Counterintelligence NEW MEXICO Working Group

NMCIWG Purple Arrow

The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
8 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 5, Softpedia – (International) **Farm supply store Rural King hacked, attackers access financial information.** The Matton, Illinois-based Rural King farm supply store began notifying customers that it experienced a data breach where attackers may have stolen names, payment card numbers, verification codes, phone numbers, addresses, and other information. The breach began February 6, was detected March 7, and attackers were completely blocked out by March 12. Source: http://news.softpedia.com/news/Farm-Supply-Store-Rural-King-Hacked-Attackers-Access-Financial-Information-436039.shtml

April 4, Associated Press – (Michigan) **Names, addresses, Social Security numbers of 2,500 stolen from state health department.** The Michigan Department of Community Health reported April 3 that an encrypted laptop and an unencrypted flash drive containing the personal information of more than 2,500 living and deceased individuals was stolen in January from the State Long Term Care Ombudsman's Office by an employee. Source: http://www.wxyz.com/news/state/personal-information-of-2500-stolen-from-state-health-department-flash-drive

April 3, Los Angeles Times – (California) **Medical data breach involves more than 170,000 additional victims.** Los Angeles County officials reported April 3 that the number of victims impacted by a medical data breach rose by 170,200, totaling 338,700 victims, after a February theft of 8 computers during a break-in at the Torrance office of Sutherland Healthcare Solutions. The computers contained personal and medical data, as well as Social Security numbers and billing information. Source: http://www.latimes.com/local/lanow/la-me-ln-sutherland-data-breach-20140403,0,7636728.story

April 4, Lansing State Journal – (Michigan) **'Phishing' attack involving MSU employees' payroll information second in last 6 months.** Michigan State University officials discovered April 1 that an estimated 10 employees had unauthorized changes to their direct deposit information in what authorities believe was a phishing attack to steal payroll earnings. Authorities continue to investigate the incident. Source: http://www.lansingstatejournal.com/article/20140404/NEWS06/304040034/-Phishing-attack-MSU-compromises-small-number-employees

April 5, Softpedia – (International) **DDoS attack enabled by persistent XSS vulnerability on top video content provider's site.** Incapsula reported that they mitigated an application layer distributed denial of service (DDoS) attack against a client which utilized a cross-site scripting (XSS) vulnerability in a popular video content provider's Web site. Malicious JavaScript code was injected into a tag associated with users' profiles, which executed whenever a legitimate user accessed the page Source: http://news.softpedia.com/news/DDOS-Attack-Enabled-by-Persistent-XSS-Vulnerability-on-Top-Video-Content-Provider-s-Site-436029.shtml

April 4, Softpedia – (International) **Upatre downloader distributed via banking-themed spam campaign.** Researchers at Trend Micro detected a spam campaign using banking-themed emails to distribute the Upatre downloader, which in a sample downloaded the Zeus trojan and the Necurs security-disabling malware. Source: http://news.softpedia.com/news/Upatre-Downloader-Distributed-via-Banking-Themed-Spam-Campaign-435975.shtml

April 4, The Register – (International) **Five-year-old discovers Xbox password bug, hacks dad's Live account.** A San Diego boy identified and reported a vulnerability in Microsoft's Xbox Live service that can allow access to a user's account by repeatedly entering 'space' characters and then hitting 'submit' when prompted for a password. Microsoft closed the vulnerability after it was reported. Source: http://www.theregister.co.uk/2014/04/04/five_year_olds_xbox_live_password_hack/

April 4, Softpedia – (International) **85% of links spotted in cyberattacks in 2013 led to compromised legitimate sites.** Websense Security Labs released their 2014 Threat Report, detailing threats and trends during the past year. The report found that 85 percent of malicious links in email and Web attacks were directed at legitimate sites that were compromised by attackers, among other findings. Source: http://news.softpedia.com/news/85-of-Links-Spotted-in-Cyberattacks-in-2013-Led-to-Compromised-Legitimate-Sites-435939.shtml

Fearing cyberattack, Israel curbs gov't websites' foreign traffic
Reuters, 3 Apr 2014: Israel will temporarily suspend some of its government websites' international traffic to fend off a potential mass cyber-attack by pro-Palestinian hackers, an Israeli security source said on Thursday, without elaborating on the threat. The precautionary measure would be in place from Friday through Monday, the source said, and include refusal of electronic payment from abroad for government services. Some routine reprogramming of websites was also on hold, the source said. The Walla news site said Israeli civil servants had also been instructed not to open emails received from foreigners. Israeli officials declined to comment. In January, an Israeli cyber security firm said hackers had broken into a Defence Ministry computer via an email attachment tainted with malicious software that looked like it had been sent by the country's Shin Bet security service. To read more click **HERE**

Zeus malware found with valid digital certificate
Network World, 3 Apr 2014: A recently discovered variant of the Zeus banking Trojan was found to use a legitimate digital signature to avoid detection from Web browsers and anti-virus systems. Security vendor Comodo reported Thursday finding the variant 200 times while monitoring and analyzing data from users of its Internet security system. The variant includes the digital signature, a rootkit and a data-stealing malware component. "Malware with a valid digital signature is an extremely dangerous situation," the company said in a blog post. To continue reading, register here to become an InsiderIt's FREE to join Learn More Already an Insider? Sign in CSO - A recently discovered variant of the Zeus banking Trojan was found to use a legitimate digital signature to avoid detection from Web browsers and anti-virus systems.   Security vendor Comodo reported Thursday finding the variant 200 times while monitoring and analyzing data from users of its Internet security system. The variant includes the digital signature, a rootkit and a data-stealing malware component.   "Malware with a valid digital signature is an extremely dangerous situation," the company said in a blog post.   Zeus is typically distributed through a compromised Web page or through a phishing attack in which cybercriminals send email that appear to come from a major bank.   A sample of the latest Zeus variant tried to trick the recipient into executing it by posing as an Internet Explorer document that included an icon similar to the Windows browser.   Because the file is digitally signed with a valid certificate, it appears trustworthy at first glance, Comodo said. The certificate is issued to "isonet ag."   When executed, the malware downloads the rootkit and a program capable of stealing login credentials, credit card information and other data a person keys into a Web form. The rootkit prevents

the malicious files from being deleted by either the computer user or AV software. Zeus malware typically launches a man-in-the-browser attack when a person visits an online banking site. The malware lets hackers create a remote session where they can see what the victim is doing and secretly intercept all data flowing from the activity. For example, if the victim transfers funds on a banking site, the payment information will display as usual, but behind the scenes the hackers will alter the transaction and send the money to another account. Zeus is one of the oldest families of financial malware. In December 2013, Kaspersky Lab discovered a 64-bit version of Zeus, an indication that hackers were preparing for the software industry's move away from older 32-bit architectures. To read more click **HERE**

Lenovo-IBM Deal Under U.S. Scrutiny Over Pentagon Server Use

Bloomberg, 4 Apr 2014: Lenovo Group Ltd. must convince government officials that buying a server unit from International Business Machines Corp. won't give China back-door access to U.S. secrets and infrastructure. The wrinkle is that the Pentagon, the FBI and the nation's biggest telecommunications companies buy the IBM servers, according to people familiar with the matter and an analysis by Bloomberg Industries. Use of the servers by the government, telephone networks and other potentially sensitive customers will spark close scrutiny from the interagency group known as the Committee on Foreign Investment in the U.S., which investigates national- security risks of foreign acquisitions of domestic companies. "It's kind of the perfect storm of issues," said Anne Salladin, a former Treasury Department official who worked on CFIUS reviews and is now at Stroock & Stroock & Lavan LLP in Washington. "Any foreign acquirer with this kind of asset purchase is very likely to be something that CFIUS would want to take a look at." Beijing-based Lenovo, which announced the $2.3 billion IBM purchase Jan. 23, has formally sought approval for the deal from CFIUS, according to a person with knowledge of the matter. Acquisitions of U.S. businesses by Chinese buyers are rising, increasing tension in Washington over Chinese access to U.S. technology. CFIUS reviews can take as many as 75 days Lenovo, which bought IBM's personal computer business in 2005, has been briefing officials on the deal, pointing out that it won't have access to the servers because IBM will continue maintenance on the equipment, according to a person familiar with the matter. That agreement lasts for five years and could be extended, said the person. The service agreement may help ease the security review by CFIUS, which examined more than double the number of transactions by Chinese investors in 2012 than it did the previous year, making them the most scrutinized foreign buyers of American assets ahead of the U.K., according to the committee's most recent report to Congress. "The government is going to take a look at the degree of penetration of the servers, where they are, how old they are, what the reach-back capability might be," Mario Mancuso, an attorney at Fried, Frank, Harris, Shriver & Jacobson LLP. "Could they use the servers as a means of insertion into U.S. government networks and data systems?" Lenovo agreed to pay a fee that's more than double the typical size should it fail to aquire IBM's low-end server unit, people familiar with the matter said in January. The breakup charge of about $200 million, according to one of the people, highlights the risk the Chinese company has chosen to bear for it's largest-ever purchase. U.S. officials will also examine any use of the servers in critical infrastructure, such as chemical plants and electric- utility companies, Michael Wessel, a member of the U.S.-China Economic and Security Review Commission. "Exfiltration and infiltration are the issues," Wessel said. "Can they get access to servers in some way and take data out or can they infiltrate the system to put in trap doors, viruses, malware or be able to take down systems in a potential conflict situation?" A Bloomberg Industries analysis of federal contract data shows government purchasers of IBM BladeCenter servers include the Pentagon, the FBI, and the Department of Homeland Security. Chris Padilla, the company's vice president for governmental programs, told Bloomberg in January that IBM servers are used by the U.S. government, without identifying which agencies. Air Force Lieutenant Colonel Damien Pickart, a spokesman for the Pentagon, acknowledged that the Lenovo-IBM transaction is pending before CFIUS and added that the Defense Department, which is a member of the committee, would be involved in the deliberations. He declined to comment further and referred questions to Treasury, which chairs the committee. Holly Shulman, a CFIUS spokeswoman, declined to comment. Spokesmen for the FBI and the Department of Homeland Security didn't respond to requests seeking comment. The servers are also embedded in telephone networks operated by AT&T Inc., Verizon Communications Inc. and Sprint Corp., according to three people familiar with the technology. IBM spokeswoman Deirdre Murphy Ramsey declined to comment on the Armonk, New York-based company's clients. IBM is prepared for a "comprehensive review" by CFIUS and is "confident of a positive outcome," she said. Mark Siegel, an AT&T spokesman, Richard Young, a Verizon spokesman, and John Taylor, a Sprint spokesman, declined to comment. Lawmakers and the Obama administration have tried to prevent China's Huawei Technologies Co. and ZTE Corp. from doing business in the U.S. A 2012 report by the House Intelligence Committee cited security threats posed by Chinese telecommunications companies and urged the government to block transactions by Huawei and ZTE. The companies provide "a wealth of opportunities" for Chinese intelligence agencies to insert malicious hardware or software into U.S. telecommunications networks, according to the report. Then U.S. Commerce Secretary Gary Locke expressed "deep concerns" to Sprint in 2010 that Huawei might win a contract to upgrade the mobile-phone carrier's network. "Anything now with China gets attention," said James Lewis, a senior fellow at the Center for Strategic and International Studies. "But Lenovo, because it's not a state- owned enterprise and because they've done deals successfully in the past, they're really well placed to get through." Lenovo would get IBM servers that use x86 processors, an industry-standard technology. The transaction includes BladeCenter and Flex System blade-style servers -- slim devices that slide into racks -- along with switches that run corporate computer networks. IBM will keep its System z mainframes, Power servers and other higher-end hardware. Lenovo is working cooperatively with CFIUS to win clearance, spokesman Brion Tingler said in a statement. The company has had three previous acquisitions cleared by the committee, including the 2005 IBM deal. While the companies say they expect to win clearance from CFIUS, Lenovo will probably have to agree to restrictions on the business, according to lawyers who advise companies on deals that require U.S. security review. Those agreements can include requirements that only U.S. citizens handle certain services, independent audits, guidelines for handling government contracts, and termination of certain business activities, according to CFIUS's most recent report to Congress. "This is not just some Chinese company you've never heard of," said Stephen Paul Mahinka, a lawyer at Morgan, Lewis & Bockius LLP. "There are ways in which you can protect U.S. interests while at the same time not preventing the acquisition." While servers can store large collections of sensitive data, the risks associated with them are about the same as that from laptops and smartphones, which consume the same data and have access to the servers, said Michael Belton, a security expert at cybersecurity company Rapid7. Once installed in a network, servers are also more heavily defended and monitored, he said. "There isn't a large difference between a server and a laptop," Belton said. "Modern laptops can and do store as much sensitive data as a server." To read more click **HERE**

CryptoDefense developers "forget" decryption key on victims' computer

Heise Security, 4 Apr 2014: A new piece of ransomware is targeting gullible users, but its developers have made a critical mistake that should allow users to decrypt the affected files without paying the demanded ransom. That ransomware is extremely effective and nets considerable money to the criminals that wield it is not news, and it consequently shouldn't come as a surprise that they are trying to copy the success of Cryptolocker. CryptoDefense - as the new "ransomcrypt" malware has been dubbed - was first spotted in late February 2014, and currently predominantly targets mostly usersin the US, UK, Canada and Australia. "Using the Bitcoin addresses provided by the malware authors for payment of the ransom and looking at the publicly available Bitcoin blockchain information, we can estimate that this malware earned cybercriminals over $34,000 in one month alone (according to Bitcoin value at time of writing)," Symantec researchers shared. The malware arrives on the victims' computer via spam email. As they open the malicious attachment, the malware is installed and contacts a C&C server. This triggers the encryption and the generation of a private decryption 2,048-bit RSA key that is then sent to the C&C. As you can see, it threatens to destroy the key after a month, and instructs the victims to access their personal page via the Tor network - it also explains how to do this. Once the victims land on this anonymous payment web page, they are urged to pay 500 US dollars or Euros to get the decryption key, and are threatened with a 100 percent increase of the ransom if they don't pay up by a specific date. "The cybercriminals offer proof through a 'My screen' button, included on the payment page, that they have compromised the user's system by showing the uploaded screenshot of the compromised desktop. They also offer further proof that decryption is feasible by allowing the victim to decrypt one file through the 'Test decrypt' button.

They then proceed to educate their victim on how to get hold of Bitcoins to pay the ransom," the researchers point out. Still, with all these precautions, the criminals have made one crucial mistake: a copy of the private decryption key that is created on the infected computer - via Microsoft's own cryptographic infrastructure and Windows APIs - remains on it even after it is sent to the C&C server. Users can find it in the Application Data > Application Data > Microsoft > Crypto > RSA folder. This is good news for those who haven't already paid the ransom, but this situation will not likely remain the same for long, as the developers of the malware are expected to soon fix the glitch. To read more click **HERE**

The U.S. Wants To Be Upfront With China about Cyberwarfare
Yahoo News, 7 Apr 2014: The Obama administration held briefings with Chinese military leadership about the United States' growing cyberwarfare program, according to a new report from The New York Times. In a speech planned for Tuesday at the People's Liberation Army's National Defense University, Defense Secretary Chuck Hagel plans to bring up the issue, and the fact the the Chinese have not been similarly forthright in detailing their cyber initiatives. The effort, senior Pentagon officials say, is to head off what Mr. Hagel and his advisers fear is the growing possibility of a fast-escalating series of cyberattacks and counterattacks between the United States and China. … American officials say their latest initiatives were inspired by Cold-War-era exchanges held with the Soviets so that each side understood the "red lines" for employing nuclear weapons against each other. America plans to have more than 6,000 cyberwarriors by the end of 2016 — more than triple the current numbers — and the Pentagon plans to spend $26 billion on related technology programs over the next five years. In the past year, the pace of cyberattacks from China has increased. Most of these attacks target technology companies in Silicon Valley, as well as military contractors and energy companies. The Obama administration's hopes for these back-channel talks to establish norms and avoid a cyberattack escalating into full-scale conflict. To read more click **HERE**

European Court Rules ISPs Won't Have to Hold Data for up to Two Years Anymore
SoftPedia, 8 Apr 2014: Today, The European Court of Justice has decided to tear to pieces a previous directive that required Internet Service Providers (ISPs) to retain data for two years. The initial directive has been deemed "invalid" by the Court since it entails a "wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary," the ruling reads. Anyone's private life could be interfered with without their knowledge due to the fact that records could be kept for up to two years and the collected information used at any time. Basically, the court said that this amounted to "constant surveillance." The information retained by ISPs includes details about the identity of the persons that one communicates with and by what means, at what times and from which locations, as well as the frequency of these communications. As a whole, this provides way too much insight into a person's private life. The directive has been around for seven years, but now it has been found to clash with the privacy rights that the bloc wants for its citizens. The court admits that the purpose of the directive – collecting data to fight against serious crime and for public security – is completely valid. However, the piece of legislation "has exceeded the limits imposed by compliance with the principle proportionality." At the same time, the directive was too broad and did not come with enough limitations. For instance, while the retention period was set between six months and two years, it did not specify on which criteria the period of detention was determined. Also, the legislation did not provide enough safeguards to ensure effective protection of the data against the risk of abuse and against any unlawful access and use of the data. Even worse, the Court points out that the directive does not require that the data be retained within the European Union, which means that the EU cannot fully ensure the control of compliance with the requirements of protection and security by an independent authority. Basically, this indicates that the European Union is concerned that data belonging to citizens could be served on a silver tray to the United States and its mass surveillance network. The fact that the decision comes as the European Union is looking into building its own local set of networks to protect the data from the eyes of the NSA cannot be overlooked. To read more click **HERE**

Adobe Flash Player 13.0.0.182 Now Available for Download
SoftPedia, 8 Apr 2014: Just like it happens on the second Tuesday of every month, Adobe rolled out a new version of its Flash Player, obviously bringing a number of fixes and improvements for all platforms. At this point, the parent company has only updated the download links, so no release notes are available for the time being, but it's safe to assume that it's focused on fixing bugs and addressing security issues in the previous builds. Adobe has recently matched its security release cycle with Microsoft's Patch Tuesday rollout, so the company launches new updates for its software on the second Tuesday of each month, just like the Redmond-based software giant does to fix vulnerabilities in Windows, Office, and other products across its range. Microsoft is also delivering the same Flash Player version via Windows Update to all users running Windows 8 and 8.1, as the company has pledged to keep users up-to-date by bundling Adobe's client runtime environment in newer flavors of Internet Explorer. Of course, all users are strongly recommended to install this new version, so download Adobe Flash Player 13.0.0.182 as soon as possible to make sure that you're fully secure when browsing the web. If you're using Internet Explorer, the same version will be shipped to you later via Windows Update. To read more click **HERE**

Windows 8.1 Update Officially Launched, Download Links Now Available
SoftPedia, 8 Apr 2014: Microsoft was expected to launch Windows 8.1 Update later today via Windows Update, but the company has just made the download links for all files needed to deploy the new OS version available online. As you can see in the list below, Microsoft has published the download links for all Windows 8.1 Update versions, so you can install it on both 32- and 64-bit devices, but also on ARM tablets such as Microsoft's very own Surface RT and Surface 2. Keep in mind that this manual download method could take a little bit longer, but it still lets you deploy the new Windows 8.1 Update right now if you can't wait for the automatic method via Windows Update. For those wondering, KB2919355 is the main package, so if you're running a fully up-to-date Windows 8.1 installation, this is the only package that needs to be downloaded. On the other hand, all the other KB files contain necessary files to successfully deploy Windows 8.1, so in case you're experiencing any error during the installation process, make sure that you also get these too. To read more (and obtain the download links) click **HERE**

Microsoft Word Users Under Attack Right Now, Expert Warns
SoftPedia, 5 Apr 2014: Microsoft has already announced that a critical security patch for Word is coming on Patch Tuesday, but it turns out that more attacks have been spotted out in the wild and lots of users could be affected. Wolfgang Kandek, CTO of Qualys, used an analysis made by McAfee to point out that "the attacks are real and happening now," which means that basically everyone still using a Microsoft Word version that's vulnerable to exploits should take the necessary steps to protect themselves right now. "The exploit does not look that hard to replicate with the information provided. Beyond patching it makes sense to disable RTF opening any way, which is what the FixIt in KB2953095 does. It certainly looks as if there is more potential for this type of vulnerability that can be found with relatively little investment into file fuzzing," Kandek explained. According to McAfee analysis, if an attacker successfully exploits the vulnerability, he could easily run malicious code on the target computer, and then perform a number of other tasks, such as injecting malware and other dangerous tools to compromise data owned by the user. The vulnerability comes down to the way Microsoft Word handles RTF documents, so disabling support for this particular file format in Microsoft's word processor would be the best way to stay secure until a full patch is being released. Those who are running Outlook 2007, 2010 or 2013 to send and receive emails are even more vulnerable, as the email client uses Microsoft Word as the default viewer for attached documents, so it's a lot easier to get hacked. Kandek has provided more instructions for those who are trying to block any potential attacks, pointing out that avoiding downloading suspicious RTF documents is usually the best way to stay secure. "The current workaround is to disable RTF as a supported format in Microsoft Office. A secondary recommended action is to work with plain text in e-mails, which is generally a recommended safeguard that prevents the 'drive-by' characters of these types of attacks," he said. Microsoft will finally address the flaw on Patch Tuesday next week, so make sure that your computer is configured to

automatically receive updates as soon as they are released.   All versions of Microsoft Word are said to be affected by this vulnerability and the software giant has already confirmed that it is aware of some “limited” attacks happening right now, which is just another sign that RTF documents should be handled with caution these days. To read more click **HERE**

Steam Users Have Been Advised to Refrain from Using Its Services Due to Security Issue
SoftPedia, 8 Apr 2014: It is recommended not to use any Steam services until Valve issues a fix for the recently discovered Heartbleed vulnerability, a bug in the popular OpenSSL cryptographic software library that two thirds of the Internet is using. SteamDB warned the gaming community via Twitter to not use any Steam services, at least not until Valve issues a fix for a recently discovered vulnerability, pointing out that the vulnerability is especially dangerous for Steam partners. The mysterious warning then revealed that the issue at hand is the Heartbleed Bug, a vulnerability that is dangerous to everyone, but especially dangerous to developers, because they deal with more sensitive content than regular users. The recently discovered security weakness allows evildoers to steal the information that is normally protected by the SSL/TLS encryption used to secure communication over the Internet. SSL (secure sockets layer) and TLS (transport layer security) provide security and privacy for all communication taking place over the Internet, for applications such as web, email, instant messaging and even some virtual private networks, and the Heartbleed bug allows anyone to read the memory of the systems protected by the versions of the OpenSSL software which contain the vulnerability. The bad news is that as long as the vulnerable version of OpenSSL is in use, it can be abused without leaving a trace, and service providers have to install the appropriate fix as quickly as it becomes available in order to prevent further damage. To read more click **HERE**

UK Department of Culture, Media and Sport Twitter Account Hacked
SoftPedia, 7 Apr 2014: The verified Twitter account of the United Kingdom’s Department of Culture, Media and Sport (@DCMS) was hijacked over the weekend. The hacker posted three messages referencing MP Maria Miller on the compromised feed. The tweets were quickly deleted, but Twitter users posted screenshots of the account while it was hijacked.   “Seriously though guys which one of us hasn’t embezzled and cheated the taxpayer?? #FreeMariaMiller,” read the first tweet.   The second, which came one minute later, read, “@Maria_MillerMP is like modern day Robin Hood, she robs the poor to help the rich.” In the last message, the hacker noted, “Is Maria @Maria_MillerMP guilty? We will let the public decide.” The DCMS quickly deleted the tweets, but hasn’t mentioned anything about them. However, the department’s representatives told The Inquirer that “the DCMS Twitter account was hacked but was quickly secured.” An investigation has been launched. It’s uncertain if the hacker is an outsider or someone from within the organization who had access to the account. To read more click **HERE**

Anonymous Hackers Target Websites of Israeli Banks and Government
SoftPdia, 7 Apr 2014: Today, April 7, hacktivists from several countries have launched a new campaign against Israel. Hundreds of websites have been targeted in the pro-Palestine campaign dubbed Operation Israel (OpIsrael). Cyberattacks of all types have been launched. Some websites have been disrupted by distributed denial-of-service (DDOS) attacks, some have been defaced, while from others the attackers have leaked information. The DDOS attacks have mainly been targeted at the websites of government agencies and financial institutions – in general, sites that are not too easy to breach. A large number of Israeli commercial websites have been defaced and data has been leaked from their databases.   The hackers, most of which affiliated with the Anonymous movement, announced their plans months ago.   As a result, the Israeli government has taken steps to protect computer systems against attacks, the Times of Israel reported. Some government websites have been shut down and the public has been warned not to open suspicious emails since some of the hackers target citizens and businesses, not just government entities. This is not the first time hacktivists launch OpIsrael. Hundreds of websites were targeted in the past years in similar operations, but Israeli officials have always denied that the attacks caused any real damage. So let’s take a look at this year’s campaign. Has it caused any damage?   As with most hacktivist operations, OpIsrael has attracted the attention of news

organizations from all over the world. However, when it comes to actual hacking, not much has been accomplished. Some high-profile websites have been disrupted briefly with DDOS attacks. Most of the breached and defaced websites belong to small businesses whose owners probably haven't invested in security. As with previous OpIsrael attacks, there are a lot of fake hacks. Many of the hackers taking part in the operation are publishing old data and claiming to have leaked it from various companies and organizations. In fact, most of the info we've analyzed is either old, or highly suspicious. For instance, one hacking group claimed to have leaked the credit cards of hundreds of Israeli citizens. However, the exact same data was leaked back in September 2013. Furthermore, it appears to belong to users from all around the world (mainly Latin America), not just from Israel, which likely means that it was stolen with the aid of malware or through a phishing scheme, not from a company's databases. To read more click **HERE**

Neiman Marcus Reportedly Breached by Major Russian Cybercrime Group

SoftPedia, 7 Apr 2014: A major criminal ring in Russia is said to be behind the recent breach suffered by high-end retailer Neiman Marcus. Authorities have been trying to dismantle the group for years, but without too much success. Two unnamed former US officials have told Bloomberg that the group in question is said to be responsible for stealing over 160 million credit card records over a period of seven years. The list of victims includes Carrefour, J.C. Penney, Visa, Citigroup, 7-Eleven, JetBlue Airways, and many others. Over 100 companies are said to have been targeted. US authorities have been working with Russian agencies in an effort to bring down the syndicate, but to no avail. Some officials believe that the Russians only pretended to assist the FBI with its investigation so that they could track down hackers who they could use for their own goals. Some members of the cybercrime group have been indicted, and some of them have even been arrested. However, it appears that these are low-level players who could be easily replaced by the masterminds of the operation. Initially, it was believed that the same hackers who breached Target were responsible for the attack on Michaels and Neiman Marcus. However, as more details came to light, it became clear that there were different perpetrators. To read more click **HERE**

End of Windows XP support spells trouble for consumers, businesses

Fox News, 8 Apr 2014: Microsoft is ending support for Windows XP on Tuesday, a move that could put consumers and businesses at risk for cyber crime. An estimated 30 percent of computers being used by businesses and consumers around the world are still running the 12-year-old operating system. "What once was considered low-hanging fruit by hackers now has a big neon bull's eye on it," says Patrick Thomas, a security consultant at the San Jose, Calif.-based firm Neohapsis. 'What once was considered low-hanging fruit by hackers now has a big neon bull's eye on it.' - security consultant Patrick Thomas. Microsoft has released a handful of Windows operating systems since 2001, but XP's popularity and the durability of the computers it was installed on kept it around longer than expected. Analysts say that if a PC is more than five years old, chances are it's running XP. While users can still run XP after Tuesday, Microsoft says it will no longer provide security updates, issue fixes to non-security related problems or offer online technical content updates. The company is discontinuing XP to focus on maintaining its newer operating systems, the core programs that run personal computers. The Redmond, Wash.-based company says it will provide anti-malware-related updates through July 14, 2015, but warns that the tweaks could be of limited help on an outdated operating system. Most industry experts say they recognize that the time for Microsoft to end support for such a dated system has come, but the move poses both security and operational risks for the remaining users. In addition to home computers, XP is used to run everything from water treatment facilities and power plants to small businesses like doctor's offices. To read more click **HERE**