# THE CYBER SHIELD

*Cyber News for Counterintelligence / Information Technology / Security Professionals*

*11 June 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




*June 10, Securityweek* – (International) **Cyber spies targeting U.S. defense, tech firms linked to China's PLA: Report.** Researchers at CrowdStrike released a report on a cyberespionage group dubbed Putter Panda that has primarily targeted U.S, Japanese, and European aerospace, satellite, and communications industries and appears to be tied to the Chinese People's Liberation Army's Unit 61486. The group has been active since at least 2007 and mostly relies on custom malware that exploits vulnerabilities in popular software, according to the report. Source: http://www.securityweek.com/cyber-spies-targeting-us-defense-tech-firms-linked-chinas-pla-report

*June 10, Securityweek* – (International) **Zeus alternative "Pandemiya" emerges in cybercrime underground.** Researchers with RSA identified a completely new banking trojan known as Pandemiya that has several typical banking fraud tools as well as a modular design. The trojan does not share any code in common with other banking fraud toolkits and has appeared for sale on underweb marketplaces. Source: http://www.securityweek.com/zeus-alternative-pandemiya-emerges-cybercrime-underground

*June 9, Hartford Business* – (Connecticut) **400 patients' data may be compromised in Access Health breach.** Access Health CT, Connecticut's health insurance exchange reported that an employee from its call center vendor Maximus dropped a backpack June 6 in Hartford containing notepads with the personal information of about 400 health insurance customers. The backpack was found and the employee was placed on leave while officials investigate the incident. Source: http://www.hartfordbusiness.com/article/20140609/NEWS01/140609922

*June 10, V3.co.uk* – (International) **Clandestine Fox hackers spreading malware via Facebook, Twitter and LinkedIn.** FireEye researchers detected a new attack campaign by a group known as Clandestine Fox which uses malicious attachments in social media and email messages to spread malware. The attackers behind the campaign previously utilized a vulnerability that affected multiple versions of Internet Explorer before a patch was issued by Microsoft. Source: http://www.v3.co.uk/v3-uk/news/2349226/clandestine-fox-hackers-spreading-malware-via-facebook-twitter-and-linkedin

*June 9, Threatpost* – (International) **'Red button' attack could compromise some smart TVs.** Researchers with Columbia University's Network Security Lab reported that a vulnerability in the Hybrid Broadcast Broadband Television (HbbTV) feature in some smart TVs could allow attackers to steal personal information, access home networks, and perform denial of service (DoS) attacks by luring users to a compromised channel. Source: http://threatpost.com/red-button-attack-could-compromise-some-smart-tvs/106547

*June 9, Securityweek* – (International) **Zeus malware control panel vulnerable: Websense.** Websense researchers published information and a proof-of-concept that illustrate how the control panel for the Zeus banking trojan can be compromised by uploading a customized file to the command and control server. Source: http://www.securityweek.com/zeus-malware-control-panel-vulnerable-websense

*June 9, Securityweek* – (International) **Majority of comment spam generated by small number of attackers: Imperva.** Imperva released their June Hacker Intelligence Initiative report, which found that during the report's 2-week survey period in September 2013, 28 percent of attack sources generated 80 percent of traffic associated with comment spam, among other findings. Source: http://www.securityweek.com/majority-comment-spam-generated-small-number-attackers-imperva

*June 9, SC Magazine* – (International) **Possibly 350K ransomware infections, $70K earned, in Dropbox phishing scheme.** Researchers with PhishMe found that an ongoing phishing campaign utilizing links to Dropbox may have infected almost 350,000 systems with the Cryptowall ransomware, bringing in over $70,000 in Bitcoins of ransom for the attackers. Source: http://www.scmagazine.com/possibly-350k-ransomware-infections-70k-earned-in-dropbox-phishing-scheme/article/353559/

**Windows Leaker to Spend 3 Months in Prison**
SoftPedia, 11 Jun 2014: Microsoft leaker Alex Kibkalo has made the headlines lately after being arrested for posting Windows builds online with the help of a French blogger, and it appears that a US court has finally decided his sentence. Myce.com is reporting via Russian media outlets that Kibkalo will spend the next three months in prison, after being found guilty of leaking confidential information and violating intellectual property belonging to Microsoft. He uploaded preview versions of Windows 8 and Microsoft Activation Server Software Development Kit (SDK), while also uploading files and information about these projects on his SkyDrive. A French blogger used information he received not only to upload screenshots on websites, but also to share Windows Server activations keys online. Kibkalo was arrested by the FBI in March this year, with initial reports claiming that he uploaded Windows 7 and Windows 8 copies to his personal cloud-based storage account. According to a report first published by the Seattle Post-Intelligencer, who received more information from Microsoft's investigation, Kibkalo worked for Redmond for a total of 7 years, during which he "uploaded proprietary software including pre-release software updates for Windows 8 RT and ARM devices, as well as the Microsoft Activation Server Software Development Kit (SDK) to a computer in Redmond, Washington and subsequently to his personal Windows Live SkyDrive account." FBI's investigation revealed quite a lot of incriminating details proving that Kibkalo was indeed behind several leaks that reached the web in the last couple of years. Conversation between Kibkalo and the French blogger revealed that he was well aware of the illegal activities he was about to do. The identity of the French blogger, on the other hand, is yet to be discovered, as Microsoft Trustworthy Computing Investigations, one of the teams that were formed to investigate this case, couldn't find too many details to track him down. The group, however, discovered a Hotmail account that has been used to communicate with Kibkalo, again containing evidence that the former Microsoft employee was behind the leaks. The blogger used several tactics to hide his identity and used an IP based in Quebec to block Microsoft officials from finding his location. Microsoft is yet to issue a statement on this, but we've reached out to the company and we'll update the article as soon as we get an answer. In the meantime, the number of Windows leaks reaching the web has dropped significantly, so it's pretty clear that Microsoft managed with just one arrest to tackle this issue for a very long time. To read more click **HERE**

**Microsoft Fights Government Order to Share User Emails in Court**
SoftPedia, 11 Jun 2014: Microsoft has recently filed for a court challenge to a government order asking for user emails from its servers located in Ireland, pointing out that it cannot be forced to provide consumer information from data centers based in non-US countries. The company has already confirmed that it decided to challenge the government order in court, saying that US search warrants should only cover local data centers and allow authorities overseas to decide whether user details should be disclosed or not. Brad Smith, general counsel & executive vice president, Legal & Corporate Affairs, Microsoft, said in a statement one week ago that the software giant was "concerned" with how the government was handling such requests, as authorities were often requesting the company to share details saved on data

centers overseas. "We're concerned about governmental attempts to use search warrants to force companies to turn over the contents of non-U.S. customer communications that are stored exclusively outside the United States," Brad Smith said in the statement. "The U.S. government wouldn't stand for other governments seeking to serve search warrants within American borders to seize the content of U.S. citizens' emails without going through U.S. legal process. Why should it expect other governments to react any differently?" The United States, on the other hand, are ahead that in case Microsoft wins the court dispute, other tech companies such as Google and Facebook could challenge similar government orders, leading to more legal disputes between authorities and tech firms in the country. However, Smith states that the United States should stop trying to force Microsoft and other large companies to provide user data stored on server overseas and calls for increased transparency as far as the legal requests concerning such an issue are concerned. The Ireland case is just an example of how tech giants should handle government orders, Smith said while also pointing out that Microsoft is very confident that "the US Constitution is on our side." Under the Fourth Amendment of the U.S. Constitution, users have a right to keep their email communications private. We need our government to uphold Constitutional privacy protections and adhere to the privacy rules established by law. That's why we recently went to court to challenge a search warrant seeking content held in our data center in Ireland. We're convinced that the law and the U.S. Constitution are on our side, and we are committed to pursuing this case as far and as long as needed. To read more click **HERE**

## 2014 Scam World Cup Has Already Kicked Off

SoftPedia, 11 Jun 2014: As it always happens with important events about to kick off, scammers have already made their plans to lure victims with appealing offers related to the FIFA World Cup competition. Symantec researchers have come across email samples containing either malicious attachments or links to web addresses that serve malware. The incentives used in the messages range from free ticket offers (with an all-expenses paid trip to the host country, Brazil) to fake news about the football teams participating in the global event. Obviously, to increase the chances of success, the scammers try to pique the interest of the victim with subjects about the popular players. As such, Neymar da Silva Santos and Lionel Messi are most commonly used as bait. These emails appear to come from an official source, but grammar mistakes and a look at the source should generally reveal them as a scam. In one email sample presented by Symantec, the cybercrook informed the victim of winning a ticket (available as an attachment) to the 2014 World Cup in Brazil as part of a promotional offer. The offer is very alluring, especially since the message informs that the ticket provides paid trips for four persons, with 4-star accommodation included. If alarm bells aren't ringing yet, "walking down the players' tunnel" and "close-up view of the players warming up" should do the job. Attachments are malicious and consist of archived executables of remote administration tools (RATs) that allow the attacker to perform tasks on the computer unbeknownst to the user, such as stealing credentials and sensitive information or making it part of a botnet that is generally used in distributed denial-of-service attacks (DDoS). According to the Symantec post, the email can also contain "a malicious word document that exploits a known vulnerability in Microsoft Word." Users are advised not to access the links in emails with messages claiming to offer free tickets to the games or promising interesting videos or surveys of any nature. Such deceiving practices are currently at the beginning, but other attack vectors are very likely to be used by criminals. One method to spread malware is via social networks, where a malicious link can be distributed very fast by making it available to the entire list of friends, who, in turn, can pass it on to their buddies. Fake Android apps have also been created, some of them with the purpose of making the user access the ads, others requesting information that has nothing to do with its functionality. By accessing official sources for live streaming of the matches or the latest news, users ensure their safety and the failure of the scammers. Also, updating the system with the latest security patches, as well as web browsers and other applications, makes the user less vulnerable to fraudulent actions. To read more click **HERE**

## Flash Player Update Patches Six Vulnerabilities

SoftPedia, 11 Jun 2014: The latest update for Adobe Flash Player (version 14.0.0.125 for Windows and Mac and version 11.2.202.378 for Linux) includes multiple security fixes against issues that would allow an attacker to gain control over the affected system. On Windows and Mac, the severity of the update is given the highest priority rating, which means that there are good chances for vulnerability exploits to already exist in the wild. The same priority applies in the case of Chrome and IE. From a total of six vulnerabilities, three of them (CVE-2014-0531, CVE-2014-0532, CVE-2014-0533) made the plug-in susceptible to cross-site scripting attacks and their discovery is attributed to Erling Ellingsen of Facebook. Two of the flaws (CVE-2014-0534, CVE-2014-0535) allowed an attacker to bypass the security of the component, while the last one (CVE-2014-0536, attributed to Leong Wai-Meng of Trend Micro) made it vulnerable to an attack that leveraged memory corruption and permitted execution of arbitrary code. Adobe's browser plug-in is automatically updated in Google Chrome, Internet Explorer 10 and 11 thanks to the auto update mechanism included in the products; in some cases a browser restart is required for the update to complete. Users that do not receive the update automatically are advised to install it manually as soon as possible in order to eliminate security risks. To read more click **HERE**

## ZeuS Replacement Found in Underground Forums

SoftPedia, 11 Jun 2014: Called Pandemiya, the new Trojan has been coded from scratch in about a year and includes protective measures to avoid detection by automated network analyzers. Researchers at RSA Security reveal that Pandemiya is currently advertised on the cyber black market for the price of $1,500 (1,100 EUR); this is only for the core application, and a complete package, with additional functions provided by plug-in components, costs $2,000 (1,480 EUR). Although it shares plenty of features with the infamous ZeuS, this is not one of its variants, as all the lines of code (over 25,000) are original. The threat is designed to allow the botmaster to spy on an infected system and get form data and login credentials, as well as take snapshots of the screen. Additional sensitive information can be obtained by injecting fake pages into the web browser (Google Chrome, Internet Explorer or Mozilla Firefox), thus tricking the victims into providing the details themselves. Data gathered from the infected machine is sent to the control server in an encrypted form, using dynamic content and URI as an evasive measure against network analyzers. According to RSA, among the default features included in Pandemiya there is "signing of the botnet files to protect them from being hijacked by other fraudsters, and from being analyzed by security analysts or law enforcement." However, the core functionality can be expanded through plug-in components that provide reverse proxy, FTP stealing and PE infecting capabilities. Additional add-ons, currently in experimental stage, include a reverse hidden RDP and a Facebook spreader. The latter relies on Facebook credentials stolen from the victim to spread malicious links to friends. Stopping the activity of the infection is not too difficult, as RSA says that the threat creates an executable file under "Application Data" folder and a new value for it in the HKEY_LOCAL_USER\Software\Microsoft\Windows\CurrentVersion\Run registry key. Next in the installation process is placing a DLL with a random name in the System32 folder and creating a registry value for it in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\AppCertDlls. By deleting the aforementioned registry keys after checking them to identify the executable and the DLL file, the threat should no longer be active. A computer restart and then deleting the files should ensure a clean system. One peculiarity noted by the RSA researchers is that the last installation step "uses a not-so-well documented Windows security function – Windows will make every process run through the CreateProcess API, and load all of the DLLs under this registry key. Pandemiya makes use of this to inject itself into every new process that is initiated." At the moment, Pandemiya has not risen in popularity, but considering that law enforcement and security firms focus on ZeuS variants, the threat's modular architecture could boost its distribution. To read more click **HERE**

## Microsoft Fixes 8-Month Old Zero-Day, Leaves Windows XP Vulnerable to Attacks

SoftPedia, 11 Jun 2014: This month's Patch Tuesday rollout brought us a total of seven different security updates, two of which have been flagged as critical and supposed to address no less than 59 vulnerabilities in Internet Explorer. While this is pretty surprising given the fact that we're discussing about a single application, this new series of updates also includes a fix for a zero-day flaw reported to Microsoft 8 months ago and publicly disclosed by HP's Zero Day Initiative last month. In an advisory released today, Microsoft explained that the most severe vulnerabilities patched today would allow an attacker to gain the same privileges as the logged-in user and run malicious code on the target computer. "The most severe vulnerabilities could allow remote code execution if a user views a specially crafted Web page using Internet Explorer. An attacker who successfully exploited the most severe of these vulnerabilities could gain the same user rights as the current user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights," Microsoft said. The company explains that this particular flaw has been considered critical on Windows clients and moderate on Windows servers. "This security update is rated Critical for Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11 on Windows clients, Moderate for Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11 on Windows servers," it added. As you can see, Windows XP is missing from this equation, so the company has indeed pulled the plug on this particular OS version completely, even though more than 25 percent of the computers worldwide are still running it right now, according to third-party statistics. Redmond warns that every single user that still has Windows XP installed on his computer needs to upgrade to a newer version as soon as possible, be it Windows 7 or Windows 8.1. Upgrading would also bring a new Internet Explorer version as well, which clearly keeps them on the safe side whenever new vulnerabilities in older builds of the browser are discovered. Today's IE fixes are available for all the other supported Windows versions via Windows Update, so if your computer is connected to the Internet, just wait until all patches are automatically downloaded and installed. If you're running Windows XP, your best options are to either upgrade to a newer OS or change Internet Explorer with another browser. To read more click HERE

## Mozilla Firefox 30 - Security Fixes Galore

SoftPedia, 11 Jun 2014: On Tuesday, Mozilla released version 30 of its Firefox browser that included a total of seven security fixes, five of them being marked as critical, and the other two labelled as having a high security impact. Out of the five critical vulnerabilities, three of them would allow an attacker to cause a potentially exploitable crash by taking advantage of flaws with SMIL Animation Controller (use-after-free when rendering malformed web content), in Web Audio Speex resampler (buffer overflow when audio content exceeds expected bounds) and in Event Listener Manager (use-after-free triggered by web content). The set of critical issues repaired in Mozilla Firefox 30 also refers to memory safety bugs present in the browser engine that is also used by the Thunderbird email client. Although a method to exploit them has not been devised, the developer believes that in certain circumstances at least a part of them could enable an attacker to run arbitrary code on the user machine. Among the flaws with a high security impact, there is a buffer overflow in the Gamepad API that could lead to an exploitable crash. The vulnerability would occur in conjunction with a gamepad with non-contiguous axes, either a physical or a virtual device. Another security fix addresses an event that can make the mouse cursor invisible after interaction with an embedded flash object and then use it outside said object. The prevalent risk in such a situation is clickjacking. This problem is not present in Windows and Linux and affects only OS X users. To read more click HERE

## Reflected XSS Vulnerability Patched in Cisco AsyncOS

SoftPedia, 11 Jun 2014: Cisco AsyncOS, the operating system powering multiple Cisco security appliances, has been patched against a reflected cross-site scripting vulnerability that allowed an unauthenticated attacker to load an arbitrary script in the context of the user's browser. The affected products are Cisco Email Security Appliance 8.0, Cisco Web Security Appliance 8.0 and Content Security

Management Appliance 8.3. Earlier versions are also vulnerable. According to the Cisco advisory, "the vulnerability is due to insufficient input validation of a parameter," in this case date_range, and the exploit could be carried out through a malformed URL the user has to access. The patch released by the company eliminates the security flaw available in the reports overview page of the management interface and should be applied as soon as possible. In the case of older products, upgrading to the latest version is recommended. However, if this cannot be done, the CERT/CC (Computer Emergency Response Team Coordination Center) provides the following workaround: "As a general good security practice, only allow connections from trusted hosts and networks. Note that restricting access does not prevent XSS or CSRF attacks since the attack comes as an HTTP request from a legitimate user's host. Restricting access would prevent an attacker from accessing the web interface using stolen credentials from a blocked network location." To read more click **HERE**

**iOS 8 will randomize devices' MAC address to increase privacy**

Heise Security, 11 Jun 2014: The next major release of Apple's iOS mobile operating system will include an important change: when local wireless networks scan for devices in range, devices running iOS 8 will provide random, locally administrated MAC addresses. Why is that important, you ask? Well, so far each device has only one unique Media Access Control (MAC) address, with which it identifies itself to every Wi-Fi network whether the user tries to connect to it or not. This allows marketing companies, location analytics firms, and and stores to track the movements of users. This information is extremely valuable to them, as it allows them to form a relatively accurate picture of what a user does and when, and what he or she is interested in. But with iOS 8, which is set to be released later this year, that advantage will be gone unless the user decides to connect to the network. Ars Technica's Lee Hutchinson posits that this change has not been made by Apple just to protect users' privacy, but also to drive companies toward iBeacon, the company's own location-based advertising service. "iOS users who would prefer to opt out of iBeacon can first ensure they have no iBeacon-aware apps installed (like the official Apple Store app), or they can disable Bluetooth," Hutchinson advises. "Until iOS 8 arrives, iOS 7 users who would prefer not to have their MAC addresses tracked in public can disable Wi-Fi when they're out and about." It's interesting to note that with iOS 7 Apple has made it impossible for app developers to collect MAC addresses of users in order to see how many have installed their app(s). They also prevented them from targeting ads. Apple is definitely making a shift towards privacy, responding to the hightened user awareness about the issue. The company has also announced that they will be including DuckDuckGo, the search engine that doesn't track its users, in the future versions of Safari on iOS and OS X. To read more click **HERE**

**Payment card breach at US restaurant chain P.F. Chang's**

Heise Security, 11 Jun 2014: Asian-themed US restaurant chain P.F. Chang's China Bistro has apparently suffered a breach that resulted in the theft of customers' payment card data. The extent of the breach and, indeed, the breach itself is yet to be officially confirmed by the company, but according to bank sources interviewed by Brian Krebs, some of the compromised cards have been used at various P.F. Chang's locations between early March and May 19, 2014. "P.F. Chang's takes these matters very seriously and is currently investigating the situation, working with the authorities to learn more," the company commented. "We will provide an update as soon as we have additional information." A strong indication that the company has suffered a breach came in the form of an ad on the popular carder store Rescator(dot)so on June 9. The seller offered a "fresh" batch of card data for prices between $18 to $140 per card, and said that they are "100%" valid, which seems to imply that the breach happened recently and has not yet been detected and, therefore, the cards in question have not yet been cancelled. "The items for sale are not cards, per se, but instead data copied from the magnetic stripe on the backs of credit cards. Armed with this information, thieves can re-encode the data onto new plastic and then use the counterfeit cards to buy high-priced items at big box stores, goods that can be quickly resold for cash (think iPads and gift cards, for example)," Krebs explained. The number of compromised cards is unknown. According to bank sources, the data was apparently stolen from P.F. Chang's restaurants in Florida, Maryland, New Jersey, Pennsylvania, Nevada and North Carolina. It's believed that the attackers

managed to compromise the establishments' point-of-sale (POS) systems. Additional guidance in the ad on how to pay for the data dump points to the criminals behind this breach being from Russia and/or Eastern Europe. To read more click **HERE**

### What to avoid in Dropbox-related phishing attack

CSO, 9 Jun 2014: Corporate employees familiar with Dropbox should take extra precautions to avoid becoming a victim of a phishing attack that uses the popular file-sharing service. Cybercriminals have been sending out emails with malicious links pointing to a ZIP file on Dropbox that contains a screensaver that is actually ransomware similar to one known as CryptoLocker, security vendor PhishMe reported Friday. The attackers try to trick the recipients into clicking on the link through a variety of ploys, including disguising the email, so that the link appears to point to an invoice or a fax report or message. If someone receives the email at work, "they may think that they're receiving a fax and it's something they need to look at, which makes them inclined to go ahead and open it," Ronnie Tokazowski, senior researcher at PhishMe, said. Clicking on the link to the ZIP file and then the screensaver file inside launches the malware that encrypts files on the victim's hard drive. PhishMe estimates that victims have had as many as 20,000 files encrypted. Files typically affected by such ransomware include documents, archive files, executables and JPEGs. Once executed, the malware launches a page on the victim's default browser, demanding that $500 in Bitcoins be deposited in the criminals' electronic wallet. Failing to do so after a certain amount of time leads to the ransom doubling to $1,000. Based on an examination of three of the attackers' wallets, the scammers have collected at least $62,000, Tokazowski estimates. The ransom demand and payment transactions are conducted over the Tor anonymity network. The attack does not exploit a vulnerability on Dropbox. PhishMe had not discussed the phishing campaign with Dropbox, which did not respond to a request for comment. PhishMe discovered the scam after its own employees received the phishing emails, Tokazowski said. Almost 20 of the company's 50 employees received the messages. PhishMe does not believe it was directly targeted in the campaign, but was just one of many companies whose employees might have received the emails. To avoid becoming a victim, companies should advise employees to be wary of downloading ZIP files and emails like the ones described above that have no recognizable sender. To read more click **HERE**

### Upsurge In Hacking Makes Customer Data 'Toxic' To Retailers

Reuters, 9 Jun 2014: With hackers stealing tens of millions of customer details in recent months, firms across the globe are ratcheting up IT security and nervously wondering which of them is next. The reality, cyber security experts say, is that however much they spend, even the largest companies are unlikely to be able to stop their systems being breached. The best defense may simply be either to reduce the data they hold or encrypt it so well that if stolen it will remain useless. Only a few ago, the primary IT security concern for many large corporations was stopping the loss or theft of physical disks or drives with customer information. Now, much harder to detect online thefts are rife. Last week, Reuters revealed a host of big name U.S. Fortune 500 companies were on a hiring spree for board level cyber security experts often offering $500,000-700,000 a year, sometimes more. Many have high-level backgrounds, at much lower pay, at signals intelligence agencies such as the U.S. National Security Agency or Britain's GCHQ - although security experts say European firms are reluctant to hire ex-NSA staff following revelations over the scale of U.S. cyber monitoring by whistleblower Edward Snowden. "Information has become toxic for retailers because the more they have, the bigger a target they become," said Lamar Bailey, security researcher at IT security firm Tripwire. "The ongoing rash of attacks brings into question what information an organization should be keeping." U.S. retailer Target ousted its CEO Gregg Steinhafel in May after the

firm said foreign hackers had stolen up to 70 million items of customer data including some PIN numbers late last year. Industry watchers said purchases on its website dropped noticeably in the run-up to Christmas with the breach also sparking lawsuits and official investigations. A report from cyber security think tank the Ponemon Institute showed the average cost of a data breach in the last year grew by 15 percent to $3.5 million. The likelihood of a company having a data breach involving 10,000 or more confidential records over a two-year period was 22 percent, it said. The corporate fallout from the largest recorded breach so far, the loss of password data on some 145 million customers from online retailer eBay, is not yet clear. A senior eBay executive told Reuters last week that "for a very long time" the firm had not realized customer data had been seriously compromised by the attack. To read more click **HERE**