THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

28 July 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

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

July 24, Help Net Security – (International) **Six men charged in StubHub cyber-theft case.** Six individuals were charged in the U.S. in connection with an alleged cybercrime ring that took over accounts on online ticket marketplace StubHub, used victims' credit cards to purchase tickets to various entertainment events in New York City, sell the tickets, and then launder the proceeds through PayPal accounts and bank accounts in the U.S., U.K., Canada, Germany, and Russia. The alleged fraud totaled around $1 million and affected over 1,000 user accounts. Source: http://www.net-security.org/secworld.php?id=17164

July 23, Massachusetts Attorney General's Office – (Massachusetts; Rhode Island) **Women & Infants Hospital to pay $150,000 to settle data breach allegations involving Massachusetts patients.** The attorney general of Massachusetts announced July 23 that Women & Infants Hospital of Rhode Island agreed to pay $150,000 to settle allegations that it failed to protect the personal health information of 12,127 patients in Massachusetts after an April 2012 data breach. The hospital discovered that 19 unencrypted back-up tapes from two if it's Prenatal Diagnostic Centers went missing in 2011 and authorities determined that they did not properly report the breach under the State's notification statute. Source: http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-07-23-women-infants-hospital.html

July 24, The Register – (International) **50,000 sites backdoored through shoddy WordPress plugin.** A researcher with Sucuri reported that around 50,000 Web sites were vulnerable to malware injection, defacement, and spam due to a vulnerability in the MailPoet plugin for WordPress. The vulnerability can affect Web sites that do not run MailPoet if the vulnerable plugin is present elsewhere on the same server. Source: http://www.theregister.co.uk/2014/07/24/50000_sites_backdoored_through_shoddy_wordpress_plugin/

July 24, Softpedia – (International) **Fake Googlebots used for layer 7 DDoS attacks.** Incapsula issued a report that shows how malicious Web crawlers that mimic Googlebots to bypass security are being used for various malicious purposes. The majority of the fake crawlers were used for collecting marketing information while 23.5 percent were used for application layer distributed denial of service (DDoS) attacks. Source: http://news.softpedia.com/news/Fake-Googlebots-Used-for-Layer-7-DDoS-Attacks-451984.shtml

July 23, V3.co.uk – (International) **DDoS attackers turn attention to SaaS and PaaS systems, Akamai reports.** Akamai released its Q2 2014 Global DDoS Attack Report, which found a 22 percent increase in distributed denial of service (DDoS) attack activity in the second quarter of 2014. The report also found that around half of DDoS attacks targeted IT infrastructure, with vendors of cloud services such as Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) being common targets. Source: http://www.v3.co.uk/v3-uk/news/2356828/ddos-attackers-turn-attention-to-saas-and-paas-systems-akamai-reports

July 23, The Register – (International) **Apple fanbois SCREAM as update BRICKS their Macbook Airs.** Users of Apple's 2011 Macbook Air reported experiencing nonresponsive systems after applying a version 2.9 EFI firmware update to their systems, while others reported difficulties installing the update. Source: http://www.theregister.co.uk/2014/07/23/apple_macbook_air_update_bricks_fanbois_machines/

July 23, Securityweek – (International) **Metro News website compromised to serve malware.** Researchers at Websense reported July 22 that the Web site of newspaper Metro.us was compromised and used to redirect visitors to a malicious Web site hosting the RIG exploit kit. The RIG exploit kit then attempts to exploit any present vulnerabilities in users' software to install a piece of malware identified as Win32/Simda. Source: http://www.securityweek.com/metro-news-website-compromised-serve-malware-rig-exploit-kit

July 23, Softpedia– (National) **Wall Street Journal acknowledges system breach.** The Wall Street Journal confirmed that its systems were compromised when an attacker gained access to news site's graphics servers, but that an ongoing investigation did not reveal any signs of damage or tampering. An individual using the handle "w0rm" known for breaching the systems of CNET claimed responsibility and stated that they were willing to sell a database stolen in the breach for one Bitcoin. Source: http://news.softpedia.com/news/Wall-Street-Journal-Acknowledges-System-Breach-451796.shtml

July 24, Greenwood Index-Journal – (South Carolina) **Self Regional announces security breach of patient info.** Self Regional Healthcare in Greenwood notified at least 500 patients July 24 of a potential security breach after two thieves broke into the Support Services Center May 25 and took a hospital-owned laptop. Police arrested and charged two men June 10 in connection with the theft where one of the suspects admitted to panicking and throwing the password protected laptop into Lake Thurmond. Source: http://www.indexjournal.com/Content/Default/Homepage-Rotating-Articles/Article/Self-Regional-announces-security-breach-of-patient-info/-3/225/26721

July 24, Arizona Republic – (Arizona) **Phoenix police recover $56,000 in stolen computers.** Four teenagers could face charges in connection to stealing about 50 Mac computers worth about $56,000 from the Desert Sands Middle School in Maryvale between July 22 and July 23. Police found almost all of the stolen equipment in a trailer after apprehending a suspect who returned to the school and set off a burglary alarm. Source: http://www.azcentral.com/story/news/local/phoenix/2014/07/25/dozens-of-computers-recovered-in-middle-school-burglary-abrk/13145341/

July 25, Softpedia – (International) **Cloud botnets used for mining crypto-currency.** Researchers from Bishop Fox created a botnet capable of mining several hundred dollars in Litecoin crypto-currency on a daily basis using free services of multiple cloud-computing businesses. Conducted distributed denial of service (DDoS) attacks was determined to be another way to use the machines. Source: http://news.softpedia.com/news/Cloud-Botnets-Used-for-Mining-Crypto-Currency-452030.shtml

July 24, SC Magazine – (International) **Sony to shell out $15M in PSN breach settlement.** Sony released a statement July 24 claiming it reached an agreement to pay $15 million in a preliminary settlement associated with the April 2011 hacking of its PlayStation Network system, its on-demand service Qriocity, and gaming portal Sony Online Entertainment, exposing the personal data of roughly 77 million users. Source: http://www.scmagazine.com/sony-to-shell-out-15m-in-psn-breach-settlement/article/362720/

July 24, Threatpost – (International) **More details of Onion/Critroni crypto ransomware emerge.** Kaspersky Lab and other researchers found that the Critroni or CTB-Locker dubbed Onion uses a number of features that separate it from other forms of malware including that the ransomware is spread through Andromeda using a version of the asymmetric ECDH (Elliptic Curve Diffie-Hellman) algorithm. Source: http://threatpost.com/onion-ransomware-demands-bitcoins-uses-tor-advanced-encryption/107408

July 24, Softpedia – (International) **Popular wireless home alarms can be hacked from afar.** Two security researchers found that wireless home alarm systems are vulnerable to remote hijacking which would allow for access into the protected environment without tripping the alarm due to the signals lack of encryption or authentication. The tools used to hack into systems are available for purchase, potentially allowing intruders to completely disable the alarm from 10 feet. Source: http://news.softpedia.com/news/Popular-Wireless-Home-Alarms-Are-Easy-to-Hack-452023.shtml

LZO Exploit Closed in Ubuntu 14.04 LTS and Ubuntu 12.04 LTS
SoftPedia, 28 Jul 2014: Canonical has published details in a security notice about an LZO vulnerability that has been found and fixed in Ubuntu 14.04 LTS and Ubuntu 12.04 LTS operating systems. The Ubuntu developers have fixed a problem and users have been asked to update their system in order to patch the issue. According to the security notice, "Don A. Bailey discovered that LZO incorrectly handled certain input data. An attacker could use this issue to cause LZO to crash, resulting in a denial of service, or possibly execute arbitrary code." For a more detailed description of the problems, you can see Canonical's security notification. Users should upgrade their Linux distribution in order to correct this issue. The flaw can be fixed if you upgrade your system(s) to the latest libminiupnpc8 package specific to each distribution. To apply the patch, users can simply run the Update Manager application. If you don't want to use the Software Updater, you can open a terminal and enter the following commands (you will need to be root): sudo apt-get update sudo apt-get dist-upgrade In general, a standard system update will make all the necessary changes. You don't have to restart the PC in order to complete the procedure, the update will suffice. To read more click **HERE**

Coin-Sized USB Flash Drive Released by PNY with 64 GB Capacity
SoftPedia, 28 Jul 2014: Reducing flash drives to tiny sizes has been turned into something of an art form on the portable storage market, and PNY has decided to become one of the most skillful artists in this. Case in point, the company has introduced the Micro M2 USB flash drive. Not to be confused with M.2 SSDs that alternate between leaving the world in stunned awe or halfway between teased and disappointed. The new flash drive from PNY is as small as a coin, with a height of just 18 mm / 0.70 inches and a weight of 1.8 grams / 0.06 oz. Yet despite that, it can pack up to 64 GB of storage space. Basically, PNY took the principles that make it possible to have 64 GB microSD memory cards and applied them to a flash drive, which use the same type of NAND Flash storage technology as them. There are lower-capacity drives though, of down to as little as 4 GB. In all situations, however, the writing speed hovers around 10 MB/s and the read speed is of up to 32 MB/s (USB 2.0 performance). The PNY Micro M2 flash drive ships in a metallic case that is scratch and dust-resistant. The matter finish makes fingerprints less likely to be left behind as well. Finally, a small hole allows you to easy hang the thing off a lanyard or key chain. PNY's Micro M2 flash drive ships with a 5-year warranty and is compatible with Windows 2000, XP, Vista, 7 and 8, plus Max OS 10.2 and above operating systems. Alas, the price was not provided. To read more click **HERE**

Open Ports Pose Risk on Android
SoftPedia, 28 Jul 2014: Security researchers found a vulnerable Android app that allowed an attacker to send messages to the phone and trigger various commands, without any sort of authentication. The mobile threats team at Trend Micro discovered that the mobile app of Meituan, a Chinese site that promotes discount deals in a similar way as Groupon, would listen on TCP port 9517 in order to receive messages from a server, but the sender would not be authenticated. Basically, a command on the phone can be triggered from any online machine once communication is established. "It parses the received TCP data in a certain format and then sends android.intent.action.VIEW with the 'intent' in the received data," says Veo Zhang, mobile threat analyst at Trend Micro, in a blog post about the flawed code. As far as the risks faced by the users of a vulnerable version of the app are concerned, the analyst said that the phone could be used for sending messages to premium rate services that bring revenue to cybercriminals. The

security glitch in Meituan's app has been removed, after the security company disclosed it privately to the affected party on June 3, allowing them time to come up with a fix and deploy a secure version of the product, two days later. The Trend Micro security researcher also draws attention to the large number of Android apps listening on an open TCP port. The risk presented by this is that the device is exposed online, and in lack of a firewall to monitor network communication and prevent malicious activity, it falls on the shoulder of the app developer to implement the necessary security measures that could fight against compromising the device. However, the Android security model does not support firewall protection of any sort at the moment. Another risk on Android is represented by vulnerabilities in Linux, the kernel the mobile platform relies on. "Because Android is based on the Linux kernel and still uses many native Linux APIs, Linux vulnerabilities may affect Android as well. For example, CVE-2014-3153 was used by root exploit tools like TowelRoot. Another example was CVE-2014-0196," Zhang says. TowelRoot is a rooting app developed by Geohot, and it relies on exploiting a vulnerability in Linux futex system. Although a patch has been released for Linux, many Android versions, build 4.4 included, are still susceptible to the security flaw, which could offer administrator privileges to a potential attacker. To read more click **HERE**

Hackers Trick Facebook Users into Self Cross-Site Scripting (XSS) Scam

SoftPedia, 28 Jul 2014: Under the pretext of providing a method to hack into any Facebook account, cybercriminals incite unsuspecting users into pasting malicious code into their web browser. This scam is relied on social engineering, because all the scammer has to do is convince the user to follow a short list of steps that ends with pasting a specific code string into the JavaScript Console accessible in the web browser. However, all the wannabe hacker ends up with is compromising their own account, giving the crook the possibility to use it to launch future malicious campaigns or to spread current ones. The message from the cybercroosks can come via email or as a Facebook post from one of the friends in the list of the potential victim. The instructions for taking over someone else's account are suitable for both Google Chrome and Mozilla Firefox users. In a sample text provided by Facebook, the scammer describes the entire procedure as a three-step operation that begins with navigating to the Facebook profile that is to be compromised. Next, from the context menu (right click) of the page, the "Inspect element" needs to be selected, and then the Console tab. Following these steps leads to the exact same result in both Firefox and Chrome. The last stage of the hack consists of pasting the code provided by the crook and running it by hitting the Enter key. By having access to a Facebook account, the cybercriminals are free to use it as they see fit; but spreading all sorts of malicious campaigns is the main purpose. These can end with compromising other profiles or with deceiving the victim into completing surveys or downloading potentially unwanted software, both activities putting money into their pockets. Infecting computers with malware that can collect banking details and send them to a remote location controlled by the attackers can also be carried out via this type of malicious activity. Facebook has added the scam on the list of threats its users have been observed to fall victim to. "Self-XSS, or a cross-site scripting scam, is designed to trick you into giving away access to your Facebook account. If a scammer gets access to your account, they can post and comment on things on your behalf," reads their post. Users of the social network are strongly advised not to copy and paste suspicious links in order to avoid the risk of cross-site scripting. To read more click **HERE**

Indian Hacker Arrested for Breaking into Microsoft Website, Stealing Product Keys

SoftPedia, 28 Jul 2014: Microsoft continues the struggle to reduce piracy across the world, and as part of its global efforts the company collaborated with the Indian authorities to arrest an individual who reportedly hacked its servers and stole several product keys for its software. Redmond worked together with the Central Bureau of Investigation to find and arrest an Indian youth who managed to break into some of its websites to access product keys which were then sold online, according to a press statement. The Central Bureau of Investigation confirmed the report in an official press release and added that it seized several hard disks and routers that were used to commit the fraud and which could serve as evidence during the trial. "The Central Bureau of Investigation has arrested a private person at Chennai

(Tamil Nadu) in a case relating to offences of alleged cyber crime offences for the purpose of stealing Microsoft's product keys as well as cheating unsuspecting consumers," Indian authorities said. "During investigation, CBI has found the perpetrator (a private person) of the said crime at Chennai. Searches have been conducted at his premises & in Chennai which led to recovery of Hard disks of Computer System; Router used for committing the crime along with numbers of Microsoft Product Kits and other documents. Account of the accused which he has used to collect the amount of sale of Microsoft Product Keys was also freezed." It's no secret that Microsoft as a software company is one of the most affected entities when it comes to piracy, so its fight against individuals who are selling counterfeited software is clearly a priority in order to improve its business. Of course, the company has launched several campaigns not only to make consumers aware that genuine software is the best choice for their computers, but also to encourage retailers and partners to purchase legitimate applications in order to avoid losing customers' trust. "While counterfeit software is offered at a lower price, there can be hidden costs, such as poor user experience, damage to devices, and the loss of personal data. Genuine software is the best deal and the right choice to avoid potential financial, professional, and social setbacks," the company explains in the description of one of its anti-piracy campaigns. China is said to be one of the leading countries as far as piracy is concerned, with former CEO Steve Ballmer himself saying that 9 out of 10 copies of Windows in the country are pirated. To read more click **HERE**

Antivirus Is as Vulnerable as Any Other Product

SoftPedia, 28 Jul 2014: Using a custom fuzzing testing suite and running basic local and remote checks, a security researcher found numerous remotely exploitable vulnerabilities in multiple antivirus software solutions. He showed that security measures present in these products could be bypassed just like in any other, and that they provided multiple entry points to the system. Joxean Koret from the Singapore-based Coseinc, a private company that offers information security services, explained how software designed to protect users from malware actually offers threat actors an increased number of attack vectors that can be leveraged to gain access to the victim's system. Since most antivirus products enjoy a default trust that allows them to run with top privileges, finding a bug in them and exploiting it allows an attacker the same privileges on the affected system. At the SyScan 360 security conference in Beijing, Koret provided a simple example, saying that "most antivirus engines update via HTTP only protocols." Relying on the man-in-the-middle (MitM) attack, "one can install new files and/or replace existing installation files," which " often translates in completely owning the machine with the AV engine installed as updates are not commonly signed." The researcher provides a list with some vulnerabilities he found when testing his tools on reputed antivirus products. The results included heap overflows, remote vulnerabilities, integer overflows, local privilege escalation, as well as command injection possibilities. The list of products with one or more of these glitches includes Avast, Bitdefender, Avira, AVG, Comodo, ClamAV, DrWeb, ESET, F-Prot, F-Secure, Panda, and eScan. Koret has said that he downloaded the antivirus (AV) engines, which are the core of the antivirus product, with a Linux version he found. "The core is always the same with the only exception of some heuristic engines," he explains. Moreover, he used some special methods to make Windows-only engines run on Linux. It seems that although AV engines are compiled with ASLR turned on, only the core components are protected this way, and other parts, like the graphical user interface and some libraries, are not. If certain conditions are met, such as the use of the built-in emulating tool, some of the engines create RWX (read/write/execute permissions) pages at fixed addresses and disable DEP (data execution prevention). A possible compromise scenario would be for an attacker to send a ZIP archive that forces the emulator to be used, containing an exploit, the researcher says in the slides for the conference. As such, taking advantage of memory leaks in the emulators or leveraging other vulnerabilities would permit access to the system's higher functions. The conclusions are quite grim, for both users and developers of antivirus software, but it is the latter who have to take the necessary steps to improve security of their products and maintain the customer trust by staying ahead of cybercriminals and adapting the source code to the current day and age. To read more click **HERE**

Englishman Indicted for Stealing Thousands of US Government Employee Records

SoftPedia, 28 Jul 2014: A man from Stradishall, England, has been indicted for offenses that allowed him access to sensitive information of more than 100,000 federal government employees. The decision was taken on Thursday, against 29-year-old Lauri Love, by a federal grand jury in the Eastern District of Virginia. He breached the security of the systems that belonged to the US Department of Energy, Health and Human Services, US Sentencing Commission, FBI's Regional Computer Forensics Laboratory, Deltek, Inc. and Forte Interactive, Inc. In 2012, aided by accomplices, Love exploited a security vulnerability in Adobe ColdFusion, which was known at that time, and managed to exfiltrate records of the employees containing their full names, Social Security numbers, addresses, phone numbers, and information about their wages. According to a statement from the FBI, the hacker also stole more than 100,000 financial records that included credit card numbers and names. It appears that the financial damage resulting from Love's nefarious actions amounted to over $5 million. Love and his associates in crime used specially crafted file managers after exploiting the ColdFusion flaw, which allowed them to achieve elevated privileges on the affected systems. "After gaining unauthorized access to the protected servers, Love and his conspirators obtained administrator-level access to the networks using custom file managers, which allowed the conspirators to upload and download files, as well as create, edit, remove and search for data," reads the statement. If found guilty of the charges brought against him, the English hacker can get up to ten years of jail time. However, it appears that Love has separate indictments on related charges in the District of New Jersey and the Southern District of New York. To read more click **HERE**

Internet Explorer Named the Most Vulnerable Browser in the First Half of 2014

SoftPedia, 28 Jul 2014: Microsoft is making really big efforts to make Internet Explorer more secure and thus help it compete with other popular browsers on the market, including Google Chrome and Mozilla Firefox, but it appears that the company has until now failed to make any difference. A report (PDF reader needed) published by Bromium reveals that Internet Explorer is not only the most vulnerable browser in the first half of 2014, but also the most vulnerable software application currently on the market, with the number of security flaws exceeding the one of other products that have become famous for such problems, including Java and Flash Player. As you can see for yourselves in the chart above, Internet Explorer currently has the biggest number of security flaws reported this year, and figures are obviously expected to continue growing as more glitches are being found. To detail the graph, Bromium marked vulnerabilities found in 2013 with a blue bar, while those reported in the first half of this year are represented by the red bar. There are two major conclusions which anyone can draw by simply analyzing these figures: Internet Explorer is clearly the most vulnerable application on the market right now and the number of issues reported this year has already exceeded the number of flaws found in the whole of 2013. As for the reasons that are making Internet Explorer such a vulnerable browser, probably the most obvious reason is the retirement of older versions, including those that were running on Windows XP, which also reached end of support on April 8. At this point, Internet Explorer 8, which is no longer supported by Microsoft, is said to be the leading browser on the market, with a market share of around 21 percent. Since Redmond is no longer patching the browser, it's really easy to see how IE8 is becoming vulnerable to attacks, with users still not willing to make the switch to another application. Microsoft has obviously released several warnings, but until now only a few users actually decided to replace Internet Explorer with another browser or to upgrade their operating system and thus get a more secure IE version. "Windows Internet Explorer 8 is also no longer supported, so if you use it (or any other browser) to surf the web, you might be exposing your PC to additional threats," Microsoft briefly said in a statement when it announced that Windows XP reached end of support. To read more click **HERE**

Russia Wants to Crack Tor, Offers Budget Reward

SoftPedia, 25 Jul 2014: The Russian government is reportedly increasing its efforts to kill all kinds of anonymity and privacy on the Internet by putting the target on the Tor network. The anonymity tool is such a thorn in Russia's side that it has started to offer money for people who can create a reliable way to decrypt data sent over Tor. The money comes from Russia's Interior Ministry who seems to have an

issue with the growing popularity of Tor within the country, especially following the various Internet censorship efforts taken by the country's government. The rather large sum of money translates into $111,290 or €84,790, but it's basically nothing compared to what someone could get on such a decryption tool. In fact, there are probably many governments out there, the United States' included, that would like nothing better than to have such a tool to get their hands on the encrypted data going through Tor. The NSA is already known for monitoring the Tor "doors," the access points where users' data enters the complex set of networks that makes tracking impossible. "Law enforcers are worried about the ability of internet users to anonymously visit the internet, and particularly blocked sites. Also, the new blogging law that comes into force in August says that all bloggers with a daily audience of over 3,000 must register their identity. But someone blogging through TOR can do so anonymously," said a lawyer for Russia's Pirate Party. Only a fraction of people in Russia actually use this sort of tools, but the goal is likely much broader and seeks access and control of this area of the Internet that is currently safe from prying eyes. However, it does seem that Tor only had 80,000 users from Russia in May, but the number jumped to 200,000 this month, as revealed by Apparat.cc, an online magazine. This is a very important issue and it's making it obvious that Internet users in Russia are none too happy with Putin's plans to take control over the Internet and to completely expose them when they most likely did nothing wrong other than want a bit of privacy. This is also not the first time someone mentions taking down Tor, trying to find a de-anonymizing solution on a budget. In fact, a talk about this very subject was pulled from a Black Hat hacker conference, leaving people confused about the decision. To read more click **HERE**

Apache HTTP Server Exploits Closed in Ubuntu OSes

SoftPedia, 25 Jul 2014: Canonical announces that a number of Apache HTTP Server vulnerabilities have been found and fixed in its Ubuntu 14.04 LTS, Ubuntu 12.04 LTS, and Ubuntu 10.04 LTS operating systems. The Ubuntu maintainers have implemented a few of the latest fixes for the Apache HTTP Server that's also integrated in their operating system. "Marek Kroemeke discovered that the mod_proxy module incorrectly handled certain requests. A remote attacker could use this issue to cause the server to stop responding, leading to a denial of service. This issue only affected Ubuntu 14.04 LTS." "Giancarlo Pellegrino and Davide Balzarotti discovered that the mod_deflate module incorrectly handled body decompression. A remote attacker could use this issue to cause resource consumption, leading to a denial of service," reads the security notice. These are just some of the issues. For a more detailed description of the problems, you can see Canonical's security notification. Users have been advised to upgrade their systems as soon as possible. The flaws can be fixed if you upgrade your system(s) to the latest libdpkg-perl packages specific to each distribution. To apply the patch, run the Update Manager application. In general, a standard system update will make all the necessary changes and users don't need to restart the PC or the laptop in order to apply the patch. To read more click **HERE**

eBay Breach Prompts Class Action Lawsuit

SoftPedia, 25 Jul 2014: Individuals whose data was compromised in the breach incident against eBay in February, 2014, are suing the company for inadequate security measures imposed for protecting sensitive customer information. Although eBay's systems were accessed without authorization by unknown individual(s) in February, the company did not notify its customers until May 21, 2014, after the incident had been reported in the media. The lawsuit was filed this week by Collin Green on his behalf and other parties affected by the security event. The details stolen from eBay's database consisted of names, encrypted passwords, email and physical addresses, phone numbers and dates of birth, but other information may also be included. According to the lawsuit complaint, "the combined claims of the proposed class members exceed $5,000,000 [€3,718,000] exclusive of interest and costs." As far as this breach is concerned, it appears that "eBay's security was not only unreasonably lax in regard to intrusion, but eBay claims it remained unaware of the breaches for weeks, or months, after they occurred," it is written in the document. Moreover, the encryption applied to the passwords was not the strongest, but the "least safe method," that did not feature hashing of the codes. The complaint also says that the company took a conscious decision not to upgrade the security measures so that the yearly revenue

stream (more than $4 / €2.97 billion) would not be affected. eBay admitted in the 10-Q SEC filing for the first quarter of 2014 that security incidents were a constant threat for the business, and that the customer perception of the company not being secure would be detrimental to its financial results. The lawsuit is filed for negligence, breaching The Stored Communications Act, breach of contract or of implied contract, of fiduciary duty, bailment, violation of multi-state privacy laws and of Fair Credit Reporting Act, among other complaints. eBay collects and stores personal details of more than 120 million customers, as it is a huge marketplace for buyers and sellers who made transactions of about $205 / €152.2 billion in 2013. When the company released the breach notice to its millions of customers in May 2014, it only asked them to change their passwords and offered no details about the compromise of additional personally identifiable information (PII), which could lead to identity theft. "eBay's profit-driven decision to withhold the fact of its security lapse further damaged the class members who were prevented from immediately mitigating the damages from the theft," says the complaint. To read more click **HERE**

The Top 5 Most Brutal Cyber Attacks Of 2014 So Far

Forbes, 28 Jul 2014: In 2014, cyber attacks and data breaches don't look like they're going to slow down. We've seen high-end data breaches of large companies, with data, personal records and financial information stolen and sold on the black market in a matter of days. Analysts, Hold Security, startlingly announced in February that it had managed to obtain a list of 360 million account credentials for web services from the black market. That's just after three weeks of research. Criminals are stepping up their game and data breaches are becoming both common and devastating. According to research from Arbor Networks, the number of DDoS events topping 20Gbps in the first half of 2014, are double that of 2013. With more than 100 attacks at over 100Gbps or higher recorded in the first half of the year. Akamai Technologies Akamai Technologies' State of the Internet report also showed that hacker attacks on websites went up 75% in the final quarter of 2013, with hackers in China responsible for 43% of all attacks. We're only half way through the year, but there has already been a few high-profile hacks that have stopped presses. Here I'll explore – in no particular order – the most brutal hacks that have taken place in 2014 so far.

- Ebay: eBay went down in a blaze of embarrassment as it suffered this year's biggest hack so far. In May, eBay revealed that hackers had managed to steal personal records of 233 million users. The hack took place between February and March, with usernames, passwords, phone numbers and physical addresses compromised. Hackers successfully stole eBay credentials and managed to gain access to sensitive data. eBay encouraged users to change their passwords and reassured them that financial information was not stolen, as it's stored separately and encrypted. Although there were further concerns that the stolen personal information could leave eBay users vulnerable to identity theft. Despite eBay not confirming who was behind the attack, the notorious Syrian Electronic Army claimed responsibility. Despite the huge data breach and the sensitivity of the data, the SEA said that it was a "hacktivist operation" and that they "didn't do it to hack people's accounts".

- Montana Health Department : The State of Montana's health department revealed that a data breach may have affected more than 1 million people. The hack actually happened in July last year, but it wasn't discovered until May this year, with the identity of the intruders, and the extent of the damage done, still unclear. The state government said that it is notifying 1.3 million people including current and former residents, families of the dead and anyone else whose personal information may have been accessed in the attack. It's not clear if the attackers made-off with sensitive information, or if it had been used or sold on the black market. Richard Opper, director of the state's Department of Public Health and Human Services, said that there's "no indication" the hackers accessed the information or used it inappropriately. If they did, hackers would've gained access to highly personal information such as Social Security numbers, medical records, medical

insurance records, names, addresses and birth certificates. Not to mention the bank details of all health department employees.

- P.F. Chang's : The chain restaurant suffered a huge data breach last month that compromised customer payment information. Chang's didn't specifically mention how many customers had been affected, but thousands of newly stolen credit and debit cards went up for sale online on June 9th. Several banks had gotten in touch with Brian Krebs, a security journalist, to say that "they acquired from this new batch, multiple cards that were previously issued to customers, and found that all had been used at P.F. Chang's locations between the beginning of March 2014 and May 19, 2014." Criminals managed to hack P.F Chang's point of sale machines and record credit and debit card data, which then found its way on to the black market. Stolen records were being sold for between $18 and $140, with the price depending on how fresh the stolen data is. Chang's responded by going low-tech and using age old manual credit card imprinting machines to take payment in its stores, which it then upgraded to new "encryption-enabled terminals". Chang's is still working with the US Secret Service to discover the identity of the hackers.

- Evernote and Feedly: It's not clear if the attacks on both Feedly and Evernote were connected, but they happened within a day of each other and the two companies work largely in tandem. Whilst Evernote was taken down with a Distributed Denial of Service (DDoS) on Tuesday June 10th and was quickly restored within a few hours, Feedly, which went down the next day, suffered much more. The news aggregation service was attacked in the early hours of Tuesday morning. CEO of Feedly, Edwin Khodabakchian, announced on Feedly's official blog that the attack had been "neutralized" and that normal service had restored. However, two more DDoS waves were launched at Feedly which bought it down for another two days, with service being properly restored on June 14th. Not much about the attacker is known, other than that they attempted to extort money out of Feedly in exchange for ending the attacks. Khodabakchian said that he refused to comply with the attacker's ransom demands and the threat, eventually, was neutralized.

- Domino's Pizza Domino's Pizza: Hacking group Rex Mundi held Domino's Pizza to ransom over 600,000 Belgian and French customer records. In exchange for the personal data, which included names, addresses, emails, phone numbers and even favourite pizza toppings, Mundi demanded $40,000 from the fast-food chain. If the ransom wasn't met, the hackers threatened to publish the information online. The group then taunted Domino's by saying: "Earlier this week, we hacked our way into the servers of Domino's Pizza France and Belgium, who happen to share the same vulnerable database. boy, did we find some juicy stuff in there." Domino's refused to comply with the ransom and reassured customers that financial and banking information was not stolen. The hacking group had its Twitter account suspended and the data was never released, although it's not clear if Domino's ever complied with the ransom demands.

To read more click **HERE**