THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

11 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 7, Miami Herald – (Florida) **TotalBank responds to computer security breach.** Miami-based TotalBank notified 72,500 customers after an investigation revealed that unauthorized individuals may have accessed the bank's systems and obtained customer names, account numbers, addresses, account balances, and other personal information. The bank stated that it took action to secure its systems and is continuing to investigate. Source: http://www.miamiherald.com/2014/08/07/4277318/totalbank-responds-to-computer.html

August 7, IDG News Service – (International) **Some mobile POS devices still affected by critical flaws months after patch.** A researcher with MWR InfoSecurity and a colleague presenting at the Black Hat 2014 conference detailed how flaws in mobile point of sale (mPOS) devices from several manufacturers may be vulnerable to being taken over by attackers using customized smart cards in order to steal the payment card information read by the devices. The researchers reported the flaws previously and a patch for the EMV library was released in April, but some vendors have yet to push out the update to their devices, leaving the devices vulnerable. Source: http://www.networkworld.com/article/2463081/security/some-mobile-pos-devices-still-affected-by-critical-flaws-months-after-patch.html

August 8, Softpedia – (International) **Network access storage devices are highly exploitable.** A researcher from Independent Security Evaluators presenting at the Black Hat 2014 conference reported finding a wide variety of vulnerabilities in network access storage (NAS) devices from several manufacturers, including directory traversal, command injection, memory corruption, authentication bypass, or back door vulnerabilities. Source: http://news.softpedia.com/news/Network-Access-Storage-Devices-Are-Highly-Exploitable-454103.shtml

August 8, Help Net Security – (International) **Critical bug in WordPress plugin allows site hijacking.** Sucuri researchers identified and reported a vulnerability in the Custom Contact Forms plugin for WordPress that could allow attackers to take control of sites using the plugin. The developers of Custom Contact Forms published an update for the plugin after the issue was published by the WordPress Security team. Source: http://www.net-security.org/secworld.php?id=17227

August 8, Help Net Security – (International) **Two Gameover Zeus variants targeting Europe and beyond.** Researchers at Bitdefender identified two Gameover Zeus variants in the wild, one botnet primarily targeting the U.S. while the second targets Belarus and Ukraine. The first botnet is generating around 1,000 domains per day while the second generates 10,000 per day but appears to currently be inactive. Source: http://www.net-security.org/malware_news.php?id=2833

August 8, Securityweek – (International) **Cybercriminals steal cryptocurrency via BGP hijacking.** Researchers with Dell SecureWorks reported finding cybercriminals using fake Border Gateway Protocol (BGP) broadcasts to redirect traffic from cryptocurrency mining pools to servers they control, diverting tens of thousands of dollars in cryptocurrency. The attackers compromised 51 mining pools hosted on 19 hosting companies. Source: http://www.securityweek.com/cybercriminals-steal-cryptocurrency-bgp-hijacking

August 7, Securityweek – (International) **Attackers used multiple zero-days to hit spy agencies in cyber-espionage campaign.** Kaspersky Lab researchers identified the infection methods used in the Epic Turla cyber-espionage campaign (also known as Snake or Uroburos) that targeted intelligence agencies, military organizations, government agencies, education institutions, pharmaceutical companies, and research groups in over 45 countries. The attackers behind the campaign used several malware platforms and zero-day exploits in Windows XP and Server 2003 and Adobe Reader to infect systems and then could upgrade the malware with additional capabilities once in place. Source: http://www.securityweek.com/attackers-used-multiple-zero-days-hit-spy-agencies-cyber-espionage-campaign

August 7, Dark Reading – (International) **Attack harbors malware in images.** A researcher with Dell SecureWorks reported finding the Lurk malware being distributed within a fake digital image as part of a click fraud campaign that infected around 350,000 systems. The malware in the campaign was spread through iFrames on Web sites containing an Adobe Flash exploit, and required victims to have a vulnerable version of Adobe Flash that is used to download the fake image file, which contains an encrypted URL that downloads a second malicious payload. Source: http://www.darkreading.com/endpoint/attack-harbors-malware-in-images/d/d-id/1297867

August 7, Securityweek – (International) **Flaws in email and Web filtering solutions expose organizations to attacks: Researcher.** A researcher at NCC Group presenting at the Black Hat 2014 conference published two whitepapers outlining how email and Web filtering solutions can be used by attackers in the reconnaissance phase of attacks to obtain information on a potential target network if the attackers can determine which products or services are being used on the target network. Source: http://www.securityweek.com/flaws-email-and-web-filtering-solutions-expose-organizations-attacks-researcher

August 8, The Register – (International) **'Up to two BEEELLION' mobes easily hacked by evil base station.** Researchers from the security firm Accuvant announced at the Black Hat 2014 conference August 7 that up to 2 billion smartphone handsets are at risk for over the air hijacking and abuse which can be exploited through the Open Mobile Alliance Device Management (OMA-DM) protocol, used by approximately 100 mobile phone manufacturers. To access the handsets remotely the hacker only needs to know the handset's unique International Mobile Station Equipment Identity (IMEI) number and a secret token. Source: http://www.theregister.co.uk/2014/08/08/two_billeeon_mobile_phones_easily_hackable_with_dummy_base_station/

Russia Tightens Control over Internet, Bans Anonymous WiFi Access, Spies on Social Media
SoftPedia, 11 Aug 2014: Russia has taken yet another step to block off any attempt to be anonymous on the Internet as the country decided to ban anonymous access to WiFi. According to news agency Itar Tass, Prime Minister Dmitry Medvedev has signed an order that bans anonymous access to the Internet in locations that offer WiFi connections, such as restaurants and other public spaces. Instead, operators will have to identify users with a full name which needs to be confirmed by an ID. Hardware also needs to be identified, although there's no specific explanation about what this would entail. In recent months, Russian officials have taken a new stance towards the Internet, where anonymity is seen as a bad thing. The government has even offered a really small money prize for anyone who finds a way to de-anonymize the Tor network. Another controversial move has been the one forcing bloggers with more than 3,000 visitors per day to register with the authorities, effectively forcing them to act as if they're a media organization, including by refraining from bashing politicians, double checking information, refraining from publishing information that can be considered as hate speech or a call to extremism and so on. Even worse is perhaps the fact that the Russian secret service has taken it upon itself to spy on social media. On August 1, a new law came into effect, allowing the Federal Security Service (FSB) to keep tabs on people's online presence. Social network platforms in Russia need to install hardware and software which

allows the secret services to access users' personal information, RT reports. This is a grave violation of privacy, but users aren't that surprised even though they are annoyed with the new law meant to control their online lives. After all, some said, the US does more or less the same way. Internet companies, such as Yandex and Mail.ru were, however, surprised with the move, although there's little they can do now but comply. It is currently unclear how the law will be implemented, but it is obvious that anyone using Russian social networks are soon going to be under the watchful eye of the country's secret service. Since the entire thing is sanctioned by law, there's nothing people can do other than complain about it. Unlike in the United States where reform is being planned to force the NSA to stop using legal loops in old laws, Russia gave itself permission to spy out in the open. To read more click **HERE**

Cybercrime Ring's Collection of 1.2 Billion Unique Credentials Likely to Be Real, Here's Why

SoftPedia, 11 Aug 2014: On Tuesday, an announcement from Hold Security informed that a single group of cybercriminals, who the company named CyberVor, had amassed as many as 4.5 billion records containing email addresses and account passwords. After eliminating the duplicates, the company said that only 1.2 billion credentials (usernames - which are generally emails and passwords) appeared to be unique and were linked to more than 500 million email addresses. All this information had been comprised from the databases of more than 420,000 websites and FTP locations, over a longer period of time; Hold Security spent more than seven months of research until they identified the gang in possession of the massive amount of data. Maybe because these numbers are so frightening, media online started to dissect the details provided by Hold Security in an attempt to dismiss the news as a lie and an attempt from the company to promote its services to both users and businesses. Advertising their services, especially ahead of the most popular part Black Hat USA in Las Vegas this year, sure seems like a business move, but making their products known to a large audience is what companies do to keep playing the game and move up to the next level. Although the amount of the collected data may sound blown out of proportion for many users, the truth is that cybercriminal rings are getting better and better at extracting information from online locations, while website administrators are not too quick at applying the latest patches and fixes that would protect their assets (one recent example would be the thousands of websites hacked through the unpatched MailPoet vulnerability). Furthermore, to create such a large database, CyberVor started by buying credentials on the black market, and used them in attacks on services that gathered large crowds of users (email providers, social media sites). They used various methods, and the latest they relied on was data gathering by botnets, infected computers controlled by cybercriminals; these would be leveraged to test for SQL injection vulnerabilities on every website visited by the owner of the compromised systems. According to Hold Security numbers, more than 420,000 were discovered vulnerable to this type of attack. Simple math would tell us that CyberVor would have to steal an estimated average of 2,850 unique credentials from each of them, and this is without deducting the records collected through other means; overall, the figure rises to 10,700 per site. Robert Capps, senior director of customer success at RedSeal Networks, a company offering end-to-end network visibility and analytics to prevent cyber-attacks, told us via email that, "while the current disclosure is unsettling for consumers, security professionals have long believed that cybercriminals were combining stolen consumer data from multiple breaches, to make their attacks more effective. This confirms their suspicions." What should be impressive is not the number of credentials in the hands of cybercriminals, but the fact that one single group has them. However, let us remember that the Target breach last year ended with information about up to 110 million customers falling into the wrong hands, 40 million records containing credit and debit card information, which benefits from increased security. About the CyberVor database, Adam Kujawa, head of Malware Intelligence at Malwarebytes, said that "the scale of this find reflects our current reality. While many cyber-criminal groups might not be holding on to billions of login credentials at one time as in this case, they grab information, either use it for their own purposes or sell it to the highest bidder." They are creative enough to find a way to make money even if they cannot use the stolen information themselves. "Phishing attacks, malware and poor password security allow these attackers to obtain the most from their efforts. This is only an instance of finding a lot of credentials collected in one place but if you put it up against the numbers that are currently circulating through the underground

markets, it would seem small," he added via email. However, there are several things to bear in mind regarding Hold Security's report, and that is that although CyberVor holds 1.2 billion unique username and password pairs, not all of these can actually be used for nefarious activities. What needs to be taken into consideration is that some users rely on disposable email addresses to create an account from a service without having to deal with notifications from them. Of course, it is very likely that this would account for a very small proportion of the 1.2 billion credentials. A stronger possibility is that many users have adopted good password security practices and change the countersigns for the most important services on a regular basis; this won't save them from spam or phishing, though, which is exactly the business CyberVor appears to be in (Alex Holden told the New York Times that the ring collects fees from other groups for sending out spam). Also to be considered is the fact that, in some cases, the database information might be encrypted and the cybercriminals may not be able to crack the cipher. "If this crime ring has company credentials then many of those credentials eventually will become stale as employees are terminated or accounts passwords are changed by the user," Joe Schumacher, security consultant for Neohapsis, told us. As far as the authenticity of the information is concerned, some security experts (an unknown source for the New York Times and security blogger Brian Krebs), who have been shown the data discovered by Hold Security's research, say that the details are for real. To read more click **HERE**

Oracle Data Redaction Service Vulnerable to Trivial Bypassing

SoftPedia, 11 Aug 2014: The data redaction feature, designed for selective, real-time protection of certain database information can be bypassed without too much effort, according to security expert David Litchfield. Employed at Datacomm TSS and recognized authority on database security, Litchfield held a presentation called "Oracle Data Redaction Is Broken" at the DefCon hacker convention last week. He informed the audience that the service supposed to prevent sensitive information from reaching SQL query results does not require complicated methods for being defeated in order to launch privilege escalation attacks. During his demonstration, he showed how a remote attacker could achieve the necessary privilege for accessing the redacted information by injecting some SQL queries, as per The Register. In the paper disclosing some of his findings, the security expert says that privilege escalation can also be obtained using DBMS_REDACT: "Anyone with the privileges to execute DBMS_REDACT can create redaction policies on any table in any schema except the SYS schema. As such an attacker can execute code as that user by passing a nefarious function in the "EXPRESSION" clause of DBMS_REDACT. When that owner next queries the table the attacker's function will execute." At the convention, Litchfield said that Oracle had a slow patching process and that they would also issue broken or incomplete fixes. According to The Register, he told the DefCon audience that patching the code is the preferred method of Oracle engineers, rather than providing a repair for a fundamental flaw. To read more click **HERE**

Twitter Account for Yahoo News Gets Hacked, Sends Tweet About Ebola Outbreak

SoftPedia, 11 Aug 2014: We all know that Yahoo is prone to fail sometimes, especially when it comes to the uptime of its services, but it seems that this time around it wasn't exactly its fault when it scared the world on Sunday. In a tweet that has now been deleted, Yahoo News delivered the chilling news that there's been an Ebola outbreak in Atlanta and that there were about 145 people infected so far after doctors carrying the disease were flown in from Africa. The message got about 900 retweets and some 125 favorites before it was taken down. The tweet was obviously not real and it seems that the company's Twitter account was hacked. Some 15 minutes later, Yahoo came forth and apologized, saying that "an unauthorized tweet with misinformation on Ebola was sent from this account," and it asked people to "please disregard" it. The tweeted message from the hacker was deleted afterwards, but not before making a few waves. Fellow Twitter users were making fun of the company, saying that Yahoo News finally changed its password from "yahoo123." The Yahoo News account has over 816,000 followers and has sent over 72,400 tweets since joining back in July 2007. Hopefully, Yahoo will, from now, keep a closer eye on its Twitter account and maybe enable two-step verification. To read more click **HERE**