commit bank fraud and aggravated identity theft. They've been in custody since their arrests in January 2013. The Romanians and their accomplices installed payment card skimming devices and pinhole cameras at various ATMs in New Jersey and Connecticut. They used the stolen information to clone the cards. They utilized these cards to withdraw $985,000 (€718,506) from Citibank ATMs New Jersey, New York, and Connecticut. Their actions are said to be part of a bigger skimming scheme that cost financial institutions a total of $5 million (€3.64 million). Eight other Romanians have been charged for their role in this scheme. Seven of them are in custody. US authorities don't know the name of the suspect that's still at large. They only know him by his nickname, "Chioru," which in Romanian means "one-eyed." To read more click **HERE**

Microsoft Launches Fix for Windows Update Corruption Errors
SoftPedia, 21 Feb 2014: Microsoft has released a new non-security update for Windows supposed to correct errors encountered after launching Windows Update. According to a report by ZDNet, the patch is being delivered in the form of a tool called System Update Readiness Tool on Windows 7, Windows Server 2008 RT, Windows Server 2008, and Windows Vista, while on Windows 8.1, Windows8, Windows Server 2012 R2 and Windows Server 2012

it's called Deployment Image Servicing and Management. The following errors are said to be fixed by the new patch: 0x80070002, 0x8007000D, 0x800F081F, 0x80073712, 0x800736CC, 0x800705B9, 0x80070246, 0x8007370D, 0x8007370B, 0x8007370A, 0x80070057, 0x800B0100, 0x80092003, 0x800B0101, 0x8007371B, 0x80070490. At this point, the patch is only available if you manually download it, but the company might start shipping it to users automatically using Windows Update and thus fix all operating systems without user input. To read more click **HERE**

Mistake Made by BitCrypt Developers Allows Experts to Recover Encrypted Files

SoftPedia, 21 Feb 2014: Ransomware like CryptoLocker, which encrypts precious files and holds them that way until a ransom is paid, is becoming more and more common. However, not all threats are as difficult to beat as CryptoLocker. A couple of French security researchers who work for Airbus, Fabien Perigaud and Cedric Pernet, have come across a new piece of ransomware dubbed BitCrypt. They analyzed the malware after it infected a computer belonging to one of their friends and encrypted all the pictures of his children. Since he had no backups, the only solution was to pay the 0.4 Bitcoin ransom or try to decrypt the files. After analyzing the ransomware, Perigaud and Pernet found that the developer had made a big mistake. He wanted to generate a 128-byte key (1024 bits), but instead generated a 128-digit number, which is the equivalent of only 426 bits. While RSA-1024 bit encryption is not easily breakable with standard computers, the 426-bit key was cracked in 43 hours on a regular quad-core PC. The cado-nfs tool has been used to obtain the encryption key. The experts have also published a Python script that's designed to restore the encrypted files. Additional technical details are available on the Cassidian Cybersecurity blog [**LINK**]. To read more click **HERE**

Churches of Scotland and Cyprus Targeted by Muslim Hackers

SoftPedia, 21 Feb 2014: Muslim hackers have launched a campaign against Christianity. Over the past couple of days, SeCuRiTy_511, a hacktivist from Saudi Arabia, has breached the websites of the Church of Scotland and the Church of Cyprus. User data has been leaked from both websites. According to Cyber War News, from the website of the Church of Cyprus (churchofcyprus.org.cy), the hacker has leaked the names, email addresses, and password hashes of around 1,400 users. The credentials for administrator accounts have also been leaked. From the databases of the Church of Scotland (churchofscotland.org.uk), the hacker has taken the details of 1,570 users and 9 administrators. The information was published on Pastebin. Both files are still available at the time of writing. Syrian hacktivist Dr.Sha6h has also targeted some websites, not all of them related to Christianity, as part of this campaign. He mainly focuses on websites in Denmark. That's because the country's government has banned the slaughter of animals, arguing that animal rights come before religion. The news hasn't been taken well by Muslims and Jews. To read more click **HERE**

Unknown Threats, a Top Security Concern Only for 37% of Global Organizations

SoftPedia, 20 Feb 2014: Dell has published a new whitepaper called "Protecting the organization against the unknown – A new generation of threats." The study shows that, while trends and technologies such as cloud computing, mobility, bring-your-own-device (BYOD), and Internet usage bring with them a lot of risks, only 37% of global organizations see unknown threats as a top security concern in the next 5 years. The numbers from the report show that 64% of respondents agree that IT processes will have to be reorganized or restructured, and collaboration between IT and other departments will need to be enhanced to stay ahead of emerging threats. Close to 90% believe the government should become involved in determining an organization's cyber defense strategies. The main problem with unknown threats is that they come from both inside and outside the organization. Companies don't need to worry only about external cybercriminals, but also about internal attacks, whether they're carried out by malicious actors or accidentally. 67% of the respondents revealed that they increased education and training funding in the past 12 months. Security training for employees is considered a priority in half of organizations. Monitoring services have also been increased over the past years – by 54% globally and by 72% in the United States. "Traditional security solutions can defend against malware and known vulnerabilities, but are generally ineffective in this new era of stealthy, unknown threats from both outside and inside the organization," said Matt Medeiros, vice president and general manager of Dell Security Products. "These

threats evade detection, bypass security controls, and wreak havoc on an organization's network, applications, and data, but despite these dangers, our study found, among those surveyed, organizations are just not prepared," Medeiros added. "There is still a disturbing lack of understanding and awareness of the type of impact and detriment caused by the unknown threats that can come from both sides of an organization's data flow. "As a result, we believe a new security approach is needed – one that's embedded in the fabric of software, governing access to every application and protecting every device, both inside and outside a corporate network." 1,440 IT decision makers from organizations with over 500 employees or end users have taken part in the study conducted between October and November 2013. The respondents are from the US, Canada, the UK, Germany, France, Italy, India, Spain, Australia, and Beijing. The complete whitepaper [**LINK**] is available on Dell's website. You can also check out an infographic that sums up the company's findings. To read more click **HERE**

Adobe Flash Player 12.0.0.70 Released for Download
SoftPedia, 20 Feb 2014: Adobe has just launched a new version of Flash Player, so all users are strongly recommended to update the app as soon as possible to make sure that all bugs are fixed. The parent company hasn't yet provided any release notes on this fresh build, but it's safe to assume that Adobe Flash Player 12.0.0.70 is very likely to come with bug fixes and performance improvements, so a slight improvement is very likely to be spotted after the update. Of course, Flash Player is available on all platforms, which means that all users should get it very fast especially if they've been experiencing issues with the previous builds. Overall, there's no doubt that this is a necessary update for everyone, so download Adobe Flash Player 12.0.0.70 right now to make sure that all bugs are fixed. To read more click **HERE**

Card Data Stolen in Target Breach Sold at Discount Prices
Softpedia, 20 Feb 2014: Brian Krebs says the payment card data stolen by cybercriminals from the US retailer Target is being sold at low prices compared to the period when the information first emerged on underground markets. That's because the number of valid cards is dropping quickly. According to the expert, shortly after the breach came to light, cards were being sold for between $26.60 and $44.80 per card on the Rescator.so website. Now, prices ranges between $8 and $28. When the data was first put up for sale, cards had a 100% validity rate. That meant all of them could be used for fraudulent transactions. Now, the validity rate has dropped to 60%. Many companies have rushed to replace impacted cards, so it's becoming more and more difficult for fraudsters to find data that they can put to good use. On the other hand, Krebs has learned that there are some organizations that still haven't replaced many of the cards. These cards have either been reissued just before the Target breach, or they're about to expire in the next month or so. To read more click **HERE**

10 Cyber Security Awareness Tips for Users Impacted by Forbes and Kickstarter Breaches
SoftPedia, 19 Feb 2014

The details of a large number of individuals have been compromised in the recent data breaches suffered by Forbes and Kickstarter. Since this is a perfect time to remind users of best cyber security practices, we've asked Bill Carey, VP of marketing at Siber Systems, the maker of the RoboForm password manager, to provide our readers with some tips. Here are the top 10 cyber security awareness tips shared by the expert:

1. Regularly update software to eliminate security weaknesses. Windows, Macs, and all browsers regularly provide free software updates; take advantage of this to close security loopholes.
2. When you're done with using a website, log off and close your browser. This will prevent others from gaining access to your account.
3. Create passwords with combinations of upper and lowercase letters, numbers and special characters.

4. Don't use personal information in your password, such as your name, your partner's name, your child's name, your occupation, telephone number, birth date, etc.
5. Small businesses have to hold their employees accountable for their security. Employees must adopt safe security habits to keep their information and the company's information protected. Consider putting a formal cyber-security policy into effect.
6. Make sure that you use a PIN or #password on your mobile phone.
7. Use the 'Keystroke' method for making passwords. Choose a password and create a keyboard mapping system. One key to the left and one up would make the password "tinmen" change to "47gh2g."
8. Disable pictures on your email and read it in plain text. The sender will not be able to identify if you've opened the email.
9. Don't keep a record or list of your passwords in unencrypted files on your computer or phone.
10. Have a disposable e-mail address. Only give your actual e-mail address out to people who need it. This will avoid mass spam and keep your inbox clean.

To read more click **HERE**

Las Vegas Sands Says It's Analyzing the 11-Minute Video Published by Hackers

SoftPedia, Feb 19, 2014: Shortly after Las Vegas Sands Corp, one of the world's largest casino operators, announced that its websites had been restored, the hackers that attacked the company's systems published a video to demonstrate that they had gained access to a lot of information – over 800 GB, to be more precise. The company's representatives say they're still analyzing the video (removed from YouTube for policy violations), but they admit that the extent of the breach is bigger than initially believed, The Associated Press reports. Las Vegas Sands has been aware that some employee information has been compromised. However, the video suggests that even passwords for slot machines and player information at the Bethlehem casino have been stolen by the attackers. The incident is being investigated by the FBI, Secret Service and Nevada Gaming Control Board, but none of the organizations has commented on the matter. The casino operator became a target after the company's CEO, Sheldon Adelson made a comment about the US dropping a nuclear bomb on Iran. The hackers threaten that it will "end in tears" for Sheldon and others who talk like him. To read more click **HERE**