The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

4 March 2014

March 1, Softpedia – (International) **Casino operator Las Vegas Sands admits hackers have stolen customer data.** Las Vegas Sands announced that cyberattacks which defaced some of its Web sites also compromised employee and customer data from its Sands Bethlehem casino in Bethlehem, Pennsylvania, potentially exposing credit card and bank account information, Social Security numbers, and other personal information. The company is continuing its investigation of the breach. Source: http://news.softpedia.com/news/Casino-Operator-Las-Vegas-Sands-Admits-Hackers-Stole-Customer-Data-430017.shtml

February 28, WMAQ 5 Chicago – (Illinois) **First American Bank reports data breach in Chicago taxis.** First American Bank announced that it has received reports of fraudulent charges after customers used taxis in Chicago that utilize two companies to process transactions. The bank is continuing to investigate the fraudulent transactions. Source: http://www.nbcchicago.com/news/local/First-American-Bank-Alleges-Data-Breach-from-Chicago-Taxis-247899551.html

February 28, IDG News Service – (International) **Gameover malware tougher to kill with new rootkit component.** Sophos researchers reported that a new variant of the Gameover banking malware that steals online banking credentials includes a kernel-level rootkit called Necurs that can make the malware more difficult to remove from infected systems. Source: http://www.networkworld.com/news/2014/022814-gameover-malware-tougher-to-kill-279308.html

March 1, Softpedia – (International) **Uroburos: Espionage rootkit allegedly created by Russian intelligence agency.** Researchers at G Data analyzed a sophisticated rootkit dubbed Uroburos that can compromise Windows systems in order to execute commands, steal files, capture traffic, and add new modules to itself. The researchers believe the rootkit was created by a Russian intelligence agency and has been in operation since 2011. Source: http://news.softpedia.com/news/Uroburos-Espionage-Rootkit-Allegedly-Created-by-Russian-Intelligence-Agency-430030.shtml

March 3, Softpedia – (International) **Meetup down for days due to DDoS attack allegedly ordered by a competitor.** Social networking portal Meetup was hit by a distributed denial of service (DDoS) attack beginning February 27 that took the portal's Web site offline for several days. An attacker contacted the company, claimed responsibility, and demanded a payment to end the attack. Source: http://news.softpedia.com/news/Meetup-com-Down-for-Days-Due-to-DDOS-Attack-Allegedly-Ordered-by-a-Competitor-430290.shtml

300,000 routers compromised in DNS hijacking campaign
Heise Security, 4 Mar 2014: Some 300,000 confirmed - but most likely many more - small office/home office (SOHO) routers have been compromised and their DNS settings changed to use two IP addresses in London, effectively allowing yet unknown attackers to perform Man-in-the-Middle attacks. "To date, we have identified over 300,000 devices, predominantly in Europe and Asia, which we believe have been compromised as part of this campaign, one which

dates back to at least mid-December of 2013," reported Team Cymru researchers, who spotted several affected TP-Link Wi-Fi routers in January and began investigating the matter. "The routers were both small office/home office (SOHO) class devices that provided Wi-Fi connectivity, local DNS, and DHCP services to customers, and were not using default passwords," they pointed out. But some of them were running a firmware version vulnerable to Cross-Site Request Forgery attacks, and at least one run firmware sporting a recently discovered flaw that allows attackers to download the device's configuration file which, of course, contains administrative credentials. The affected routers come from different manufacturers - the aforementioned TP-Link, D-Link, Micronet, and others - and they are predominantly located in Vietnam, India, Italy, Thailand, and Colombia, but also in Serbia, Ukraine, and Bosnia and Herzegovina. The interesting thing about this campaign is that it seems that currently the DNS requests sent to those two IP addresses are forwarded on to legitimate servers. "Attempts to log into local banking websites in affected countries, and to download software updates from Adobe and others all appeared to function normally, though many requests resolved noticeably slowly or failed to complete. Websites we tested also appeared to display normal advertising using these DNS servers," the researchers noted. So either this mass compromised is a preparation for later mischief, or the damage has already been done. Team Cymru researchers have noticed some similarities between this campaign and one other that was mostly limited to targeting customers of several Polish banks, but they concluded that "subtle differences in the tradecraft employed makes it likely that [they] are observing either separate campaigns by the same group, or multiple actors utilizing the same technique for different purposes." They also added that they don't believe that the also recently discovered Moon worm campaign targeting Linksys routers is mounted by the same attackers. The researchers have notified the authorities about this campaign, and also the manufacturers of the affected devices. Team Cymru spokesman Steve Santorelli shared with PC Pro that the two IP addresses to which the DNS requests are redirected are located on machines in the Netherlands, but are registered with UK-based company 3NT Solutions. This company's IP ranges have previously and repeatedly been associated with spammy sites. The researchers have shared helpful techniques for mitigating this type of attack in a whitepaper (**LINK**). The campaign detailed in this report is the latest in a growing trend Team Cymru has observed of cyber criminals targeting SOHO routers," they noted. Is it any wonder that the criminals are going after these devices, given that they are notoriously full of exploitable security holes, and users are lax when it comes to changing the default administrator password? To read more click **HERE**

Cyber crooks will go after medical records next

Heise Security, 3 Mar 2014: As security firms and law enforcement agencies continue to cooperate and successfully take down botnets, cyber crooks will be forced to look for new and more lucrative targets, and especially ones that are poorly secured. In a panel held at the RSA Conference held last week in San Francisco, the Microsoft/Agari team behind the Citadel botnet takedown said that these new targets will likely be in the healthcare industry. After explaining just how they went about affecting the takedown, they explained the reasoning behind their belief that healthcare IT systems and hospital databases are next in line for data breaches. Agari CEO Patrick Peterson shared that the price of medical records belonging to a single person might fetch around $60, while a single credit card record is worth a couple of dollars in the underground markets. He also pointed out that among the industries targeted so far, financial organizations and social networks have worked hard on protecting their customers, and have made cybercriminals' attempts more difficult and, therefore, more costly. On the other hand, the majority of the healthcare industry has not followed suit. In addition to all this, medical records give crooks much valuable information about a target that can be misused for mounting effective social engineering attacks, noted Richard Boscovich, assistant general counsel with the Microsoft Digital Crimes Unit. You might believe that information such as that contained in medical records might be that helpful, but in the hands of skilled social engineers it can turn to gold. "These guys are good, we've seen that happen," commented Boscovich. To read more click **HERE**

Wi-Fi-Hopping Malware Behaves Like Actual Virus

Yahoo: 3 Mar 2014: This malware is sick: The experimental "Chameleon" malware spreads rapidly among Wi-Fi networks in densely populated areas, much as a disease spreads through crowded urban areas. Developed in a laboratory at the University of Liverpool in England, Chameleon is the first malware known to propagate by hopping from one Wi-Fi network to another. "It was assumed ... that it wasn't possible to develop a virus that could attack Wi-Fi networks; but we demonstrated that this is possible and that it can spread quickly," Alan Marshall, Professor of Network Security, said in a statement. Chameleon is technically a worm, not a virus, because it replicates without human assistance by trying to crack the password of each new Wi-Fi router it encounters. Chameleon nevertheless behaves like a biological infectious organism, jumping among overlapping Wi-Fi networks as an airborne disease spreads among humans. The researchers simulated Chameleon infections in London and Belfast and found that just a few infected devices can spread the worm to "thousands of infected devices within 24 hours." Furthermore, because Chameleon doesn't migrate beyond Wi-Fi routers, it is undetectable to current anti-virus software, which scans for threats on computers and the Internet. In its current state, Chameleon doesn't do much more than replicate itself and identify poorly protected Wi-Fi networks, but the researchers say in their paper that such malware could be used to eavesdrop on Internet traffic, alter or destroy data packets or destroy an infected Wi-Fi router. Chameleon doesn't exist in the wild, so there's no real risk of infection. The good news is a strong Wi-Fi password will keep your router safe from this kind of malware; if it can't break into your router, it will simply move on to the next available one. The bad news is that many commercial and private Wi-Fi networks have weak passwords, or simply aren't password-protected at all. To read more click **HERE**

Credit card data breach targets Marriott, Sheraton and other hotels

CNBC, 4 Feb 2014: A credit card data breach has been detected that exposed guests at certain Marriott, Holiday Inn, Sheraton and other hotel properties to theft, hotel management firm White Lodging Services Corp said on Monday. The breach occurred at food and beverage outlets at 14 hotels, including some operated under the Westin, Renaissance and Radisson names, between March 20 and December 16 last year, White Lodging said in a statement. The company said information subject to potential theft by cyber criminals included names and numbers on consumers' debit or credit cards, security codes and card expiration dates. Customers who used their cards at the affected outlets should review all statements from the time in question and consider placing fraud alerts on their credit files, White Lodging said. White Lodging would not estimate how many card numbers might have been taken. Krebs on Security, the cyber security blog that first reported the breach on Friday, said thousands of accounts had been compromised. FBI warned retailers last month to prepare for more cyber attacks after discovering about 20 hacking cases in the past year involving the same kind of malicious software used against Target Corp over the holiday shopping season. The incident involving Target, the No. 3 U.S. retailer, was one of the biggest retail cyber attacks in history. Gregg Steinhafel, Chairman & CEO of Target details Target's data breach saying malware was installed on Target point of sale registers. Target is accountable and responsible and will not rest until they get to the bottom of the breach, Steinhafel adds.In a confidential, three-page report to retail companies the FBI described the risks posed by "memory-parsing" malware that infects point-of-sale (POS) systems, which include cash registers and credit-card swiping machines in checkout aisles. Restaurants and lounges affected by the White Lodging breach were at hotels in Chicago; Austin, Texas; Richmond, Virginia; Plantation, Florida; Denver, Boulder and Broomfield, Colorado; Louisville, Kentucky; Erie, Pennsylvania; and Indianapolis and Merrillville, Indiana, the company said. White Lodging, which manages 169 hotels that include brands of Marriott International, Starwood Hotels and Resorts and Inter Continental Hotels Group, said it planned to offer affected consumers one year of identity protection services. The company, based in Merrillville, Indiana, said it notified federal authorities of the suspected breach and had begun a review of other properties it manages. A spokeswoman for White Lodging declined to comment beyond the company's statement. Marriott said one of its franchise management companies had "unusual fraud patterns" with payment systems, according to a statement from spokesman Jeff Flaherty. He added that Marriott was working with the company in the probe. "Because the suspected

breach did not impact any systems that Marriott owns or controls, we do not have additional information to provide," Flaherty added. To read more click **HERE**

Hackers use '.enc' trick to deliver Zeus banking malware

IDG News Service, 3 Feb 2014: Hackers found a new way to slip past security software and deliver Zeus, a long-known malicious software program that steals online banking details. Security company Malcovery Security, based in Georgia, alerted security analysts after finding that none of 50 security programs on Google's online virus scanning service VirusTotal were catching it as of early Sunday. Gary Warner, Malcovery's chief technologist, posted on his blog an assortment of spam messages, which spoofed brands and organizations such as the payment processor ADP, the Better Business Bureau and the British tax authority HMRC. The spam messages contain a ".zip" file, which, if opened, contains a small application called UPATRE. That executable file downloads a ".enc" file, which it then decrypts. The decrypted file is GameOver Zeus, a variant of the notorious Zeus malware. Zeus first appeared in 2006 and has long been a thorn in the side of banks. Its source code was leaked in May 2011, and cybercriminals have continued to make improvements to make its network more resilient, according to Dell's SecureWorks unit. Security products are appearing to stumble on the ".enc" file since it doesn't end in ".exe," which designates an executable program, Warner wrote. "Why? Well, because technically, it isn't malware," he wrote. He advised that network administrators check their logs to see if any ".enc" files have been downloaded on their networks. The spam is distributed by the Cutwail botnet, another long-running botnet known for distributing malware. To read more click **HERE**

Cybercriminals Hijack Internet Connections by Changing DNS Settings in Routers

SoftPedia, 4 Mar 2014: Security holes in various home and small office routers are allowing cybercriminals to change the devices' DNS settings in an effort to redirect users to arbitrary IP addresses and domains. Experts have identified 300,000 compromised wireless routers. According to Team Cymru researchers, most of the impacted devices are located in Europe and Asia. Most of the victims have been spotted in Vietnam, but compromised machines have also been identified in India, Italy and Thailand. The campaign is said to have started in mid-December 2013 or possibly earlier. Interestingly, the attackers are exploiting several vulnerabilities to hijack a wide range of routers, including ones made by TP-Link, Micronet, D-Link and Tenda. The exploits leveraged by the cybercriminals include a recently-disclosed authentication bypass in ZyXEL firmware, and cross-site request forgery (CSRF) issues, such as the one found by security researcher Jakob Lell back in October 2013. Experts say small office and home (SOHO) routers is an attractive target to cybercriminals because they're easy to compromise. Furthermore, taking control of routers enables them to make considerable profit without too much effort. Once they hijack the devices, the attackers can direct users to malware or phishing sites, replace advertisements, and even redirect search results. So how can you tell if your device has been compromised? The DNS settings are altered to send request to these IP addresses: 5.45.75.11 and 5.45.75.36. If your router is configured with these DNS servers, you are impacted by this attack. The problem with these DNS poisoning attacks is that – similar to the case of the notorious DNSChanger malware – once the malicious servers are taken down, victims are no longer able to access the Web until they restore DNS settings. This makes mitigation a bit more problematic. A couple of similar attacks were spotted in the past period. One of them involves the Moon worm which targets Linksys routers. In another campaign, analyzed by CERT Poland, cybercriminals hijacked the DNS settings of routers to lure unsuspecting Internet users to fake bank websites in an effort to steal their data. However, Team Cymru says the attacks don't appear to be connected. The security firm has reached out to impacted vendors to let them know about the malicious campaign. Team Cymru also provides mitigation strategies for both end users and organizations that might house such devices. For additional technical details and recommendations check out the "SOHO Pharming" white paper published on the company's website. To read more click **HERE**

Twitter Resets User Passwords, Tells Them Their Accounts May Have Been Hacked

SoftPedia, 4 Mar 2014: A few hours ago, a large number of Twitter users started receiving password reset notifications. It turns out that the emails have been sent out by mistake, not because of hacker attacks. The large number of emails led many to believe a third-party service or website had been breached. "Twitter believes that your account may have been compromised by a website or service no associated with Twitter. We've reset your password to prevent others from accessing your account," the emails read. Around one year ago, Twitter reset the passwords of 250,000 users after suffering a data breach. However, this time, the social media company says there's no hacking involved. Instead, the passwords have been reset unintentionally. "We unintentionally sent some password reset notices tonight due to a system error. We apologize to the affected users for the inconvenience," Twitter representatives have told The Next Web. While most of the users who have received the password reset notifications haven't had their accounts exposed, the incident has caused unnecessary panic. On the other hand, some users' accounts could have been really targeted by cybercriminals just as the emails were being sent out. Now that Twitter has revealed that the reset has been unintentional, many people might make the mistake of continuing to use the same password. If your password has been reset, change it. Even if it hasn't been compromised, users are recommended to periodically change their passwords to make sure their accounts are secured. To read more click **HERE**

ISO: Tiny, inexpensive counterfeit electronics detector

GCN, 28 Feb 2014 Used and non-authentic counterfeit electronic components are widespread throughout the defense supply chain. According to the Defense Advanced Research Projects Agency, over the past two years alone, more than 1 million suspect parts have been associated with known supply-chain compromises. The problem is pervasive, with both expensive and inexpensive electronic parts being targeted. Counterfeit or otherwise suspect electronic components present a critical risk for the Department of Defense, where a malfunction of a single part could lead to system failures that can put missions at risk. A new DARPA program seeks to develop a tool to verify the trustworthiness of a protected electronic component without disrupting or harming the system. The DARPA Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program seeks proposals to develop a small (100 micron x 100 micron) component, or dielet, that authenticates the provenance of electronics components. Proposed dielets should contain a full encryption engine, sensors to detect tampering and would readily affix to microchips and other components. "SHIELD demands a tool that costs less than a penny per unit, yet makes counterfeiting too expensive and technically difficult to do," said Kerry Bernstein, DARPA program manager. "The dielet will be designed to be robust in operation, yet fragile in the face of tampering. What SHIELD is seeking is a very advanced piece of hardware that will offer an on-demand authentication method never before available to the supply chain." The dielet will be inserted into the component at the manufacturing site or affixed to existing trusted components, without any alteration of the host component's design or reliability. There is no electrical connection between the dielet and the host component. Authenticity testing could be done anywhere with a handheld probe or with an automated one for larger volumes. Probes need to be close to the dielet for scanning. After a scan, an inexpensive appliance (perhaps a smartphone) uploads a serial number to a central, industry-owned server. The server sends an unencrypted challenge to the dielet, which sends back an encrypted answer and data from passive sensors—like light exposure—that could indicate tampering. "The Department of Defense puts severe demands on electronics, which is why a trusted supply chain is so important" said Bernstein. "SHIELD is a technology demonstration leveraging the asymmetry of scaling for security. While the program is being funded by DARPA, industry will adapt future implementations to make the technology scalable to the industry and the defense supply chain." SHIELD is seeking proposals that would revolutionize electronic authentication with scalability and advanced technology not available today. DARPA will host a Proposers' Day Workshop in support of the SHIELD program on March 14, 2014. To read more click **HERE**