THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

16 July 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

July 15, IDG News Service – (International) **Critical design flaw in Microsoft's Active Directory could allow password change.** Researchers with Aorato identified a flaw within Microsoft's Active Directory which could allow attackers to change a victim's password and use the new password to access a company's network and enterprise functions. The vulnerability relies on the older NTLM authentication protocol to perform a "pass-the-hash" attack to gain access. Source: http://www.pcworld.com/article/2454103/critical-design-flaw-in-active-directory-could-allow-for-a-password-change.html

July 15, Help Net Security – (International) **Amazon-based malware triples in 6 months.** Solutionary released an analysis of Internet service providers (ISPs) and hosting providers hosting malware and found that Amazon was the top malware-hosting ISP, with a 250 per cent increase during the second quarter of 2014, among other findings. Source: http://www.net-security.org/malware_news.php?id=2808

July 15, Softpedia – (International) **Google's Dropcam monitoring device open for video hijacking.** Researchers with Synack found that the Google Dropcam home monitoring cameras contain vulnerabilities which could allow the camera's video and sound content to be intercepted by attackers. The vulnerabilities stem from an old version of OpenSSL that is vulnerable to the Heartbleed flaw and other issues, and from an old version of BusyBox that contains exploitable flaws. Source: http://news.softpedia.com/news/Google-s-Dropcam-Monitoring-Device-Open-for-Video-Hijacking-450737.shtml

July 15, Help Net Security – (International) **CNET attacked by Russian hackers, user database stolen.** CBS Interactive confirmed that media Web site CNET was compromised after attackers claiming affiliation with the Russian hacker group W0rm stated that they were able to obtain databases containing usernames, emails, and encrypted passwords for over 1 million users. The attackers stated that they used a flaw in the site's implementation of the Symfony PHP framework and claimed that the attack was performed for security demonstration purposes and the information would not be sold. Source: http://www.net-security.org/secworld.php?id=17117

July 14, The Register – (International) **Gameover ZeuS botnet pulls dripping stake from heart, staggers back from the UNDEAD.** Sophos researchers reported that a new variant of the GameOver Zeus trojan is being used to re-establish a botnet 6 weeks after an international law enforcement effort disrupted the original botnet used for banking credential theft and the distribution of the CryptoLocker ransomware. Source: http://www.theregister.co.uk/2014/07/14/gameover_zeus_botnet_back/

This Hotel Will Put a Surface Pro Tablet in Every Guest Room
SoftPedia, 16 Jul 2014: It was only a matter of time, but it's finally happening: hotels across the world have started offering guests Surface tablets to get easier access to hotel services, such as room service and laundry. Microsoft today announced a deal with the Mandarin Oriental Hotel Group, which agreed to put Surface Pro tablets in guest rooms of four of its hotels, namely those in London, Washington DC, Las Vegas, and Tokyo. These tablets will have a custom lock screen and apps that would allow guests to benefit from easier servicing

while staying at the hotel. "As a brand known for our legendary hospitality, we're always pushing ourselves to create unique, premium guest experiences," said Monika Nerger, CIO of Mandarin Oriental. "We are currently operating in 25 countries, and with our expansion into new markets we needed a powerful, secure, yet easy-to-manage solution with robust language support, which Microsoft technologies can offer. Through this partnership we can create digital experiences that cater to our guests' needs and expectations whenever they stay with us." Microsoft says that so far everything goes according to the plan and the early feedback collected by the hotel shows that guests are actually finding these tablets very helpful. As a result, the Mandarin Oriental Hotel Group will soon start a new pilot program that would include an additional 1,000 tablets, including the new Surface Pro 3. Microsoft says that this is going to happen in the near future, so if you're staying at one of the aforementioned hotels, don't be too surprised if you find Redmond's new-generation tablet in your room. What's interesting is that guests are also allowed to log in with their own Microsoft accounts and get emails and access personal files stored on OneDrive. When the checkout is officially processed, the device is automatically wiped clean of personal guest data and the original data, with hotel information and apps, is restored to make sure that the next guest is provided with the same experience. "Through the Microsoft platform, we have a bespoke digital experience that allows guests to easily place a complex meal order and request other guest services with a touch of the finger," Nerger said. "Early feedback from our guests has been extremely positive, and we will continue to tailor the solution as we extend the tablet deployment to more of our markets, with an initial target installation of 1,000 tablets across the portfolio in the near future." To read more click **HERE**

Hamas Hacks Israel's Channel 10 TV Station

SoftPedia, 16 Jul 2014: The satellite communication of the Channel 10 TV station in Israel has been hijacked for a few minutes on Monday by the military wing of the Hamas organization. It appears that responsible for the incident were the Izz al-Din al-Qassam Brigades, who managed to take over the satellite broadcast of the TV station and feed the tuned in viewers images of wounded people from Israeli air-strikes on Gaza area. They also broadcast a message saying that retaliating actions would be deployed if the government did not put a stop to the campaign. "Your government chose the opening hour of this campaign. If your government does not agree to our terms, then prepare yourself for an extended stay in shelters," read the message that was displayed along with the images of the wounded. Since they hijacked the satellite transmission, viewers receiving the station through digital converters were not exposed to the incident. This is not the first time Channel 10's broadcast has fallen into the hands of Hamas; Israel National News reports that back in 2012 a similar attack, which also affected Channel 2, occurred during Operation Pillar of Defense, an 8-day military operation of the Israel Defense Forces on the Gaza Strip. A short video of the live broadcast takeover has been published online. To read more click **HERE**

vBulletin Exploitable Through SQL Injection

SoftPedia, 16 Jul 2014: The developers of popular forum software vBulletin are currently working on releasing a fix for an SQL injection vulnerability discovered by members of the largest hacking community in Romania, Romanian Security Team (RST). The hackers discovered the glitch during routine security tests on their forum, which runs version 5.1.2 of vBulletin. Nytro, one of the hackers involved in the testing process, told us via email that they found an SQL syntax error message and discovered the troublesome query upon closer examination, with the forum software installed in debug mode. He says that the SQL injection is far from being complex, one of the queries not being properly sanitized. This offered the possibility to inject an SQL command, which allowed reading and extracting the details of all the admins without authorization. Armed with this information, a potential attacker could gain access to the administration panel and from there, to databases containing sensitive information (usernames, email addresses, passwords); they could even execute code by writing malicious PHP code, if write permission is enabled. Although SQL injection attacks are among the most trivial and widespread, exploits such as this one are worth a lot to cybercriminals, who can use this attack vector to gain access to sensitive information. On underground forums, a zero-day exploit could be sold for thousands of dollars. However,

Nytro told us that Romanian Security Team would not sell their finding. Instead, they disclosed it privately to vBulletin and will publish all the details as soon as a fix is released and is adopted by a larger crowd. They are not at their first disclosure of a vBulletin vulnerability. Back in April, this year, Romanian Security Team made a responsible disclosure of several cross-site scripting (XSS) flaws that allowed a potential attacker to insert arbitrary web script or HTML to various sections in the vBulletin forum. The set of vulnerabilities was identified as CVE-2014-3135. There are tens of thousands of websites relying on vBulletin for the forum section, and according to W3Techs, the software is one of the top choices for high-traffic websites. Not all the forums rely on version 5.x, though, which would limit the impact of the exploit. vBulletin is a proprietary cross-platform software written in PHP, and a new version is in development at the moment. Nytro said that the vBulletin response was prompt and he noticed that the issue has already been solved, a day after it was reported; fixes have not been released yet, but a new release with the necessary patches is expected to appear soon. The hackers published a video demonstrating the success of the SQL injection exploit, on both their forum and vBulletin's. You can check it below. To read more click **HERE**