The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

30 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

The Heartbleed Hit List: The Passwords You Need to Change Right Now
Mashable, 30 Apr 2014: An encryption flaw called the Heartbleed bug is already being called one of the biggest security threats the Internet has ever seen. The bug has affected many popular websites and services — ones you might use every day, like Gmail and Facebook — and could have quietly exposed your sensitive account information (such as passwords and credit card numbers) over the past two years. But it hasn't always been clear which sites have been affected. Mashable reached out some of the most popular social, email, banking and commerce sites on the web. We've rounded up their responses below. Some Internet companies that were vulnerable to the bug have already updated their servers with a security patch to fix the issue. This means you'll need to go in and change your passwords immediately for these sites. Even that is no guarantee that your information wasn't already compromised, but there's also no indication that hackers knew about the exploit before this week. The companies that are advising customers to change their passwords are doing so as a precautionary measure. Although changing your password regularly is always good practice, if a site or service hasn't yet patched the problem, your information will still be vulnerable. Also, if you reused the same password on multiple sites, and one of those sites was vulnerable, you'll need to change the password everywhere. It's not a good idea to use the same password across multiple sites, anyway. To view the list click **HERE**. To read more click **HERE**

April 26, Baltimore Sun – (Maryland) **Former Hopkins grad students' personal data exposed online.** Johns Hopkins University officials notified 2,166 former students that their Social Security numbers were exposed to potential hackers after discovering March 19 that the information was stored on a server which was available on the Internet. The files were taken offline and the university does not believe the information was accessed maliciously but found that the records were retrieved a few dozen times, potentially by search engines or web crawlers. Source: http://articles.baltimoresun.com/2014-04-26/news/bs-md-hopkins-data-20140426_1_social-security-numbers-hopkins-grad-personal-data

April 28, V3.co.uk – (International) **Critical Microsoft Internet Explorer flaw leaves one in four web users vulnerable.** Microsoft warned users of its Internet Explorer (IE) browser after FireEye researchers discovered a critical zero day vulnerability that affects IE 6 through IE 11 and could allow an attacker to use a Flash exploitation technique to remotely execute code. FireEye researchers spotted attacks using the vulnerability targeting IE 9 through IE 11, representing about a quarter of total browser users. Source: http://www.v3.co.uk/v3-uk/news/2341834/critical-microsoft-internet-explorer-flaw-leaves-one-in-four-web-users-vulnerable

April 28, Softpedia – (International) **4 vulnerabilities and 38 bugs fixed with the release of MyBB 1.6.13.** The latest version of MyBB was released for download, closing 4 security vulnerabilities and addressing 38 functionality bugs. Source: http://news.softpedia.com/news/4-Vulnerabilities-and-38-Bugs-Fixed-With-the-Release-of-MyBB-1-6-13-439653.shtml

April 28, Softpedia – (International) **Apache Struts 2.3.16.2 released to properly fix zero-day vulnerability.** The Apache Software Foundation released an update for its Apache Struts open-source framework, addressing an issue with a previous update that included a fix for a zero day vulnerability that was not efficient. Source: http://news.softpedia.com/news/Apache-Struts-2-3-16-2-Released-to-Properly-Fix-Zero-Day-Vulnerability-439621.shtml

April 28, Softpedia – (International) **XSS vulnerability in Sohu.com leveraged for large-scale DDoS attacks.** The source of a distributed denial of service (DDoS) attack on a client of Incapsula early in April that involved 20 million GET requests was found to be Sohu.com, a popular Chinese Web portal. Incapsula informed Sohu.com of the issue and the site was able to close a cross-site scripting (XSS) vulnerability that was used to power the attack. Source: http://news.softpedia.com/news/XSS-Vulnerability-in-Sohu-com-Leveraged-for-Large-Scale-DDOS-Attacks-439606.shtml

April 25, Softpedia – (International) **Security patches released for IP.Board 3.3.x and 3.4.x.** Invision Power Services released security patches for its IP.Board 3.3.x and 3.4.x products, addressing three file inclusion issues and a cross-site scripting (XSS) vulnerability. Source: http://news.softpedia.com/news/Security-Patches-Released-for-IP- Board-3-3-x-and-3-4-x-439416.shtml

April 25, Threatpost – (International) **Exploiting Facebook Notes to launch DDoS.** A security researcher discovered and reported a method that can be used to launch distributed denial of service (DDoS) attacks through the Facebook Notes feature by using random GET parameters for HTML tags. Facebook stated that they acknowledged the issue but would not change the method the tags are handled because it would degrade user functionality. Source: http://threatpost.com/exploiting-facebook-notes-to-launch-ddos/105701

April 28, KTBC 7 Austin – (Texas) **Computer containing patient data stolen from Seton.** Seton Northwest Hospital in Texas notified approximately 180 patients that a password-protected Hewlett Packard desktop device, which holds their personal information, was stolen from a locked storage area of the hospital's sleep lab in February. The hospital is investigating the incident. Source: http://www.myfoxaustin.com/story/25372824/computer-containing-patient-data-stolen-from-seton

April 29, Softpedia – (International) **Siemens patches Heartbleed bug in industrial products.** Siemens published an advisory and updates for several of its industrial control systems (ICS) programs that address the Heartbleed vulnerability in OpenSSL. Some Siemens ICS software remain unpatched, and the company advised users to apply workarounds until a full patch is made available. Source: http://news.softpedia.com/news/Siemens-Patches-Heartbleed-Bug-in-Industrial-Products-439837.shtml

April 29, Softpedia – (International) **Apple fixes vulnerability that granted anyone access to personal details of developers.** Apple closed a vulnerability in its Developer Center's Radar application that could have been exploited to obtain the contact information of Apple retail and corporate employees and iOS, Mac, and Safari developers. A proof-of-concept was revealed by the researcher who discovered the vulnerability after Apple closed the vulnerability. Source: http://news.softpedia.com/news/Apple-Fixes-Vulnerability-That-Granted-Anyone-Access-to-Personal-Details-of-Developers-439812.shtml

April 29, Softpedia – (International) **Phishers abuse Microsoft Azure to target PayPal, Apple, and Visa customers.** Researchers at Netcraft reported that cybercriminals are making use of 30-day trials of Microsoft's Azure cloud service to host phishing Web sites. The researchers identified several Azure-hosted phishing pages targeting Apple, Comcast, PayPal, Visa, American Express, and Cielo customers. Source: http://news.softpedia.com/news/Phishers-Abuse-Microsoft-Azure-to-Target-PayPal-Apple-and-Visa-Customers-439800.shtml

April 29, The Register – (International) **Researchers warn of resurgent Sefnit malware.** Researchers at Facebook reported that the Sefnit malware has been seen in use again, but without the use of a Tor client. The malware instead establishes direct connections to one or more command and control servers using a secure Plink connection. Source: http://www.theregister.co.uk/2014/04/29/researchers_warn_of_resurgent_sefnit_malware/

April 28, Help Net Security – (International) **Flash 0-day exploited in watering hole attacks, Adobe provides patch.** Adobe released updates for it Flash Player for Windows, Mac, and Linux following the discovery of a new zero-day vulnerability that is being actively exploited in the wild. Users were advised to update immediately. Source: http://www.net-security.org/secworld.php?id=16750

April 28, CNET News – (International) **Stop using Microsoft's IE browser until bug is fixed, US and UK warn.** The U.S. Computer Emergency Readiness Team (US-CERT) advised users to stop using the Internet Explorer browser until Microsoft can develop a patch for a recently-disclosed vulnerability that can allow attackers to run malicious code. The vulnerability is currently being used in attacks against U.S. defense and financial organizations, according to FireEye researchers. Source: http://www.cnet.com/news/stop-using-ie-until-bug-is-fixed-says-us/

Microsoft's Internet Explorer Gets Hit by 'Operation Clandestine Fox' -- What You Need to Know
Fool.Com, 29 Apr 2014: The U.S. Department of Homeland Security has just advised Americans to not use Microsoft's Internet Explorer browser until a serious security flaw can be resolved. The flaw -- which allows malicious hackers to circumvent security measures in Windows operating systems when compromised websites are visited -- exploits a corrupted Adobe Flash file to attack the victim's computer. FireEye Research Labs, which discovered the bug, has stated that the hackers exploiting the bug are calling the attack "Operation Clandestine Fox." In response, Microsoft stated that it was working to repair the vulnerability in versions 6 through 11 of IE, although Windows XP users -- who lost support earlier this month -- will be left without a fix. However, Symantec, the makers of Norton Antivirus, recently released a tool for XP users to protect themselves from the bug. Microsoft has advised downloading its Enhanced Mitigation Experience Toolkit version 4.1 to guard against attacks. FireEye has stated that disabling Adobe's Flash plugin can temporarily fix the issue across all platforms. At the time of this writing, Microsoft has not released a fix for the bug yet -- a dire problem considering that nearly 57% of all PCs worldwide run one of the affected versions of IE. Operation Clandestine Fox could mean a few things for Microsoft. First, it ironically benefits the company, since this could be the canary in the coal mine that tells late adopters that it's finally time to let go of XP. However, that sales boost will come at the expense of Microsoft's reputation. Microsoft's operating systems -- both on PCs and Xbox consoles -- have long been riddled with security flaws. ATMs running on Windows XP were repeatedly hit by USB drive and text-message based hacks. Last month, a 5-year-old boy discovered a security flaw in the Xbox One, simply by typing a series of spaces when prompted for a password. Problems like these often lead critics to claim that Linux distributions or Apple's Mac OS are much safer alternatives to Windows. Yet in reality, PCs running Microsoft Windows are popular targets for hackers simply because they comprise the vast majority of the computers in the world. It's simply a wasted effort to write a virus targeting Macs or Linux systems, which together only account for 5% of the world's computers. If Microsoft can't solve its Clandestine Fox issue soon, Chrome could experience a spike in market share. Google intends for Chrome to house its cloud-based apps, such as Drive, GMail, and YouTube, in a miniature operating system. This mini-OS approach has

been seen before in Chrome OS and the Windows 8 version of Chrome, which adds a Google Apps-based taskbar to the bottom of the screen. Chrome's greatest advantage over IE is that it quietly synchronizes search histories, bookmarks, and even autocomplete form information across multiple devices. Therefore, users abandoning IE for Chrome might eventually get drawn into Google's ecosystem, ditching Outlook for Gmail, OneDrive for Drive, and Bing Maps for Google Maps. That will lead straight to an increased dependence on Google's ecosystem -- the vital engine that keeps sales of Android devices churning along. While this is certainly a black eye for Microsoft, it could be far worse for Adobe, which has been struggling to convert itself from a packaged software company to a cloud-based subscription one. Adobe's reputation was severely tarnished last October after hackers broke into its servers and stole customer account information and the source code for Adobe's top products such as Adobe Acrobat and ColdFusion. The theft of the ColdFusion source code is especially troubling, since it supports the newer HTML5 standard used by many mobile apps. As a result, hackers could use the ColdFusion source code as an open guidebook to create dangerous exploits. Meanwhile, Adobe Flash, which was directly implicated in the Clandestine Fox hack, has been exploited many times in the past. Like Javascript, Flash can execute malicious code via a plugin on a webpage upon loading to circumvent a computer's security protocols and steal information. In 2010, Steve Jobs called Flash "the number one reason Macs crash." He also cited Symantec's statement that Flash had "one of the worst security records." Four years later, Operation Clandestine Fox looks like a firm validation of Jobs' declaration. At the moment, there's not much computer users can do except avoid using IE and disable Adobe's Flash plugins. However, the hackers behind Operation Clandestine Fox claim that the exploit is part of an ongoing campaign, which means that this "bug" could actually be much more vicious and dynamic than a simple virus. The longer this debacle drags on, the worse it will get for Microsoft and Adobe. Microsoft will struggle with keeping its IE users from flocking to Chrome, while Adobe will have a tough time convincing its corporate customers that it takes cloud-based security seriously. To read more click **HERE**

Sensors Used for Traffic Control Systems Can Be Hacked, Experts Warn

SoftPedia, 30 Apr 2014: At the upcoming Infiltrate conference in Florida, IOActive researcher Cesar Cerrudo will demonstrate that hackers can manipulate the vehicle traffic control systems used in 40 major cities in the United States. According to Wired, Cerrudo had found that hackers could use the magnetic sensors embedded in the street as an attack vector. The sensors feed data on traffic to access points and repeaters. These components then pass on data to traffic signal controllers. The sensors are efficient because they're easy to install and their battery lasts for 10 years. The information from these sensors is used for traffic lights and traffic information systems. The solution is developed by Sensys Networks. The expert tested his findings on the Sensys Networks VDS240 wireless vehicle detection system. He managed to convince the company to sell him an access point for $4,000 (€2,900). These access points can't be purchased by anyone, but the researcher got the company to sell him one by claiming that he needed a unit to conduct some tests for a customer. The problem, as the expert highlighted in a report sent to the DHS's ICS-CERT, is that the wireless communication between the sensor and the access point is based on a protocol called the Sensys NanoPower Protocol, which doesn't implement any security mechanism. Communications are not encrypted, and the NanoPower Protocol could be reverse-engineered, the researcher noted. An attacker could disable or misconfigure the sensors, and manipulate the data that's being sent by mimicking sensor information. This could lead to traffic disruptions, accidents and congestions. Cerrudo has conducted his tests with a device from the vendor, but he highlights the fact that an attack could also be carried out without the original access point. An attacker could simply use a wireless transceiver. It would be a bit trickier because it would be more difficult to interpret the data, but it can be done. With a regular wireless transmitter, the attacker would have to be within 150 feet (45 meters) from the sensor, but a powerful antenna increases the maximum distance to 1,500 feet (450 meters), maybe even a mile (1.6 kilometers) if a strong antenna is utilized. The security expert has also conducted a test with a drone, managing to send data from over 600 feet (180 meters) in the air. So will these issues be addressed? Apparently, not any time soon. New versions of the sensors developed by Sensys are a bit more secure since the firmware updates are encrypted. It's unlikely that the old ones will be replaced any time soon because that would require digging up the roadbed. Furthermore, Sensys representatives

have told Wired that the DHS is "happy with the system." Cerrudo reported his findings to ICS-CERT, which got in touch with Sensys. The company has told ICS-CERT that the encryption mechanism was removed in the early stages of the development cycle based on customer feedback. ICS-CERT has told the researcher that there's nothing more it can do at this point. If there is evidence of vulnerabilities being exploited, the matter will be revisited. To read more click **HERE**

14 Security Issues Addressed with the Release of Firefox 29

SoftPedia, 30 Apr 2014: Firefox 29 is available for download. In addition to the visual enhancements, numerous security issues have been fixed with the latest release of Mozilla's web browser. A total of 14 vulnerabilities have been addressed. Five of them are critical, six are high and three are moderate. No low-impact flaws have been fixed this time. The list of critical-impact security holes includes a use-after-free in nsHostResolve, a use-after-free in imgLoader when resizing images, a privilege escalation issue through the Web Notifications API, a use-after-free in the Text Track Manager for HTML video, and various memory safety hazards. Tyson Smith, Jesse Schwartzentruber, Nils, Mariusz Mlynski, and Abhishek Arya have been credited for identifying and reporting the flaws. The memory safety hazards have been identified by Mozilla's internal security team. The high-impact vulnerabilities are an XSS affecting history navigations, an out-of-bounds write bug in Cairo, a buffer overflow when using non-XBL object as XBL, memory corruption issues in Web Audio, and privilege escalation through the Mozilla Maintenance Service Installer. In addition, Mozilla's Boris Zbarsky found that the debugger will work with some objects while bypassing XrayWrappers, leading to privilege escalation under certain circumstances. Additional details on the vulnerabilities are available on Mozilla's Security Advisories page. You can download Firefox for Windows, Mac and Linux from Softpedia. To read more click **HERE**

Tool for Exploiting Flaws in McAfee ePolicy Orchestrator Made Available

SoftPedia, 29 Apr 2014: In June 2013, someone published a video to YouTube to show off a tool called the McAfee ePolicy 0wner. The hacking tool, which is designed to exploit a couple of vulnerabilities in McAfee's ePolicy Orchestrator (ePO), has been recently released to the public. ePolicy 0wner is designed to exploit a couple of ePO vulnerabilities that McAfee patched last year, Tripwire experts report. The flaws in question – CVE-2013-0140 and CVE-2013-0141 – were reported by experts from Verizon Enterprise Solutions. According to McAfee, the bugs can be exploited for unauthorized information disclosure, unauthorized modification or disruption of service. The hacking tool enables users to carry out various tasks, including add rogue systems to an ePO server, upload files, steal domain credentials, and execute commands both on the ePO server and on other systems managed with McAfee's centralized security management software. It's worth noting that the attacker must be on the victim's network for the attack to work. The vulnerabilities impact versions 4.5 (RTW) to 4.5.6, and 4.6 (TRW) to 4.6.5. Tripwire's IP360 and the SecureScan tool are capable of detecting the presence of the vulnerabilities, but the company advises administrators to make sure that their installations are patched. Check out the video that shows the ePolicy 0wner hacking tool in action (**link**). To read more click **HERE**

Trend Micro Publishes Research Paper on Russian Cybercrime Underground

SoftPedia, 29 Apr 2014: Max Goncharov, a member of Trend Micro's Forward-Looking Threat Research team, has published a new whitepaper on the Russian cybercrime underground. This is Goncharov's second paper on this topic, the first, "Russian Underground 101," being published back in 2012. The report reveals some interesting details about the Russian underground and the services it offers. When it first emerged in 2004, the underground market was a place where Russian cybercriminals exchanged information with one another. However, it slowly evolved into a market where criminals sell and purchase everything that's needed to carry out a malicious cyber operation. There is a wide range of services and products being offered, actors in the Russian underground being specialized in selling traffic direction systems (TDSs), and pay-per-install (PPI) services. Since some services and products are not as good and reliable as they're advertised, sellers and buyers increasingly rely on escrows or "garants." These are third parties that get 2-15% of

the sales price in return for ensuring the safety of both the seller and the buyer. Underground websites can have tens of thousands of unique members. These members rely on various methods (Tor and VPNs) to stay anonymous. They're only identified based on their nicknames and ICQ numbers. The Russian underground is just like any other business. The prices for products and services vary depending on demand and supply. For instance, now that cybercriminals have come up with efficient ways of stealing payment card data, the price of credit and debit card records has been decreasing over the past years. The situation is the same with stolen accounts. For example, the price of stolen Facebook accounts has halved between 2011 and 2013. On the other hand, there are some types of accounts for which experts haven't observed any significant changes (e.g. Gmail, Hotmail and Odnoklassniki). "Even though the prices of most products and services sold in the Russian underground market have been decreasing, that does not mean that business is not doing well for cybercriminals. It can even mean that the market is growing, as we see more and more product and service offerings as time passes," Goncharov explained in his paper. "Cybercriminals, like legitimate businesspeople, are also automating processes, resulting in lower product and service prices. Of course, 'boutique' products and services remain expensive because these involve specialized knowledge and skills to develop that only a few bad guys have." The complete "Russian Underground Revisited" paper is available on Trend Micro's website (**link**). To read more click **HERE**

Syrian Electronic Army "Hacks" Website of RSA Conference

SoftPedia, 29 Apr 2014: The Syrian Electronic Army has redirected the visitors of the RSA Conference website to a defacement page. The attack was carried out in response to an RSA Conference presentation in which Secure Mentem President Ira Winkler talked about the Syrian Electronic Army's hacking methods. In his presentation, Winkler made fun of the Syrian Electronic Army and the hackers didn't like it. The SEA became aware of the presentation after a video was published on the RSA Conference's website. "We were enjoying our summer peacefully, but the annoy of cockroaches like [Ira Winkler] and other security firms led to 3 reports about SEA," the hackers wrote on Twitter. On the page to which the visitors of the RSA Conference website were redirected, the hacktivists wrote, "Dear Ira Winkler, Do you think that you are funny? Do you think that you are secure? You are NOT. If there is a cockroach in the internet it would be definitely you." In a blog post published on Monday, Winkler explained that the hackers didn't actually hack into the RSA Conference's website. Instead, they redirected the site's visitors to a defacement page by leveraging Lucky Orange, an analytics tool installed on the website. The expert explained that the hacktivists sent out phishing emails to the staff of the DNS hosting company used by Lucky Orange. They sent employees emails purporting to come from the company's CEO. The messages instructed recipients to read a BBC article about the firm. When they clicked the link, employees were taken to a phishing website. An account executive fell for it and provided the hackers with the credentials needed to log in to the customer account management system. Once they had access, they reset the Lucky Orange password and logged in to the control panel. When a website that uses Lucky Orange is visited from a computer with JavaScript enabled, the analytics tool makes a call to an external website located at w1.livestatserver.com/w.js. "They reset the address of the 'w1' subdomain of the livestatserver.com domain which sent calls to w1.livestatserver.com to a server controlled by the SEA," Winkler explained. As a result of the modifications made by the SEA, all of the RSA Conference website's visitors were directed to the defacement image. Other websites using Lucky Orange were also impacted. The Syrian Electronic Army says there are a total of three reports about the group (three reports that they don't like), so they warn that there will be three attacks. To read more click **HERE**

Warning: Extremely Convincing Phishing Scam Steals Apple IDs and Credit Card Info

SoftPedia, 29 Apr 2014: Managed email security provider MX Lab has happened upon one of the most convincing email scams purporting to be a memo from Apple with a burning request to validate your account information. The people behind the scam will steal your Apple ID account and credit card information. MX Lab claims to have started to intercept these phishing emails earlier today. The subject of the message states, "Validate Your Account Information" and the message body includes a memo that looks and sounds exactly like a legitimate email from Apple's Support department

(screenshot above). Despite its seemingly legitimate nature, the memo "will try to steal your Apple ID account information including your credit card details," according to MX Lab. The phishing email says, "We need to ask you to complete a short and brief step to securing and validating your account information," adding that "Failure to complete our validation process will result in a suspension of your Apple ID." That's not something Apple would normally do, but unwary users would undoubtedly be alarmed by this fake warning. "We take every step needed to automatically validate our users, unfortunately in your case we were unable to," the email continues. "The process only takes a couple of minutes and will make sure there is no interruption to your account." The so-called "Apple Customer Service" team even goes to the trouble of explaining to the customer why he/she received the memo. "This email was sent automatically during routine security checks. We are not completely satisfied with your account information and require you to update your account to continue using our services uninterrupted. For more information, see our FAQ." According to the security firm, clicking the links supplied in the message will lead to a malicious host at hxxp://31.204.130.145/~apple/secure/SenH37d3lPuNqeIc561gswPd6d4RN/, where the unknowing user will be presented with a form to enter their Apple credentials, along with their credit card information. Needless to point out, cyber-criminals don't need your card's PIN number to wreak havoc, as the iTunes Store only requires your Apple ID and password, along with the billing information you've supplied. Again, the email in question will look extremely convincing to the untrained eye. It even uses iconic paper graphics employed by Apple in various listings on its web site, complete with a near-perfect signature, proper spacing in the text body, etc. Beware of any emails that force you to hand over your personal information using "or else" as a method of convincing you to take action. To read more click **HERE**

CERT UK Issues Warning for Windows XP Users

SoftPedia, 29 Apr 2014: Windows XP won't receive any other updates and security patches, which means that once a vulnerability is discovered in the operating system, users running it will remain completely unprotected against the attacks supposed to exploit it. This moment has come, as Microsoft yesterday confirmed that an Internet Explorer zero-day flaw also exist in Windows XP and other OS versions, including Vista and Windows 7. The Internet Explorer security glitch can be exploited by getting users to a compromised website hosting malware designed to take advantage of it. Microsoft has already confirmed a limited number of attacks aimed at Internet Explorer users and said that while Internet Explorer 10 and 11 are fully protected, it's also investigating the issue to make sure that everyone will be on the safe side as soon as possible. That's not going to happen for Windows XP users though, as this OS version no longer receives updates and security patches, so computers running it will basically stay unprotected. CERT UK, however, recommends users to switch to a different browser, especially if they're running Windows XP, as both Google Chrome and Mozilla Firefox do not have such a vulnerability in their engines. Of course, the same thing has also been said by many other security experts across the world, but it remains to be seen how many users actually get this message. "To mitigate this vulnerability for machines running Windows XP, users should consider downloading Microsoft's Enhanced Mitigation Experience Toolkit (EMET) 4.1, which in its default configuration should help to mitigate this vulnerability. Users should also consider using alternative browsers, such as Google Chrome and Mozilla Firefox; and ensure that their antivirus software is current and regularly updated," a notification rolled out this morning reads. At the same time, the UK government body also explained that upgrading from Windows XP to a newer OS version is always a better choice because Windows 7 and Windows 8.1 come not only with more secure builds of Internet Explorer, but also with enhanced stability and performance that could help you if similar problems occur in the future. "In the longer term, our advice remains (as per alerts issued during March and April 2014) that where possible users and enterprises should implement a controlled migration from Windows XP to later versions of the operating system," it said. Windows XP is still being used by 28 percent of the desktop computers worldwide, but figures are very likely to drop as many large companies are completing the transition to a newer OS. To read more click **HERE**