The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

25 April 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

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, Sandia 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 open source data

April 24, Help Net Security – (International) **Mobile bad bots running across most top mobile operators.** Distil Networks released a report on harmful bot traffic and found that harmful bots increased their share of Web traffic in 2013 from 12.25 percent of traffic to 23.6 percent. The report also found that the financial services industry had more organizations contributing a high percentage of harmful bot traffic than other industries, and that mobile harmful bots are running across nine of the world's top ten mobile operators, among other findings. Source: http://www.net-security.org/secworld.php?id=16732

April 24, The Register – (International) **Cisco: Hey, IT depts. You're all malware hosts.** Cisco released its latest security survey and found that 100 percent of companies in the survey sample show malicious traffic calling to malware hosts and that the length of time that the activity persists suggests that network penetrations are ongoing and undetected, among other findings. Source: http://www.theregister.co.uk/2014/04/24/cisco_youre_ialli_malware_hosts/

Nine Members of Cybercrime Ring Sentenced to a Total of 24 Years for Attacks on Banks
SoftPedia, 25 Apr 2014: Nine individuals involved with a cybercriminal group responsible for stealing £1.25 million ($2.1 million / €1.51 million) from bank accounts have been sentenced to a total of 24 years and 9 months by the United Kingdom's Southwark Crown Court. The fraudsters used KMW (Keyboard, Video, Mouse) switches to transfer money from bank accounts at Barclays and Santander. They also made fraudulent purchases with payment cards obtained after intercepting or stealing around 1 million letters. The cards were used to purchase expensive watches, jewelry and other high-value items worth more than £1 million ($1.68 million / €1.21 million). Lanre Mullins-Abudu, 25, has been sentenced to a total of 8 years in prison for one count of conspiracy to commit fraud, two counts of conspiracy to steal and one count of possession of articles for use in fraud. Steven Hannah, 53, has been sentenced to 5 years and 10 months in prison for conspiracy to commit fraud and possession of drugs with intent to supply. The list of sentenced individuals also includes Tony Colston-Hayter (5 years and 6 months in prison), Darius Valentin Boldor (2 years and 6 months in prison), Dean Outram (3 years in prison), Segun Ogunfidodo (9 months suspended, community work and tag-monitored curfew), Adam Raeburn Jefferson (1 year and 9 months suspended and tag-monitored curfew for 6 months), and Dola Leroy Oduns (9 months suspended, community work and curfew). James Lewis Murphy has been sentenced to six months in prison, but he has already served his sentence while in custody. Other members of the conspiracy will be sentenced in the upcoming period. "Today's convictions are the culmination of a long and highly complex investigation into an organised crime group whose aim was to steal millions of pounds from London banks and credit card companies," said Detective Chief Inspector Jason Tunn, of the MPS Cyber Crime Unit. "Through working with industry partners such as Santander and Barclays, whose efforts in assisting us were immense, we have been able to bring this group to justice," he added. "This case demonstrates the sheer investigative skill we are able to apply to tackling cyber crime, as we continue working to keep London people and businesses safe from cyber criminals. We are determined to make London a hostile place for cyber criminals and not allow the internet to be a hiding place for those who defraud people in the capital," he went on to say. To read more click **HERE**

Hackers Blackmail Belgian Hosting Firm AlfaNet

SoftPedia, 25 Apr 2014: Rex Mundi, a hacker group that's known for breaching into the systems of various companies in an effort to blackmail them, is back. A few hours ago, they announced hacking Belgian hosting company AlfaNet. According to the hackers, AlfaNet provides hosting services for 13,000 websites. The cybercriminals threaten to leak data and attack some of the websites if the company doesn't pay up. "We have hacked their database and we have stolen all of their customer data. Alfanet has two more days to pay us 15,000 Euros. Unfortunately, so far, they did not reply to our emails. We hope that they will decide to protect their customers before the deadlines expires on Friday evening," the hackers said. "If no money is received on Friday evening, we will post their entire database and we will directly attack some of their customers," they added. To prove their point, they've leaked some customer data samples and some database information. We've reached out to AlfaNet to see what they plan on doing. So far, they haven't responded to our inquiry, but we've received confirmation that they got our email. It's worth noting that Rex Mundi is usually not bluffing. They've leaked data stolen from the systems of numerous companies that have refused to give in to their demands. The list of targeted companies includes Numericable, Habeas, Websolutions.it, Buy Way and Hoststar. Many of their targets are Belgium-based organizations. It remains to be seen if AlfaNet pays up, but the most likely scenario is that they will not give in to extortion. Experts advise companies that find themselves in this situation not to pay up until the breach has been properly investigated. Security expert and malware researcher Bart Blaze believes that the best thing they can do is contact authorities – police and even the local CERT. According to the expert, in most cases, cybercriminals will sell the stolen data regardless of whether the company pays up or not. As for damage control, Blaze recommends that logs be checked for any clues that might help in identifying the attackers. Another important step is notifying customers, and being as transparent as possible in the process. It remains to be seen how AlfaNet acts. As Blaze highlights, it's uncertain what messages have been exchanged directly between the company and the attackers. On the other hand, it's unlikely that a company that's publicly blackmailed will admit paying up, even if they do decide to go down that path. To read more click **HERE**

Windows Phone 8.1 Fix for Error 80188309 Pushed Back Until May

SoftPedia, 25 Apr 2014: It's been more than a week since Microsoft released Windows Phone 8.1 Developer Preview and many users have yet to install the new version of the operating system. Although all that Windows Phone 8 owners would need in order to install the Developer Preview on their device is an App Studio account, it looks like those who own Huawei smartphones or handsets other than Nokia have been unable to upgrade. Lots of Windows Phone fans complain that they cannot update their smartphones to Windows Phone 8.1 Developer Preview due to the infamous error 80188309. Microsoft acknowledged the issue at the end of last week and promised that more details on the matter would be offered on April 24. True to its promise, the Redmond-based company took it to its support site and issued a short statement that offered a glimpse on the status of a fix for this error. The good news is that Microsoft has been able to find a solution to the issue, which is now going through normal testing, but the bad news is that it won't be released for at least another week. Here is Microsoft's full statement: "Thank you all for waiting patiently over the last week, and continuing to stick with us as we work on getting you the Windows Phone 8.1 Preview. We believe we have identified the fix and will be going through some of our normal testing to confirm. With that being said, I don't have an update yet on when we will roll this fix out to you. I plan to provide more information on Thursday May 1st. In the meantime, please continue to hold on and thank you again for your willingness to participate in our Developer Preview Program." We expect the next update on the status of the fix to drop in on May 1, as promised by Microsoft's officials. However, that doesn't mean that the highly anticipated fix will be provided in the first day of May. Keep in mind that most of the Windows Phone fans affected by this error 80188309 own Huawei devices, but the upcoming fix will be provided to all those that cannot install Windows Phone 8.1 Developer Preview on their smartphones. We will keep an eye out for any additional details, but we doubt that Microsoft will offer the fix ahead of the mentioned deadline. Nevertheless, the good news is that the company nailed the fix and is about to roll it out to users. Let's hope that nothing bad happens during testing. To read more click **HERE**

British IT Workers Are Increasingly Stressed Out Because of Heartbleed

SoftPedia, 25 Apr 2014: British security experts are incredibly stressed out these days, a recent survey indicates, and it's all because of Heartbleed and its security implications. The OpenSSL vulnerability isn't the only cause of stress, of course, since the list also includes the discontinuation of support for Windows XP by Microsoft. As if the IT industry weren't stressful enough already, these recent events have made things even harder for employees in this sector. In fact, 68 percent of the IT staff in the United Kingdom is currently considering leaving their current role due to job-related stress. For the third time in a year, high levels of work stress are contributing to high job dissatisfaction among people working in IT. Despite some budget pressure reductions, these levels were only slightly reduced over 2013. The study conducted by Opinion Matters takes into account the thoughts of 200 British administrators in companies of 10 or more people and it sought to gauge the respondents' stress levels at work, while also trying to locate their main stressors. Key findings of the survey indicate that 36 percent of IT workers have missed social functions or cut down on family time due to issues they had to handle at work. Another 28 percent have admitted to regularly losing sleep over work pressure and 19 percent to even falling ill due to high stress levels. A quarter of all those interviewed felt that they were by far the most stressed person in their social or family group. It's also become a habit for IT staffers to frequently work overtime, often without additional pay, as well as during the weekends. "IT is renowned for being one of the most stressful white-collar jobs to undertake, now more so than ever given the critical role IT plays in everything from ecommerce to facilities management. There is a lot that organisations can do to reduce the burden – and with it the stress levels – carried by IT staff. Providing realistic IT budgets and staffing levels helps a lot, but there are productivity changes that can also significantly de-stress the IT department, such as investing in technology to automate personnel-intensive activities like deploying software updates and managing sprawling Wi-Fi networks and the myriad of mobile devices that users are bringing to work," said Sergio Galindo, general manager of the infrastructure business unit at GFI Software. While this paints a pretty sad picture, things over in the United States seem to be even worse. According to data, 78.5 percent of US IT staff are already looking for a new job. To read more click **HERE**

Anonymous Cambodia Isn't Giving Up After the Arrest of Two Members

SoftPedia, 25 Apr 2014: Earlier this week, we learned that two members of Anonymous Cambodia were arrested. Other hacktivists have announced their plans to attack Cambodian government websites in response to the arrests. The suspects are Bun King Mongkolpanha, aka "Black Cyber" or "Machine," and Chu Songheng, aka "Zoro." They're both 21 and students at the SETEC Institute in Phnom Penh. Mongkolpanha has reportedly admitted hacking websites, but Songheng said he was only trying to learn how to hack. They were arrested on April 7 after an eight-month investigation by local authorities and the US Federal Bureau of Investigation. The suspects face up to two years in prison for hacking and disrupting numerous government websites. We've attempted to get in touch with the individual behind the Anonymous Cambodia Twitter account, but the account has been inactive since news of the arrests broke. However, in the meantime, Anonymous Cambodia has set up a new Facebook page where they've announced their plans. The hacktivists have published several messages written in Khmera. They claim that they have a lot of supporters that will help them launch attacks until the arrested individuals are released. It's worth noting that their Facebook page already has over 12,000 likes. The list of targets includes a number of websites belonging to private organizations, but also ones belonging to the Cambodian government and the national police. The hackers have already leaked some data and they've published a video to show their supporters how to launch distributed denial-of-service (DDOS) attacks. The hacktivists say the arrest of two members doesn't stop them from continuing their operations against the government. "You arrested only two of us, but still we can continue our work and will be stronger than before. Ten times to 1,000 times and 10,000 times. It will never end," they wrote on Facebook. To read more click **HERE**

Heartbleed Bug Patched on All US Government Websites

SoftPedia, 25 Apr 2014: A large number of the world's top websites have been impacted by the OpenSSL vulnerability dubbed the "Heartbleed bug." Fortunately, many organizations have already patched their installations. According to Trend Micro, less than 10% of websites are still vulnerable. The US government has ensured that all its 117 .gov websites are patched. In fact, .gov is the only top-level domain (TLD) with 0 vulnerable websites. Domains for Australia, the United Kingdom, Germany and India are also mostly patched up. There still are many vulnerable sites in Russia, China and Brazil, experts have determined. "Overall, the numbers leave room for optimism when it comes to addressing Heartbleed. Most system administrators have paid attention to the warnings and patched their servers accordingly," Trend Micro Senior Threat Researcher Maxim Goncharov explained in a blog post. "The question is now whether the remaining 10% of vulnerable domains will be patched sooner rather than later, or if we will be stuck with a non-trivial portion of the Internet that will be left at risk." The fact that most organizations have patched their OpenSSL installations is also confirmed by Distil Networks. Earlier this week, the company reported that 84% of the top 10,000 global websites had applied the patch to fix the Heartbleed bug. Distil, which specializes in bot protection, has developed a bot capable of checking the dates on which SSL certificates have been issued. Companies must re-issue their digital certificates because they could have been compromised by hackers exploiting the Heartbleed vulnerability. For the time being, Distil says that 9% have issued new certificates, but 15% haven't done so. For the other 76%, the results are inconclusive. Several tools have been released to help organizations determine if their installations are vulnerable. Trend Micro has also developed a couple of tools to help users determine if the websites they're visiting or the Android applications they're using are susceptible to Heartbleed attacks. The problem with Heartbleed attacks is that they're difficult to detect. That's why many of the impacted companies have decided to change all their digital certificates and advise their customers to change their passwords as a precaution. Of course, changing passwords was the first piece of advice given by experts after the world learned of Heartbleed. However, as many have highlighted, changing passwords would have been ineffective if the service in question hadn't patched its OpenSSL installation. To read more click **HERE**

Spammers Use Non-Latin Characters to Evade Spam Filters

SoftPedia, 25 Apr 2014: Spammers keep coming up with new ways to evade spam filters. Recently, they've started replacing regular characters with similar-looking symbols in hopes that their scammy emails make it to inboxes. According to experts from Kaspersky Lab, the subject and the body of these spam emails might appear to be normal at first sight. However, a closer look reveals that many Latin characters have been replaced with symbols that look similar from other alphabets. This trend appears to be popular among cybercriminals targeting users in Italy. Experts have spotted various types of spam messages in which this technique is utilized. The spammers use Cyrillic, Greek and even IPA symbols to replace Latin characters. This is possible because of the UTF-8 coding system, which enables users to combine multiple types of characters in the same message. This simple trick could be enough to bypass classic spam filters. On the other hand, Kaspersky says its own anti-spam solutions are not so easy to trick. They can detect spam even if non-Latin characters are utilized. In any case, this proves that we can't rely only on service providers to keep our inbox spam free. Users must always be careful when opening links or attachments from unsolicited emails. To read more click **HERE**

AOL confirms Mail service hacked

Daily Record, 22 Apr 2014: AOL Mail has been hacked and several users have reported their accounts are being used to send spam to others. Although AOL has confirmed the hack, which thousands were complaining about on Twitter, it is currently unknown how widespread the issue is. "AOL takes the safety and security of consumers very seriously, and we are actively addressing consumer complaints," AOL said in a statement. "We are working to resolve the issue of account spoofing to keep users and their respective accounts running smoothly and securely." Users' AOL email accounts are sending messages that contain a link in them which could lead to malware, viruses or phishing attacks. "If you do find

email in your Sent folder that you did not send, your account has been compromised (hacked)," AOL's help page on spoofing states. "If you do not find any strange email in your Sent folder, your account has most likely been spoofed." To read more click **HERE**

Global shipping fleet exposed to hacking threat

Reuters, 23 Apr 2014: The next hacker playground: the open seas - and the oil tankers and container vessels that ship 90 percent of the goods moved around the planet. In this internet age, as more devices are hooked up online, so they become more vulnerable to attack. Hackers recently shut down a floating oil rig by tilting it, while another rig was so riddled with computer malware that it took 19 days to make it seaworthy again; Somali pirates help choose their targets by viewing navigational data online, prompting ships to either turn off their navigational devices, or fake the data so it looks like they're somewhere else; and hackers infiltrated computers connected to the Belgian port of Antwerp, located specific containers, made off with their smuggled drugs and deleted the records. While data on the extent of the maritime industry's exposure to cyber crime is hard to come by, a study of the related energy sector by insurance brokers Willis this month found that the industry "may be sitting on an uninsured time bomb". Globally, it estimated that cyber attacks against oil and gas infrastructure will cost energy companies close to $1.9 billion by 2018. The British government reckons cyber attacks already cost UK oil and gas companies around 400 million pounds ($672 million) a year. In the maritime industry, the number of known cases is low as attacks often remain invisible to the company, or businesses don't want to report them for fear of alarming investors, regulators or insurers, security experts say. There are few reports that hackers have compromised maritime cyber security. But researchers say they have discovered significant holes in the three key technologies sailors use to navigate: GPS, marine Automatic Identification System (AIS), and a system for viewing digital nautical charts called Electronic Chart Display and Information System (ECDIS). "Increasingly, the maritime domain and energy sector has turned to technology to improve production, cost and reduce delivery schedules," a NATO-accredited think-tank wrote in a recent report. "These technological changes have opened the door to emerging threats and vulnerabilities as equipment has become accessible to outside entities." As crews get smaller and ships get bigger, they increasingly rely on automation and remote monitoring, meaning key components, including navigational systems, can be hacked. A recent study by security company Rapid7 found more than 100,000 devices - from traffic signal equipment to oil and gas monitors - were connected to the internet using serial ports with poor security. "The lines get blurry, and all industries and all technologies need to focus more on security," said Mark Schloesser, one of the authors of the study. Mark Gazit, CEO of ThetaRay, an internet security company, said an attacker managed to tilt a floating oil rig to one side off the coast of Africa, forcing it to shut down. It took a week to identify the cause and fix, he said, mainly because there were no cyber security professionals aboard. He declined to say more. Lars Jensen, founder of CyberKeel, a maritime cyber security firm, said ships often switch off their AIS systems when passing through waters where Somali pirates are known to operate, or fake the data to make it seem they're somewhere else. Shipping companies contacted by Reuters generally played down the potential threat from hackers. "Our only concern at this stage is the possible access to this information by pirates, and we have established appropriate countermeasures to handle this threat," said Ong Choo Kiat, president of U-Ming Marine Transport, Taiwan's second-largest listed shipping firm by market value. The company owns and operates 53 dry cargo ships and oil tankers. A spokeswoman for Maersk Line, the world's top shipping container group, said: "Yes, we consider cyber risk a threat, but vessels are no more vulnerable to such attacks than onshore systems and organisations. We are taking this risk seriously and ensuring that we are protected against such threats." A study last year by the Brookings Institution of six U.S. ports found that only one had conducted an assessment of how vulnerable it was to a cyber attack, and none had developed any plan to response to any such attack. Of some $2.6 billion allocated to a federal program to beef up port security, less than 1 percent had been awarded for cyber security projects. When CyberKeel probed the online defences of the world's 20 largest container carriers this year it found 16 had serious security gaps. "When you look at the maritime industry there's extremely limited evidence of systems having been breached" compared to other sectors, said CyberKeel's Jensen. "That suggests to us that they've not yet been found out." Michael Van Gemert, a security consultant to the oil

and gas industry, said that on visits to rigs and ships he has found computers and control systems riddled with viruses. In one case, he said it took 19 days to rid a drilling rig en route from South Korea to Brazil of malware which had brought the vessel's systems to a standstill. "The industry is massively in need of help, they have no idea what the risks are," he said. The main ship navigation systems - GPS, AIS and ECDIS - are standards supported by bodies such as the International Maritime Organisation (IMO). Indeed, that body has made AIS and ECDIS mandatory on larger commercial and passenger vessels. Researchers from the University of Texas demonstrated last July that it was possible to change a ship's direction by faking a GPS signal to dupe its onboard navigation system. Marco Balduzzi and colleagues at anti-virus vendor Trend Micro last month showed that an attacker with a $100 VHF radio could exploit weaknesses in AIS - which transmits data such as a vessel's identity, type, position, heading and speed to shore stations and other ships - and tamper with the data, impersonate a port authority's communications with a ship or effectively shut down communications between ships and with ports. In January, a British cyber security research firm, NCC Group, found flaws in one vendor's ECDIS software that would allow an attacker to access and modify files, including charts. "If exploited in a real scenario," the company concluded, "these vulnerabilities could cause serious environmental and financial damage, and even loss of life." When the USS Guardian ran aground off the Philippines last year, the U.S. Navy in part blamed incorrect digital charts. A NATO-accredited think-tank said the case illustrated "the dangers of exclusive reliance upon electronic systems, particularly if they are found vulnerable to cyber attack." "Most of these technologies were developed when bandwidth was very expensive or the internet didn't exist," said Vincent Berk, CEO of security company FlowTraq. Fixing this will take time, and a change in attitude. "Security and attack scenarios against these technologies and protocols have been ignored for quite some time in the maritime industry," said Rapid7's Schloesser. Researchers like Fotios Katsilieris have offered ways to measure whether AIS data is being faked, though he declined to be interviewed, saying it remained a sensitive area. One Google researcher who has proposed changes to the AIS protocol wrote on his blog that he had been discouraged by the U.S. Coastguard from talking publicly about its vulnerabilities. Indeed, AIS is abused within the industry itself. Windward, an Israeli firm that collects and analyses AIS data, found 100 ships transmitting incorrect locations via AIS in one day - often for security or financial reasons, such as fishing boats operating outside assigned waters, or smuggling. In a U.N. report issued earlier this year on alleged efforts by North Korea to procure nuclear weapons, investigators wrote that one ship carrying concealed cargo turned off its AIS signals to disguise and conceal its trip to Cuba. It's not clear how seriously the standards bodies treat the threat. Trend Micro's Balduzzi said he and his colleagues were working with standards organisations, which he said would meet next year to discuss his research into AIS vulnerabilities. The core standard is maintained by the International Telecommunications Union (ITU) in association with the IMO. In a statement, the IMO said no such report of vulnerabilities had been brought to its attention. The ITU said no official body had contacted it about the vulnerabilities of AIS. It said it was studying the possibility of reallocating spectrum to reduce saturation of AIS applications. Yevgen Dyryavyy, author of the NCC report on ECDIS, was sceptical that such bodies would solve the problems soon. First, he said, they have to understand the IT security of shipboard networks, onboard linked equipment and software, and then push out new guidelines and certification. Until then, he said, "nothing will be done about it." To read more click **HERE**