THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

29 August 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

August 28, IDG News Service – (International) **FBI, Secret Service studying 'scope' of reported bank cyberattacks.** A spokesperson for the FBI stated August 27 that the FBI and U.S. Secret Service are investigating to determine the scope of recently reported cyberattacks against several major U.S. financial services institutions. Source: http://www.networkworld.com/article/2599961/fbi-secret-service-studying-scope-of-reported-bank-cyberattacks.html

August 27, SC Magazine – (National) **Ground system for weather satellites contains thousands of 'high-risk' bugs.** The National Oceanic and Atmospheric Administration (NOAA) was urged by the U.S. Department of Commerce Office of Inspector General in an August 21 memo to quickly patch several high-risk vulnerabilities in the Joint Polar Satellite System (JPSS) ground system after an audit found 23,868 vulnerabilities in the JPSS ground system for the second quarter of the fiscal year 2014. NOAA initiated a system update process in order to patch the vulnerabilities. Source: http://www.scmagazine.com/ground-system-for-weather-satellites-contains-thousands-of-high-risk-bugs/article/368479/

August 28, Computerworld – (International) **Microsoft purges 1,500 copycat, fraudulent Windows 8.1 apps.** Microsoft stated August 27 that it removed over 1,500 fake Windows 8 and 8.1 apps from its Windows Store marketplace due to the apps attempting to charge users for free software. Source: http://www.networkworld.com/article/2599810/windows-apps/microsoft-purges-1-500-copycat-fraudulent-windows-8-1-apps.html

August 27, The Register – (International) **Scratched PC-dispatch patch patched, hatched in batch rematch.** Microsoft released an updated version of a security patch following reports that some users experienced 'blue screen of death' crashes after applying the original patch. Source: http://www.theregister.co.uk/2014/08/27/microsoft_reissues_security_patch/

August 27, Softpedia – (International) **Crypto-malware steals email addresses and passwords, spreads itself.** Avast researchers analyzed a new piece of ransomware that uses several freely available tools to infect users, encrypt files, and demand a ransom. The ransomware also steals email credentials to attempt to propagate itself and is currently targeting users in Russian-speaking countries. Source: http://news.softpedia.com/news/Crypto-Malware-Steals-Email-and-Passwords-Spreads-Itself-456658.shtml

CryptoWall Infects 625,000 Systems in About Six Months
Softpedia, 29 aug 2014: Relying on multiple infection vectors, Cryptowall managed to achieve wider presence than the infamous CryptoLocker, affecting 625,000 systems across the world in a period of about five and a half months. Recorded by Dell SecureWorks Counter Threat Unit (CTU), most of these infections were traced in the United States because of the numerous malicious campaigns targeting English-speaking users. The security researchers say that the total number of files encrypted by CryptoWall in the monitored timeframe (mid-March until August 24, 2014) amounted to 5.25 billion files. CryptoWall has been seen being distributed through various methods, from drive-by downloads to exploit kits and spam campaigns. By sinkholing one domain used as a backup command and control server by the attackers, CTU could observe that 40.6% of the infected machines

were located in the US, accounting for 253,521 of the total number. Far on the second place was Vietnam, with 66,590 machines infected (10.7%), followed by the United Kingdom, recording 6.4% of the infections (40,258). Other countries affected include Canada (32,579), India (22,582), Australia, (19,562), France (13,005), Germany (12,826) and Turkey (9,488). The threat actors behind CryptoWall are organized and use identification codes for each sample, representing the malicious campaign that distributed them. According to the researchers, five campaigns distributing the ransomware are currently in use, relying on the spam spewing the Cutwail botnet, Gozi/Neverquest and Magnitude exploit kit. At the beginning, CryptoWall would pretend to be CryptoLocker, but its simpler architecture did not fool security researchers who quickly noticed that it was a different threat. However, after CryptoLocker was taken down back in June this year, CryptoWall took its place as the most prevalent crypto-malware and even managed to cause more infections across the globe. Despite compromising 100,000 computers more than CryptoLocker, CryptoWall caused smaller financial damage, collecting only "37% of the total ransoms collected by CryptoLocker." Contributing to its smaller success may be the fact that the operators behind it do not have highly organized "cash-out" and laundering services as those handling CryptoLocker. "In mid-March 2014, CryptoWall emerged as the leading file-encrypting ransomware threat. The threat actors behind this malware have several years of successful cybercrime experience and have demonstrated a diversity of distribution methods. As a result, CTU researchers expect this threat will continue to grow," says the report from Dell SecureWorks. The ransomware starts locking the data on the compromised computer after retrieving the RSA public key from the command and control (C&C) server; blocking communication to this location results in failure of the encryption process. The researchers reported that from the 625,000 infections recorded over the monitored period, only 1,683 victims paid the ransom, increasing the profits of the cybercriminals by more than $1.1 million. The lowest ransom was $200 and it was paid six times. However, most of the victims paid the $500 ransom, and the security researchers also saw that one person made a $10,000 payment to the crooks. To read more click **HERE**

Microsoft to Kill MSN Service in China

Softpedia, 29 Aug 2014: Although it's still the subject of an anti-trust probe in China, Microsoft started notifying customers in the country that the MSN service would be shut down in October, one year and a half after the same thing happened in the rest of the world. As local publication Dongfang Daily reports, the software giant is now sending emails to all MSN Messenger users to notify them about the change, recommending everyone to switch to Skype before this deadline comes. Microsoft officially retired MSN and Windows Live Messenger in the entire world, except China, in April 2013, moving all accounts to Skype and providing a new modern way of communications over the Internet. Redmond offered MSN to Chinese users through a partnership with local tech company TOM Group, but once the deal came to an end, Microsoft decided not to renew it, most likely amid plans to pull the plug on the service. In China however, these services are getting the axe in October, and according to the email sent to users, Microsoft is also offering a $2 Skype coupon for international calls through the app. In the meantime, Microsoft is still trying to solve its issues with the Chinese government, as local authorities are investigating the firm for a possible anti-trust violation with Internet Explorer and Windows Media Player. In May this year, China banned Windows 8 on government computers, with sources close to the matter revealing that it all happened because local officials were afraid that Microsoft might be using the operating system to access state secrets and send them to US intelligence agencies. Redmond has always denied such claims and expressed its intention to work with Chinese authorities upon addressing the complaints, offering instead Windows 7 until the government lifts Windows 8's ban in the country. More recently, anti-trust regulators have revealed that Microsoft is indeed cooperating on the case, but have shown that one of the reasons for the investigation is the way the company is bundling Internet Explorer and Windows Media Player in its Windows operating system. Similar issues have also been experienced in Europe, where Microsoft has actually got fined, but China is only now looking into the matter. Microsoft is not the only company that's involved in anti-trust probes in China, as some other large companies, including Qualcomm and German car manufacturer Daimler, are also said to be facing similar issues after being investigated by the central government for possible breaches of competition rules. To read more click **HERE**

Dairy Queen Confirms Breach of Payment Systems

SoftPedia, 29 Aug 2014: Fast food restaurant Dairy Queen has confirmed that systems in some of their locations have been infected with malware that puts at risk credit and debit card data of customers of the retail chain. The company has been alerted by the US Secret Service that its systems were affected by a piece of PoS malware also found in hundreds of other retail intrusions. This suggests that Backoff PoS malware is at fault, since this is the threat that has been announced in an advisory from the Department of Homeland Security (DHS) to impact more than 1,000 businesses in recent attacks. The company said in a statement to the Business Journal that "customer data at a limited number of stores may be at risk" and that the affected franchised locations had been notified along with the credit card processors and credit card companies in order to collect relevant information about the incident. At the moment, there is no information about the number of stores impacted, or the number of customers whose data has been exposed. The intrusion disclosure follows a report earlier this week from security blogger Brian Krebs, who learned from several financial institutions that fraud on cards used at half a dozen Dairy Queen (DQ) locations had been detected. Krebs contacted company representative Dean Peters to ask for details, but was informed that no card fraud reports had been received at individual DQ stores, stressing "that nearly all of Dairy Queen stores were independently owned and operated." Furthermore, even if a breach or any other problem was detected, Peters said that the franchisees are not required to notify the company. To read more click **HERE**

Cyber Attacks Aim at Oil and Energy Sector Businesses in Norway

SoftPedia, 29 Aug 2014: A flurry of cyber-attacks directed at companies in the energy and oil sector have been detected by the National Security Authority (NSM) in Norway, causing the release of an alert regarding attempts of stealing information. The organization, which is a cross-sectoral professional and supervisory authority within the protective security services in Norway, says that more than 50 attempts have been uncovered recently. As such, advisories have been sent to companies, in order to impose security measures designed to thwart the attacks. According to NSM, the perpetrators send emails with infected attachments to gain unauthorized access to the computer and the company's assets. These notifications have reached 300 organizations. The purpose is to create awareness and have the businesses test how vulnerable they are against this type of attacks. It is recommended to apply the latest updates for the operating system and software installed on their systems, as well as to restrict elevated privileges to administrators. The authority also advises the use of strong passwords coupled with a two-factor authentication mechanism. Enabling system activity logging also comes in handy for detecting suspicious actions on the system. As far as employees are concerned, checking the legitimacy of email senders is one of the best practices to be adopted. To read more click **HERE**

Australian Federal Police Accidentally Discloses Highly Sensitive Details

Softpedia, 29 Aug 2014: Confidential information from the Australian Federal Police (AFP) has been exposed to the public for several years because the organization failed to redact documents that were published online. The documents contained details about criminal investigations and communication interception operations, with the names of the subjects being detectable because of an improper electronic redaction process. The leak occurred because the AFP provided the details to the Senate without obfuscating the classified text strings; the Senate then published the documents in their unaltered form on parliamentary websites, where they could be accessed for years. According to The Guardian, the law enforcement agency along with the federal government are trying to implement a mandatory data scheme that would constrain telecommunication businesses to store personal data acquired from phone and web users. It appears that the documents leaked online comprised not only the names of investigation targets, but also the offenses under the AFP scope and identification details like addresses and phone numbers. The ASP reported the leak to the Australian Privacy Commissioner and the documents were taken offline. It is unclear if this information managed to tip off any of the subjects of investigations. According to the Privacy Act, organizations holding personal information about individuals are obligated to take all the measures to protect it and avoid unauthorized access to it. To read more click **HERE**

Over 677,000 Racing Post Accounts Compromised in 2013 Breach

Softpedia, 29 Aug 2014: An intrusion on the systems of Racing Post ended with a total of 677,335 registered customers having their accounts compromised and personal information stolen. The incident was possible because the company did not keep the security patches for the website's software updated, as per the investigation carried out by the Information Commissioner's Office (ICO); this offered the hackers the possibility to leverage a vulnerability and run an SQL injection attack on its website (racingpost.com). As a result, a database containing customer's names, addresses, passwords, date of birth and telephone numbers was stolen by the hackers. ICO determined that the last security audit was carried out by the company way back, in 2007, and no security patches were applied after this date. "The Racing Post pulled up short when it came to protecting their customers' information by failing to keep their IT systems up-to-date. This data breach should act as a warning to all businesses that poor IT security practices are providing an open invitation to your customers' details," said Stephen Eckersley, ICO head of enforcement. The company signed a commitment to improve security practices for its website by February 28, 2015, through introducing routine verifications and making sure that updates are applied regularly. This is actually ICO showing leniency towards the incident since no financial information was compromised. However, email addresses and phone numbers are coveted assets for cybercriminals, who can use them for digging up more information about their owners. To read more click **HERE**