The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

25 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 24, Softpedia – (International) **Banking malware distributed via YouTube ads.** Bromium researchers found that cybercriminals compromised an ad network that hosted the Styx exploit kit used to serve advertisements on YouTube. The exploit kit pushes Caphaw malware onto infected devices leveraging Java vulnerabilities to obtain banking information. Source: http://news.softpedia.com/news/Banking-Malware-Distributed-via-YouTube-Ads-429011.shtml

February 21, South Jersey Times – (New Jersey) **Inspira Health Network informs patients of possible data breach after computer thefts.** A former Inspira Health Network employee was charged in connection with allegedly stealing two computers from the Inspira Medical Center Vineland's radiology department in December 2013 and selling them to a recycling yard. The health network notified 1,411 patients about a potential data breach. Source: http://www.nj.com/cumberland/index.ssf/2014/02/inspira_health_network_informs_patients_of_possible_data_breach_after_computer_thefts.html

February 24, Help Net Security – (International) **Apple fixes critical crypto bug in iOS, OS X fix to be released "soon."** Apple released software updates for its iOS mobile operating system and Apple TV addressing a critical encryption flaw, but advised users of its OS X system to avoid using public networks until a fix is provided after a SSL implementation vulnerability was discovered. The vulnerability applies to Apple's Safari browser and default Mail.app, potentially allowing a Man-in-the-Middle attack. Source: http://www.net-security.org/secworld.php?id=16409

February 21, IDG News Service – (International) **Glitch hits Google Drive, Docs, trips them for hours.** Google announced a service disruption of its Drive cloud storage service, Docs word processing and Sheet spreadsheet applications, and its Sites intranet builder that lasted more than 5 hours February 20. Source: http://www.networkworld.com/news/2014/022114-glitch-hits-google-drive-docs-278976.html

Bitcoin exchange Mt. Gox disappears in blow to virtual currency
Reuters, 25 Feb 2014: Mt. Gox, once the world's biggest bitcoin exchange, looked to have essentially disappeared on Tuesday, with its website down, its founder unaccounted for and a Tokyo office empty bar a handful of protesters saying they had lost money investing in the virtual currency. The digital marketplace operator, which began as a venue for trading cards, had surged to the top of the bitcoin world, but critics - from rival exchanges to burned investors - said Mt. Gox had long been lax over its security. It was not clear what has become of the exchange, which this month halted withdrawals indefinitely after detecting "unusual activity." A global bitcoin organization referred to the exchange's "exit," while angry investors questioned whether it was still solvent. A document circulating on the internet, and purporting to be a crisis plan for the exchange, said more than 744,000 bitcoins were "missing due to malleability-related theft", and noted Mt. Gox had $174 million in liabilities against $32.75 million in assets. It was not possible to verify the document or the exchange's financial situation. Tokyo investors in the frontier electronic currency, who have endured a volatile ride in the value of

the unregulated cyber-tender, said the problem was with Mt. Gox, not with the revolutionary bitcoin itself. Mt. Gox officials did not answer the telephone or respond to email requests for information. The concierge at the home of the chief executive, Mark Karpeles - an upscale apartment in the Shibuya district - said he was not answering his intercom. His mailbox was so stuffed with mail that the flap would not close. The Mt. Gox homepage was not loading, although no error message appeared. Its source code contained a line saying, "put announce for mtgox acq here." To read more click **HERE**

Cybercriminals Use Pony Botnet to Steal 700,000 Account Credentials, Virtual Currencies

SoftPedia, 25 Feb 2014: Back in December 2013, security researchers from Trustwave's SpiderLabs revealed uncovering a stash of 2 million account credentials stolen by cybercriminals with the aid of the botnet dubbed Pony. Now, in addition to account credentials, experts say Pony has also been utilized to steal virtual currencies. Cybercriminals have managed to steal a total of more than 700,000 credentials, 600,000 of which are for websites, 100,000 for email accounts, 16,000 for FTP servers, 900 for SSH, and 800 for Remote Desktop. This data was stolen between September 2013 and mid-January 2014. Based on data from the control panel of the attack, experts determined that after four months of stealing information, the cybercriminals decided to stop the operation. Most credentials have been stolen from Germany (41,177), Poland (17,214), Italy (15,672), the Czech Republic (14,835), Bulgaria (7,063), France (5,513), Croatia (4,725), Peru (4,616), India (2,761) and Vietnam (2,234). Close to 80,000 Facebook accounts have been impacted, followed by ones on accounts.google.com (13,740), nk.pl (13,169), seznam.cz (11,712), profil.wp.pl (8,036), abv.bg (6,589), yahoo.com (6,554), szn.cz (6,175), google.com (5,842) and pl-pl.facebook.com (3,974). The Pony botnet has also been used to target Bitcoin and other virtual currency wallets. Experts have found that the cybercriminals have stolen $220,000 (€160,000) worth of virtual currencies. In addition to Bitcoin, the list also includes Litecoin, Feathercoin, Fastcoin, Bytecoin, Namecoin, Mincoin, Zetacoin and many others. In total, around 30 virtual currencies have been targeted. Because of the high value of Bitcoin, the attackers didn't even have to compromise a large number of wallets. They only hijacked a total of 85, out of which they transferred 355 Bitcoins, 280 Litecoins, 33 Primeoins and 46 Feathercoins. While stealing money from bank accounts is becoming increasingly difficult for cybercriminals, when it comes to Bitcoin heists, there are a number of advantages. First of all, while all transactions are public, they're also irreversible. This means that if someone empties your wallet, there's nothing you can do about it. There's no one who can put the "money" back into the wallet and the accounts cannot be frozen to prevent theft. Cybercriminals simply need to transfer the funds into their account on a trading website, convert the virtual coins to a real currency and move the money into their bank account. If you fear that you might be one of the victims of the virtual currency heist, enter your public key (not private key) into an app made by SpiderLabs to see if you're impacted. The company has also published a tool that allows users to check if their other accounts have been compromised - just enter your email address to find out if your credentials have been stolen. To read more click **HERE**

iOS 7.0.6 and iOS 6.1.6 Still Vulnerable to Hacker Attacks, Says FireEye

SoftPedia, 25 Feb 2014: Security researchers from FireEye have discovered that, despite Apple's attempts to secure iOS 7 and iOS 6 last week, there is still a serious vulnerability inside the software that can allow a hacker to perform keylogging attacks. FireEye writes on its blog, "We have created a proof-of-concept 'monitoring' app on non-jailbroken iOS 7.0.x devices. This 'monitoring' app can record all the user touch/press events in the background..." These events include screen touches, home button presses, and even volume button presses. The TouchID fingerprint sensor is no exception, "and then this app can send all user events to any remote server." "Potential attackers can use such information to reconstruct every character the victim inputs," the security researchers say. The security firm explains that the "background app refresh" feature in iOS 7 disables unnecessary refreshing and "contributes to preventing the potential background monitoring," but adds that "it can be bypassed." The blog post includes an example using the music app that plays in the background without having to turn on its "background app refresh" behavior, since it's designed differently for multitasking. As such, FireEye says, "a malicious app can disguise itself as a music app to

conduct background monitoring." The firm asks readers to note that the flaw affects all device models and all iOS versions up to the latest firmware updates dished out by Apple last week. "Note that the demo exploits the latest 7.0.4 version of iOS system on a non-jailbroken iPhone 5s device successfully. We have verified that the same vulnerability also exists in iOS versions 7.0.5, 7.0.6 and 6.1.x," FireEye writes. It then warns that customers are susceptible to remote attacks, meaning Apple will have to deliver yet another firmware patch in the near future. "Based on the findings, potential attackers can either use phishing to mislead the victim to install a malicious/vulnerable app or exploit another remote vulnerability of some app, and then conduct background monitoring." An earlier post from FireEye, which got removed for one reason or another, said (emphasis ours), "FireEye successfully delivered a proof-of-concept monitoring app through the App Store that records user activity and sends it to a remote server. We have been collaborating with Apple on this issue." In other words, expect this flaw to get patched either in iOS 7.0.7 or iOS 7.1, a forthcoming update known to be in development at Apple. To read more click **HERE**

Google Paraguay Hijacked via NIC.py Hack

SoftPedia, 25 Feb 2014: An Iranian hacker who uses the online moniker Mormoroth has managed to breach the systems of the Network Information Center of Paraguay (nic.py). The attacker used the access to make it look like Google Paraguay (google.com.py) was defaced. The hacker hasn't actually breached any of Google's systems. Instead, he altered the DNS records for google.com.py to redirect the site's visitors to his defacement page. Mormoroth published a number of screenshots to demonstrate that he had gained access to NIC.py's backend systems. He leaked some user credentials and other information stolen from the site's databases. In a blog post on ha.cker.ir, the hacker has explained that he has leveraged a remote code execution (RCE) vulnerability to breach NIC.py. "By executing simple localroot exploit we are able to gain root access and cp all data on server but that is not necessary, admin have set inappropriate permissions on all directories which made us capable of browsing everywhere and reading any file," Mormoroth noted. The hacker says that initially he didn't want to publish any data stolen from the NIC. However, he decided to leak some information after Paraguayan authorities allegedly said "there wasn't any hack." A cyber security expert told ABC Color that he alerted Paraguay's National Computing Center of the vulnerability exploited by the Iranian hacker five years ago. To read more click **HERE**

South Korea Wants to Develop Stuxnet-like Malware

SoftPedia, 24 Feb 2014: South Korea's Ministry of Defense has revealed that the country plans on developing cyber warfare tools that can be used against North Korea's nuclear facilities and missile systems. This basically means that South Korea wants to develop a piece of malware similar to Stuxnet, which back in 2010 was used to damage an Iranian nuclear facility, the Yonhap news agency reported. Seoul's Cyber Warfare Command was created back in 2010 due to the large number of cyber attacks launched by Pyongyang. However, so far it has mostly focused on psychological warfare activities. In the second phase, the cyber command will "carry out comprehensive cyber warfare missions," said an unnamed official. The Ministry of Defense also wants to set up a Cyber Defense Department that will oversee cyber warfare operations, particularly defensive missions. To read more click **HERE**

Experts Find Vulnerabilities in Microsoft's EMET

SoftPedia, 24 Feb 2014: Security researchers from Bromium have been analyzing Microsoft's Enhanced Mitigation Experience Toolkit (EMET), a free tool that's designed to help Windows users enhance the security of third-party software. Experts say that EMET is vulnerable to custom-built exploits that attackers can use to bypass the protections offered in the tool. "EMET is a viable personal and corporate defense add-on, but given other researchers have found EMET bypasses before, we sought to understand how EMET is vulnerable to the presence of novel exploits," said Rahul Kashyap, chief security architect and head of security research at Bromium. "We want users to better understand the facts when making a decision about which PC protections to use. We conducted this research within Bromium Labs to further enhance EMET-like exploit mitigation tools so we as an industry can come together to better protect against

future exploitation vectors." Bromium has published a whitepaper that contains the technical details. Jared DeMott, principal security researcher with the company, is presenting the findings today, February 24, at BSides San Francisco. To read more click **HERE**

Adobe releases emergency Flash update amid new zero-day drive-by attacks

ARS Technica, 20 Feb 2014: Adobe has released an emergency update for its widely used Flash Player to combat active attacks that exploit a previously unknown security bug that hackers are actively exploiting to surreptitiously install malware on end-user computers. The vulnerability, which affects the latest versions of Flash, was being exploited in drive-by attacks on the websites of at least three nonprofit organizations, according to a blog post published Thursday by researchers from security firm FireEye. Two of the institutions—the Peter G. Peterson Institute for International Economics and the Smith Richardson Foundation—focus on matters of national security and public policy. The targets, combined with the technical signatures of the attacks themselves, have led researchers to suspect that the attackers are the same ones behind similar campaigns from 2012. The FireEye researchers wrote: This threat actor clearly seeks out and compromises websites of organizations related to international security policy, defense topics, and other non-profit sociocultural issues. The actor either maintains persistence on these sites for extended periods of time or is able to re-compromise them periodically. This actor also has early access to a number of zero-day exploits, including Flash and Java, and deploys a variety of malware families on compromised systems. Based on these and other observations, we conclude that this actor has the tradecraft abilities and resources to remain a credible threat in at least the mid-term. The vulnerability, which is indexed as CVE-2014-0502 under the common vulnerabilities and exposure system, allows attackers in certain cases to execute malicious code by overwriting the virtual function table pointer of a Flash object. In a testament to the growing effectiveness of modern exploit mitigation techniques, a protection known as address space layout randomization (ASLR) prevents the exploit from working on the vast majority of machines. ASLR vastly decreases the chances that a remote-code-execution attack will succeed by loading downloaded scripts in a different memory location each time the computer is rebooted. The attackers behind the campaign discovered by FireEye found a way to bypass ASLR on computers running older software. Specifically, PCs running Windows XP, Windows 7 with the now-unsupported 1.6 version of Oracle's Java, and Windows 7 with a now out-of-date version of Office 2007 or Office 2010 don't benefit from the protection of ASLR. Readers should remember that versions 12.0.0.44, 11.7.700.261, or earlier of Flash, regardless of the platform they run on, contain the underlying vulnerability. It's not uncommon for attackers to find new ways to exploit the same vulnerability. That means everyone should install Adobe's emergency update. ASLR, security sandboxes, and similar mitigations are highly valuable protections, but they are by no means foolproof, as the attacks demonstrate. Users should never regard these tools as a substitute for patching vulnerable software. The attacks are also a reminder of the damage that can result when running out-of-date programs from third parties. Adobe's Flash update is the second unscheduled release for the ubiquitous program this month. Adobe has more details about it here. It comes within hours of Microsoft releasing a stop-gap fix for vulnerabilities in versions 9 and 10 of its Internet Explorer browser to combat a separate zero-day campaign. To read more click **HERE**

Security vulnerabilities found in 80% of best-selling SOHO wireless routers

Heise Security, 21 February 2014: Tripwire has analyzed the security provided by the most popular wireless routers used in many small and home offices and found that 80 percent of Amazon's top 25 best-selling SOHO wireless router models have security vulnerabilities. Of these vulnerable models, 34 percent have publicly documented exploits that make it relatively simple for attackers to craft either highly targeted attacks or general attacks targeting every vulnerable system they can find. Routers are an ideal target for cyberattackers because they can be used to eavesdrop on traffic sent to and from nearby enterprise access points. After an attacker has gained control of a router, they are able to monitor, redirect, block or otherwise tamper with a wide range of online activities. Once a router is compromised, devices guarded by the router's firewall become targets for additional network-based attacks. Even technically oriented users

find it difficult to identify a wireless router cyberattack because router user interfaces are minimal, and the traffic sent from a compromised device to cyberattackers is typically invisible. Key study findings include:

- 30 percent of IT professionals and 46 percent of employees do not change the default administrator password on their wireless routers. With access to the configuration interface, attackers can easily compromise the device.
- 55 percent of IT professionals and 85 percent of employees do not change the default Internet Protocol (IP) address on their wireless routers, making Cross-Site Request Forgery (CSRF) attacks much easier for cyberattackers.
- 43 percent of IT professionals and 54 percent of employees use Wi-Fi Protected Setup (WPS) – an insecure standard that makes it simple for attackers to discover a router's encryption passphrase, regardless of its complexity or strength.
- 52 percent of IT professionals and 59 percent of employees have not updated the firmware on their routers to the latest version, so even when security updates from router vendors are available, most users do not receive the additional protection.

A few key security practices can help users can effectively limit wireless router cyberattacks. However, Tripwire's study of wireless router security practices among IT professionals and employees who access corporate networks from remote locations shows that these practices are not widely used. "VERT's research and SANS recent discovery of The Moon worm currently infecting exposed Linksys routers indicates that threats to routers will continue to increase as malicious actors recognize how much information can be gained by attacking these devices," said Craig Young, security researcher for Tripwire. "Unfortunately, users don't change the default administrator passwords or the default IPs in these devices and this behavior, along with the prevalence of authentication bypass vulnerabilities, opens the door for widespread attacks through malicious web sites, browser plugins, and smartphone applications," Young added. To read more click **HERE**

Russia and China: The Most Dangerous Countries for Smartphone Attacks

Bloomberg, 20 Feb 2014: Russia and China are the top two countries where smartphone users are most likely to encounter attacks. In news accounts of the cyber-attacks plaguing computer networks in the U.S., the bad actors are almost always the same - faceless adversaries hailing from shadowy regions of Asia and Eastern Europe. But what if the issue was examined from the other direction, from the perspective of people living in countries identified as launching pads for the world's hacking attacks? New research by security firm Lookout shows that when it comes to cyber-threats, countries reap what countries sow. The Lookout report (**LINK**) shows that Russia and China aren't just the source of sophisticated attacks on infrastructure abroad - they are also the top two countries where smartphone users are most likely to encounter attacks and harmful programs targeting their mobile devices. France, the U.K., the U.S. and Germany came next on the list. The report defined mobile threats as including outright malicious software - such as applications that steal personal information - along with programs that operate in more of a gray zone, such as bombarding users with an endless stream of advertisements. The findings show that lax policing of hacking attacks has allowed criminal enterprises in Russia and China to more easily launch outbound attacks and target citizens, said Marc Rogers, principal security researcher at Lookout. "In these countries, malware is much more prevalent, exposing their citizens to financial fraud, privacy violations and disruptive user experiences via the malicious software that plagues alternative app stores," Rogers wrote in an e-mail. "With limited access to legitimate app stores and loose regulations on premium SMS billing and privacy standards, citizens are more exposed." To read more click **HERE**

SEA hacks Forbes, steals and leaks 1M user records

Heise Security, 17 February 2014: Business news site Forbes and its registered users are the latest victims of the Syrian Electronic Army (SEA) hacker collective, which proved that they have broken into the company's network and took off

with a database containing over 1 million user and some Forbes' staffers records. "Forbes.com was targeted in a digital attack and our publishing platform was compromised," the company behind the publication TEXTconfirmed shortly after the revelation, and warned: "The email address for anyone registered with Forbes.com has been exposed. Please be wary of emails that purport to come from Forbes, as the list of email addresses may be used in phishing attacks." They also added that the passwords were encrypted, but that users would do well to change them anyway once sign-on is made available again. After initially claiming that they would sell the database, SEA hackers changed their minds and made it available for public download. Sophos' Paul Ducklin and his colleagues managed to get their hands on the file, and discovered that the records contained usernames, encrypted password data, users' full names, email address, and more. They have analyzed the data, and discovered that the passwords were not encrypted, but salted and hashed. "They use what's called PHPass Portable format," shared Ducklin, and explained how it works. "You can 'work backwards' from the Forbes datatbase to recover the passwords, but you need a lot of computing power, or time, or both," he noted, and added the scheme is good if the users chose complex and long passwords. But after they managed to crack the passwords belonging to Forbes staffers, it was clear that even they had used very poor passwords. "Forbes did the wrong thing by getting breached in the first place, and by letting the SEA make off with its password database," Ducklin commented. "And while the the 8193-iteration MD5-based hashing system described is a little short of modern best practice (try a stronger hash that takes longer to calculate, with more iterations), it's better than Adobe's disastrous 'one key to encrypt them all' system. To read more click **HERE**

Have Linksys routers? Watch out for this malware

IT Manager Daily, 18 Feb 2014: There's a new threat to one of the most popular equipment manufacturers. Malware targeting multiple Linksys routers is turning up all over the place – and it's not immediately apparent what this particular worm is up to. The malware – dubbed "The Moon" – scans routers trying to find out more information about them, according to research by the SANS Institute. It appears to be searching for the router model, and the version of firmware its running. That could indicate this malware looking for outdated or unpatched hardware to infect. The second wave of the attack is to request the actual worm – a small file with an unknown impact. This worm then replicates itself, scanning for other victims. The odd thing: It's not quite clear what this worm does. It looks to just be spreading without any end goal. Right now it appears to just be spreading far and wide across the Internet. It could be that this is just an experiment for a hacker. Or it could be a test run to see how easily more malicious software could spread. At this point, it's all speculation, though. So far, the list of vulnerable routers includes Linksys' E4200, E3200, E3000, E2500, E2100L, E2000, E1550, E1500, E1200, E1000, and E900. If you have one of these routers, SANS has a test from the MsDos/Command prompt you can do to see if you're infected:

```
echo "GET /HNAP1/ HTTP/1.1\r\nHost: test\r\n\r\n" | nc routerip 8080
```

if you get the XML HNAP output back, then you MAY be vulnerable. At the end of the day, the best lesson: Make sure firmware is up to date. It's just as important as updating applications, if not more so. And make sure you disable the remote management option on your router if possible. To read more click **HERE**