Counterintelligence NEW MEXICO Working Group

NMCIWG Purple Arrow Established 2001

THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

7 October 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

JPMorgan Bracing for 'Spear Phishing' Campaign

Reuters, 6 Oct 2014: Morgan Chase officials are bracing for a massive spear phishing campaign launched by cyber thieves who broke into the bank's servers in the biggest cyber-attack on a U.S. bank to date. Cyber criminals thought to be emanating from Russia or former Soviet satellite states hacked into numerous JPMorgan computer servers and accessed contact information like names and email addresses for 76 million customers and seven million small businesses. JPMorgan is saying no bank account information was compromised, but it now fears the hackers will come back for this information in another wave of attacks directly on bank customers. Cyber criminals broke into JPMorgan's servers in June; the breach was then shut down in August. While JPMorgan says in a statement it has not yet "seen unusual fraud activity related to this incident," bank insiders are preparing for a spear phishing campaign, whereby JPMorgan customers in coming days could get targeted by an official-looking email complete with the bank's corporate logo, or they could get a phone call from a fake JPMorgan account executive. The email or caller could, say, tailor the e-mail to the customer with personalized information they downloaded in the first hack to grab their attention. The fake bank account executive or emailer will then indicate there is an urgent problem with the customer's account, and then ask for birthdates, Social Security numbers or passwords. The virtual trap could also be set by the official-looking email asking customers to click on a link embedded in the email to, say, update their account information. But the link takes the unsuspecting victim to a fake but legitimate-looking website, where the customer is then tricked into listing passwords, bank account numbers, Social Security numbers, user IDs, access codes, and PINs. "We would never ask for that personal information on the phone or in emails, its information that verifies who you are," says a bank insider. "The problem is, other banks often ask for this information on the phone or in emails, so customers could be fooled." An FBI official warns: "Once criminals have your personal data, they can access your bank account, use your credit cards, and create a whole new identity using your information." The FBI also warns that spear phishing can "trick you into downloading malicious codes or malware after you click on a link embedded in the e-mail." The criminal can then read everything on your computer or in your account. The malware also "is an especially useful tool in cyber hacking crimes like economic espionage where sensitive internal communications can be accessed and trade secrets stolen," the FBI says. "Malware can also hijack your computer, and hijacked computers can be organized into enormous networks called botnets that can be used for denial of service attacks." Government, or state-sponsored, cyber-attacks on other foreign governments, overseas retailers, banks, or other companies typically arise as massive "denial of service" attacks to shut down websites, or theft of trade secrets, not small-bore identity theft, meaning profiteering via fraud. Bank insiders are talking about individuals either connected to the Russian government, or working in criminal gangs within Russia or countries in the former Soviet Union. These insiders say they don't believe the Russian government sponsored the attacks in retaliation for U.S. sanctions on Russian companies due to Russia's incursion into the Ukraine. However, officials say foreign governments including Russia and the former Soviet satellite states are not doing enough to shut down cyber thieves, and instead are consciously turning a blind eye to this criminal activity. Officials warned: "The way the hackers do it is, they start with small charges on your Visa or MasterCard, $1, $10, $50, to see if their hack works, then they ramp it up and go bigger with a larger hit and run charge." To read more click HERE

Chinese-owned company “Lenovo” to Close on $2.1 Billion IBM x86 Server Deal

Newsfactor, 29 Sep 2014: Nearly nine months after first announcing its purchase plans, Lenovo expects to close on its acquisition of IBM's x86 server business this Wednesday. The final $2.1 billion purchase price was reduced from the initial offered price of $2.3 billion due to IBM's lower-than-expected inventories. Lenovo said the acquisition will make it the number three player in the global market for x86 servers, estimated at a value of $42.1 billion. HP currently occupies the top spot in that market, while IBM had previously occupied the number two position. This is not the first time that China-based Lenovo has acquired a segment of IBM's business. It took over Big Blue's line of personal computers in 2005. During a media conference call regarding the new acquisition this morning, we asked Lenovo chairman and CEO Yang Yuanqing to comment on the keys to successfully integrating IBM's x86 business into Lenovo. "We have a lot of experience (with) integrating the culture," he said, referring to the 2005 acquisition of IBM's PC line. "We have both walked down that road before." Based on its previous experience bringing an IBM business into its fold, Lenovo will know how best to integrate the leaderships, product lines and cultures of the two companies, Yang said. "We are very confident," he added. Under the deal, Lenovo will acquire IBM's System x, BladeCenter and Flex System blade server and switch lines, along with its x86-based Flex integrated systems, NeXtScale and iDataPlex servers and software, blade networking and maintenance operations. IBM will retain control of other lines, including its System z mainframes, Power Systems, Storage Systems, Power-based Flex servers, PureApplication and PureData appliances. IBM will also continue to provide maintenance delivery on Lenovo's behalf during the transition to ensure a "seamless transition" for current customers. Meanwhile, Lenovo will serve as an original equipment manufacturer to IBM and will resell some of IBM's storage and software products to enterprise customers. Lenovo is also on track to complete its acquisition of Motorola Mobility from Google. That deal is expected to make Lenovo the world's third-largest manufacturer of smartphones. Also announced in January, that $2.91 billion purchase is expected to expand Lenovo's reach in the North American, Latin American and western European markets. To read more click HERE

H-P Failed to Keep Up With Market, CIOs Say

WSJ, 5 OCt 2014: The Wall Street Journal reported Sunday that 75-year-old H-P planned to put its computer business and its higher margin printer business into one company, and to put its corporate hardware and services into another company focused on enterprises, or large firms. The company has not confirmed the move, but it could be announced as early as Monday, the Journal said. An H-P spokeswoman declined to comment for this article. Hewlett-Packard ProLiant commercial data servers are assembled by workers at a company manufacturing facility in Houston, Nov.19, 2013.“In my personal experience, they were at least two years behind in everything, and as you know, six months in this business is a long time,” said Luis Garzon, senior director of enterprise architecture at fashion company Coach Inc.COH -1.11% “What I really noticed is that they had not evolved their products, and they were not necessarily involving their customers, who wanted to help them.” H-P fell behind in the shift to the cloud, which refers to the distribution of software and IT services online, instead of through a company data center, Mr. Garzon said. He said he thought H-P invested a lot of effort into building up its desktop and mobile computing, when it might have been better off focusing more on services. “It’s no surprise,” said Mr. Garzon, who was in Orlando to attend Gartner Inc.IT -0.40%’s Symposium ITXPO 2014, a massive technology conference that kicked off Sunday. Mr. Garzon said Coach used H-P ProLiant servers, but that he had urged his company some time ago to diversify its tech spending among other vendors such as International Business Machines Corp.IBM +0.20% and Oracle Corp. “There won’t be a lot of impact for us,” he said. An IT professional with a financial services company, who declined to be identified, agreed that the breakup of H-P came as no surprise. Speaking during an informal interview at the Gartner conference, he described his firm as a large H-P shop. At a round table discussion several years ago, company IT managers were invited to speculate about which vendors might not survive another three to five years, and he said that H-P’s name came up a lot. H-P, he said, was slow to react to market forces, including the shift to the cloud. “Over half of our users are now relying on mobile devices and applications. PCs have mostly become a commodity. This announcement should not affect us much,” Verizon Communications Inc. Executive Vice President and CIO Roger Gurnani said in an email. One IT executive said the breakup of H-P followed the pattern established by its rival, IBM, which has sold its server as well as its PC units to rival Lenovo Group Ltd. to focus on business services. The sale of the server business closed just a few days ago. "It is IBM dejavu. It reinforces our view that hardware is a commodity and will not be a differentiator unless tightly coupled with the software," Manish Kapoor, senior vice president of information systems at NuStar Energy L.P., said in an email. "I am not surprised. H-P a few years ago hesitated to do the same thing. It is not a surprise now, but the timing is very late," said Paul Stokes, CIO of the University of Victoria, in British Columbia, who also was in Orlando for the Gartner conference. He said he had no sales contacts with the company—and used none of its products. "To me, they are not serving all the markets they could be serving," he said. Mr. Stokes said he believed that H-P's printers were first rate, but that its PCs and laptops had fallen behind the curve. The university's primary tech suppliers include IBM, Dell Inc. and Lenovo, he said. Most recently, H-P's services have been a mixed bag, according to Gartner analyst Neil MacDonald. But overall, he said, "HP has been slow to embrace the cloud, and it lacks certain capabilities of rivals." H-P has been in merger discussions with storage giant EMC Corp. To read more click HERE

China cyber-war costing US billions: FBI chief
AP, October 6, 2014: China is waging an aggressive cyber-war against the United States that costs American business billions of dollars every year, Federal Bureau of Investigation director James Comey said. The FBI chief told CBS television's "60 Minutes" program China topped the list of countries seeking to pilfer secrets from US firms, suggesting that almost every major company in America had been targeted. "There are two kinds of big companies in the United States," Comey said. "There are those who've been hacked by the Chinese, and those who don't know they've been hacked by the Chinese." Annual losses from cyber-attacks launched from China were "impossible to count," Comey said, but measured in "billions." Asked which countries were targeting the United States, Comey replied: "I don't want to give you a complete list. But ... I can't tell you top of the list is the Chinese." Comey cited the historic case of five members of China's People's Liberation Army indicted with hacking US companies for trade secrets, a move which outraged China when announced in May. The case is the first-ever federal prosecution of state actors over cyber-espionage. The PLA unit is accused of hacking into US computers to benefit Chinese state-owned companies, leading to job losses in the United States in steel, solar and other industries. "They are extremely aggressive and widespread in their efforts to break into American systems to steal information that would benefit their industry," Comey said of China's hackers. Comey said China was seeking to obtain "information that's useful to them so they don't have to invent." "They can copy or steal to learn about how a company might approach negotiations with a Chinese company all manner of things," he said. But China's hacking efforts were often easy to detect, Comey said. "I liken them a bit to a drunk burglar. They're kickin' in the front door, knocking over the vase, while they're walking out with your television set," he said. "They're just prolific. Their strategy seems to be, "We'll just be everywhere all the time. And there's no way they can stop us." Last week, big bank JPMorgan Chase revealed that a hack it had reported in August had compromised data on 76 million household customers and seven million businesses, including their names, email addresses and telephone numbers. Treasury Secretary Jack Lew, speaking on ABC television, declined to address the JPMorgan Chase case specifically. In August, the Federal Bureau of Investigation acknowledged that it and the US Secret Service were investigating the scope of recent cyberattacks against several US financial institutions. To read more click HERE

October 6, Softpedia – (National) **Data leak reported with five-month delay by Touchstone Medical Imaging.** Touchstone Medical Imaging announced October 3 that personal and billing information collected from patients before August 2012 were available online since the beginning of May. The exposed folder was removed by the company's IT department once it was discovered that the patient data was readable. Source: http://news.softpedia.com/news/Data-Leak-Reported-With-Five-Month-Delay-by-Touchstone-Medical-Imaging-461080.shtml

October 6, Softpedia – (International) **Yahoo, WinZip servers compromised through Shellshock vulnerability.** A security researcher with Future South Technologies identified and reported Yahoo, WinZip, and Lycos servers that were compromised by attackers exploiting the Shellshock vulnerability to run a malicious Perl script to scan for potential targets. Source: http://news.softpedia.com/news/Yahoo-WinZip-Servers-Compromised-Through-Shellshock-Vulnerability-461164.shtml

October 6, Securityweek – (International) **Apple updates XProtect security feature to block iWorm malware.** Apple updated its XProtect security feature to enable it to block the iWorm malware that infected over 18,500 systems running the OS X operating system. The malware can collect information on infected systems, download additional files, execute instructions, and take other actions. Source: http://www.securityweek.com/apple-updates-xprotect-security-feature-block-iworm-malware

October 4, Softpedia – (International) **Twitch bombers deliver malware and PUPs.** Researchers with Malwarebytes found the Trojan.Crypt malware and a potentially unwanted program (PUP) associated with a pay-per-install scheme disguised as 'raiding' (also known as 'bombing') utilities used to redirect users of the Twitch streaming service. Source: http://news.softpedia.com/news/Twitch-Bombers-Deliver-Malware-And-PUPs-461012.shtml

AT&T data thief fired after accessing 1,600 private customer accounts
Reuters, 7 Oct 2014: AT&T has written to a select few subscribers warning that an employee gained access to restricted customer files earlier this year, potentially viewing private information. No possible motivation for the breach has been given. The network has subsequently fired the person in question, and offered those people affected a level of compensation. A copy of the letter has been published online in template form, by the Attorney General of Vermont, which confirms the data breach took place in August this year. According to Reuters, 1,600 AT&T customers had their files accessed, and private data which may have been exposed includes Social Security numbers, driver's license numbers, and information on which AT&T services were active on each account. After apologizing, the letter outlines the ways AT&T plans to make amends. First, it will ensure any changes or charges falsely made to an account are reversed, and forwarded confirmation of the hack to law enforcement agencies. The network will also provide a year's worth of free credit monitoring, to help guard against identity theft. To read more click HERE

Windows 10 will not come with built-in key-logging capabilities
Heise Security, 7 October 2014: In case you missed it, a big fuss has been raised about the keylogging and other "spying" capabilities of the recently released Technical Preview version of Windows 10. While the claim is true, it's also true that this ability is not a secret. Anyone who downloaded the OS for testing was presented with the Privacy Statement first, and it explicitly says that "when you acquire, install and use the Program, Microsoft collects information about you, your devices, applications and networks, and your use of those devices, applications and networks." "Examples of data we collect include your name, email address, preferences and interests; browsing, search and file history; phone call and SMS data; device configuration and sensor data; and application usage," Microsoft points out. "For example, when you install the Program, we may collect information about your device and applications and use it for purposes such as determining or improving compatibility; [when you] use voice input features like speech-to-text, we may collect voice information and use it for purposes such as improving speech processing; [when you] open a file, we may collect information about the file, the application used to open the file, and how long it takes any use it for purposes such as improving performance; or [when you] enter text, we may collect typed characters and use them for purposes such as improving autocomplete and spellcheck features." To read more click HERE