# THE CYBER SHIELD

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

*4 August 2014*

**Purpose**
Educate recipients of cyber events to aid in protecting electronically stored DoD, corporate proprietary, and/or Personally Identifiable Information from theft, compromise, espionage

**Source**
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

**Publisher**
* SA Jeanette Greene
Albuquerque FBI

**Editor**
* CI SA Scott Daughtry
DTRA Counterintelligence

**Subscription**
To receive this newsletter please send an email to scott.daughtry@dtra.mil

**Disclaimer**
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

**NMCIWG Members**
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, and Sandia National Labs

**Distribution**
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings. Credit is given to the NMCIWG for the compilation of this open source data

*July 29, WDAY 6 Fargo* – (North Dakota) **Essentia Health informs patients of information breach.** About 430 Essentia Health patients in Fargo were notified the week of July 21 of a security breach after they were invited to an educational event through an outside marketing firm who had been given their personal information without their permission or knowledge. Source: http://www.wday.com/content/essentia-health-informs-patients-information-breach

*July 31, Securityweek* – (International) **Innominate patches vulnerability in mGuard industrial security routers.** Innominate Security Technologies fixed a vulnerability in its mGuard series of industrial security routers that could have allowed an unauthenticated attacker to obtain configuration information. The routers are frequently used in the manufacturing, healthcare, and communications industries, and users were advised to update their firmware to close the vulnerability. Source: http://www.securityweek.com/innominate-patches-vulnerability-mguard-industrial-security-routers

*July 31, The Register* – (International) **POW! Apple smites Macbook Air EFI firmware update borkage.** Apple released a firmware update for 2011 and later MacBook Air systems that addresses an issue encountered by users in an EFI firmware update released the week of July 21 that caused MacBooks to become unresponsive. Source: http://www.theregister.co.uk/2014/07/31/apple_macbook_air_sleep_patch_repatched/

*July 30, Softpedia* – (International) **Pushdo botnet continues to stay strong.** Researchers with Bitdefender reported that they have recorded a steady increase in the number of infected systems attempting to contact the command and control servers for the Pushdo malware botnet, with around 200,000 unique IP addresses observed. Source: http://news.softpedia.com/news/Pushdo-Botnet-Continues-to-Stay-Strong-452835.shtml

*August 1, Softpedia* – (International) **New point-of-sale malware "Backoff" scrapes RAM for card data.** The U.S. Computer Emergency Response Team (US CERT) published an advisory warning of a new family of malware known as "Backoff" that can compromise point-of-sale (PoS) systems by compromising remote desktop applications and then performing memory scraping to obtain payment card track data. The malware currently has very low rates of detection in most antivirus engines and contains various other capabilities including keystroke logging and injecting a malicious stub into explorer.exe to increase persistency. Source: http://news.softpedia.com/news/New-Point-of-Sale-Malware-Backoff-Scrapes-RAM-For-Card-Data-453051.shtml

*July 31, Krebs on Security* – (National) **Sandwich chain Jimmy John's investigating breach claims.** Sandwich restaurant chain Jimmy John's reported that it is working with authorities to investigate a possible breach of customer payment data. Source: https://krebsonsecurity.com/2014/07/sandwich-chain-jimmy-johns-investigating-breach-claims/

*August 1, Securityweek* – (International) **USB device firmware can be reprogrammed to hide sophisticated malware.** Researchers from SRLabs reported developing a new piece of malware that can reprogram USB controller chips to spoof other devices, allowing an attacker to take control of a computer, steal data, and perform other actions. The researchers plan to demonstrate the "BadUSB" malware at the upcoming Black Hat security conference. Source: http://www.securityweek.com/usb-device-firmware-can-be-reprogrammed-hide-sophisticated-malware

*August 1, Softpedia* – (International) **Hackers steal video game source code.** Dell SecureWorks' Counter Threat Unit identified a group of attackers labeled Threat Group-3279 that has been observed targeting video game and entertainment companies to steal source code and create cracks or cheat codes for games. The group is believed to be associated with the China Cracking Group and leverages a variety of tools and pieces of malware, including ones created by the group. Source: http://news.softpedia.com/news/Hackers-Steal-Video-Game-Source-Code-453108.shtml

*August 1, Securityweek* – (International) **"Pitty Tiger" threat actors possibly active since 2008: FireEye.** Researchers at FireEye analyzed the "Pitty Tiger" advanced persistent threat group first identified by Airbus Defense & Space and found that the group may have been active since 2008. The Pitty Tiger campaign targeted a variety of sectors including the defense and telecoms industries, and is believed to be operating from China. Source: http://www.securityweek.com/pitty-tiger-threat-actors-possibly-active-2008-fireeye

*August 1, Securityweek* – (International) **New ransomware uses GnuPG to encrypt files.** Researchers at Symantec and Trend Micro analyzed a new piece of ransomware dubbed Trojan.Ransomcrypt.L or BAT_CRYPTOR.A that uses GNU Privacy Guard to encrypt files for ransom and can be easily updated by its controllers. Trend Micro also identified another new piece of ransomware dubbed Cryptoblocker which does not use RSA keys and appears to have been written by inexperienced writers. Source: http://www.securityweek.com/new-ransomware-uses-gnupg-encrypt-files

*August 1, Softpedia* – (International) **Fiesta Exploit Kit delivers double payload.** A Malwarebytes researcher reported that attackers have modified the way the Fiesta Exploit Kit delivers its malicious payload by delivering two malicious files at once to attempt to avoid antivirus detection for at least one file. Source: http://news.softpedia.com/news/Fiesta-Exploit-Kit-Delivers-Double-Payload-453143.shtml

### OSPF Vulnerability Patched by Cisco

SoftPedia, 4 Aug 2014: Late last week, Cisco announced that a security glitch touching on Open Shortest Path First (OSPF) Routing Protocol Link State Advertisement (LSA) database had been fixed in the new versions of affected products. The developer warns that this vulnerability could allow a potential attacker to take complete control of the OSPF Autonomous System (AS) domain routing table, blackhole and intercept traffic without having to go through an authentication process. According to Cisco, leveraging this security flaw involves determining certain parameters in the LSA database on the target's router and injecting crafted OSPF packets; successful exploitation would result in flushing the routing table and sending the crafted OSPF LSA type 1 update through the targeted domain. "Network devices running the OSPF protocol may be impacted by this vulnerability if they receive a crafted LSA type 1 packet. This packet does not have to be acknowledged, and it can originate from a spoofed IP address," the developer notes. However, the intruder needs to know certain parameters in order to be successful, such as the network placement and the IP address of the targeted device, the sequence numbers for the Link State Advertisement database, and the ID of the OSPF Designated Router. The affected products are: Cisco ASR 5000, Cisco NX-OS Software, Cisco Firewall Services Module (FWSM), Cisco Adaptive Security Appliance (ASA), Cisco ASA Service Module (ASA-SM) and Cisco Pix Firewall, Cisco IOS-XE Software, and Cisco IOS Software. To read more click HERE

### Registry-Residing Malware Creates No File for Antivirus to Scan

SoftPedia, 4 Aug 2014: A new form of persistent malware has been discovered, one which does not create any file on the disk and stores all activities in the registry. In a blog posted at the end of July, security researcher Paul Rascagneres of GData details the particularities of the new type of malware, dubbed Poweliks, whose methods he labels as "rather rare and new," since everything is performed in the memory of the computer system and there are several layers of code to get through in order to avoid analysis. The attack vector is an email with a malcrafted Microsoft Word document attached. The vulnerability leveraged by the attackers is CVE-2012-0158, which affects Office and several other Microsoft products. It is not new, but many users are still using old versions of the software that could be compromised. Once the file is launched, the cybercriminals turn on the persistency feature of the malware by creating an encoded autostart key in the registry. It seems that the encoding technique used by the malware was originally created by Microsoft to safeguard their source code from being altered. In order to avoid detection by system tools, the registry key is hidden by providing a name in non-ASCII characters, which makes it unavailable to the Registry Editor (regedit.exe) in Windows. By creating the auto-start key, the attackers make sure that a reboot of the system does not remove it from the computer. By decoding the key, Rascagneres observed two sets of code: one that verified if the affected machine had Windows PowerShell installed, and another one, a Base64-encoded PowerShell script, for calling and executing the shellcode. According to the researcher, the shellcode executes the payload, which attempts to connect to a remote command and control (C&C) server for receiving instructions. There are multiple IP addresses for C&C servers, all hard-coded. The peculiarity of this malware is that it does not create any file on the disk, making it more difficult to be detected through classic protection mechanisms. "To prevent attacks like this, AV solutions have to either catch the file (the initial Word document) before it is executed (if there is one), preferably before it reached the customer's email inbox. Or, as a next line of defense, they need to detect the software exploit after the file's execution, or, as a last step, in-registry surveillance has to detect unusual behavior, block the corresponding processes and alert the user," writes Rascagneres. This type of malicious behavior is not new though, as a sample was also analyzed on KernelMode.info in mid-July, this year. In that case, the same vulnerability was exploited through a malicious RTF attached to an email claiming to be from Canada Post and/or USPS mail service. To read more click HERE

### New Citadel Trojan Variant Creates Backup Backdoor Access

SoftPedia, 4 Aug 2014: A new version of the Citadel Trojan, which is based on the infamous Zeus banking malware, has been discovered by security researchers to allow access to the affected systems even after it has been detected and eliminated. The feat is pulled via the remote desktop capabilities available in Windows operating system. In a recent blog post, security researchers from IBM have analyzed a sample of the new Citadel strain that appears to be used for specifically targeting enterprise environments. Although Citadel has included remote desktop capabilities since its first release via the built-in VNC module, when it was removed from the affected system it would no longer have access to it. However, the most advanced types of malicious software today have built-in remote control capabilities. Once it infects a machine, the latest version of the malware offers operators the possibility to execute commands via the Windows shell to add a new local user with a specific name and a password that is set never to expire. Next, they add it to the local administrator group and then to the local RDP (Remote Desktop Protocol) group. This way, they gain remote access to the system. The attackers provide their own name and password for the user. In the sample analyzed by the IBM researchers, the name was "coresystem" and the password was "Lol117755C." Since threat actors can access the computer system remotely through a service that is not connected to the malware, even if Citadel is detected and removed, their presence on the system remains unaffected, allowing them to initiate future attacks. IMB security researcher Etay Maor believes that the current variant has been designed to target companies. Under this scenario, the new Citadel offers attackers multiple advantages, one of them being the fact that intercepting a rogue RDP connection is more difficult to achieve, especially since many companies use the protocol for technical support. Moreover, he says that the illusion of safety after administrators find the malware on the systems is also contributing to the persistency of the attack. "A user who was vigilant enough to detect and remove Citadel will now feel safe to use his or her device, thinking it is clean," he writes. If this strain switched its financial fraud purpose and it is aimed at corporate environments, it shows that threat actors have no problem using code that has been involved in numerous cybercrime incidents and adapt it to fresh needs. To read more click HERE

### Symantec, Kaspersky Security Products Blacklisted by Chinese Government

SoftPedia, 4 Aug 2014: The Chinese government has banned the usage of security products from foreign developers Symantec and Kaspersky for national security and public interests. At the moment, on the list of the government's procurement agency there are five approved security software brands, all from China. These include Qihoo 360 Technology, Venustech, CAJinchen, Beijing Jiangmin, and Rising. The announcement came from People's Daily newpaper, which first posted the news on Twitter and then offered slightly more details on their Facebook page. Back in May, China's State Internet Information Office informed that it would initiate an investigation on the major IT products used by government institutions for national and public interests. It looks like the assessment has been completed and led to banning foreign technology that could be used for protecting government systems. The news post on People's Daily says that there is no evidence that the decision was taken as a result of Edward Snowden's revelations about the US National Security Agency's mass surveillance program, PRISM. However, this is an effort made by the Chinese government to promote domestic IT products. The newspaper also says that, currently, the only foreign operating system brand still on the suppliers list is Microsoft, although in May a notice was issued to ban the purchase of Windows 8 operating system. "China's homegrown technology companies also got the better of their foreign counterparts in the personal computer operating system supplier list, making Microsoft the only foreign brand," writes Zhang Qian for the Chinese publication. Earlier this month, Symantec's Data Loss Prevention Product was replaced by the Chinese government with a domestic product. The reason was that the US company allegedly included backdoors to gather intelligence, according to a post in the newspaper Sina. The same post informed that public security agencies at all levels were prohibited the installation of Symantec products. Last week, multiple Microsoft offices in China have been raided by investigators, who seized computers, documents and email communication of the company's employees. The authorities targeted locations in Beijing, Shanghai, Chengdu, and Guangzhou. It appears that China believes that Microsoft, Apple, Symantec and Cisco are important partners of the NSA, allowing the intelligence service access to their systems in order to collect information. As far as Kaspersky is concerned, spokesperson Alejandro Arango talked to Reuters and said that the company was investigating the matter and engaged in communication with the Chinese authorities in order to sort things out, but no details were made available. To read more click HERE

### Mozilla Warns of Accidental Leak of Developer Network Email Database

SoftPedia, 4 Aug 2014: Email addresses of 76,000 members of Mozilla Developer Network (MDN) and 4,000 passwords have become publicly available because of a process failing to sanitize data properly. Mozilla issued a warning about the incident, saying that they were informed by a web developer that around June 23 a data sanitization flaw caused the disclosure of the sensitive information about the developers. It appears that the error persisted for a period of 30 days, and when Mozilla learned about the leak, they immediately pulled the database dump file and disabled the glitchy process in order to prevent further disclosure. "While we have not been able to detect malicious activity on that server, we cannot be sure there wasn't any such access," says a blog post from Stormy Peters, Director of Developer Relations, and Joe Stevensen, Operations Security Manager. The passwords were encrypted and the erroneous disclosure offered only salted hashes, which means that they cannot be used for authentication on the Mozilla Developer Network website. However, email addresses could be used for sending spam. All users affected by the incident have been alerted of the accidental leak and advised to change their passwords for other non-Mozilla websites or authentication systems if they are similar to the leaked ones for MDN. "In addition to notifying users and recommending short term fixes, we're also taking a look at the processes and principles that are in place that may be made better to reduce the likelihood of something like this happening again," say the Mozilla representatives. To read more click HERE

## PoS Malware Attacks Increase, Simple Solutions Could Stop Some of Them

SoftPedia, 4 Aug 2014: Credit and debit card data is what cybercriminals are after these days and there are plenty of ways to get it, but with thousands of transactions processed by point-of-sale (PoS) systems of large retailers on a daily basis, the payment terminals make for a prime target. Point-of-sale terminals read the information from the magnetic stripe (magstripe) of a credit or debit card when it is swiped through. The information is then either sent directly to the bank of the retailer, or to a back-of-house (BoH) server that gathers card data from multiple PoS systems and delivers it to a payment processing service. Regardless of the method used to handle the transactions, an authorization message needs to be returned to the PoS system for the purchase to be accepted; the entire communication is encrypted. Malware designed for this type of payment systems seek to collect the information on the card that can be used for online purchases, and if the details on the magstripe (Track 1 and Track 2) are also taken, cards can be cloned and used in brick-and-mortar stores. Infecting PoS systems is a trend on the rise many security experts warned about towards the end of last year, especially since retailer Target reported it suffered a breach that led to the loss of card data information of about 40 million customers. The cybercriminals who compromised the Target PoS systems on November 27, 2013, used specific malware that would steal the card information from the memory of the system, where it is not encrypted before being sent securely for processing. This method, called RAM scraping, is not new. Dexter, one PoS malware relying on the same memory scraping method for stealing data, was discovered back in 2012, and its code has been leaked at one point, giving birth to several variants, StarDust and Revolution being considered subsequent versions of the first Dexter release. Kaptoxa (slang for "potato" in Russian), a malware that later changed its name to the better known BlackPOS, is believed to have been employed in the Target data breach and has been on sale on underground forums for some time. Apart from these two, other malicious tools exist, specifically designed for stealing the card data from the memory of PoS systems. Alina is yet another solution of the same malware breed, having several variants and versions crooks can leverage. Lacking complexity, ChewBacca malware managed to steal card data from the RAM of the infected PoS systems of dozens of retailers in more than 10 countries, the US, Russia, Australia and Canada among them, since October 2013. Another PoS malware family, discovered at the beginning of 2014 and responsible for compromising thousands of credit cards in the US and Canada, is JackPOS; security boffins at Fortinet said in a blog post in June that they detected only one version of the threat, but that it had multiple strains. The criminal activity relying on this type of malicious utilities has increased in both frequency and complexity. In more recent attacks, cybercriminals have employed botnets to scan for computer systems that can be accessed from afar, through remote desktop programs such as LogMeIn, VNC, Microsoft RDP, PCAnywhere. Then they look for PoS software and attempt to brute-force the remote login feature with credentials available in a dictionary file downloaded from the command and control server. The malware has been dubbed BrutPOS by FireEye, while researchers at IntelCrawler say that the name of the botnet project carrying out the PoS search has been released on underground forums since May 2014. A recent warning from US CERT (Computer Emergency Readiness Team) puts in the spotlight a new PoS malware family called Backoff, which has been identified in multiple forensic investigations. The organization says that the threat is still persistent as of July 2014. In this case, memory scraping is not the only method to steal financial information, as Backoff also integrates keylogging functionality, which can help the attacker determine the nature of the captured information. Although it is not easy to thwart malicious activity targeting PoS systems, there are several controls that can be imposed to limit the risks. Strong passwords, enabling two-factor authentication and limiting remote access to the systems are among the easiest methods that can prevent attackers from stealing the login credentials. US CERT also recommends configuring the remote access account to lock after a period of time or after a specific number of failed login attempts. Firewalls for network segmentation of the sensitive systems, changing the default remote desktop listening port, and encrypting the communication to the remote computer through the use of SSH and SSL are also among the recommendations. Highly important, systems should be reviewed periodically by pen-testing them for weak spots that can be leveraged by an intruder, and employees should be educated to detect attempts to deceive them into providing cybercriminals with a backdoor to the business' computer systems. "Companies need to shift their approach to security from an 'outside-in' mentality of perimeter-based security to an 'inside-out' model where they assume the bad guy is already on the network." "Access controls, role-based monitoring and data encryption are critical requirements to protect critical systems from insider threats, which can be especially damaging in concentrated environments like cloud infrastructure," says via email Eric Chiu, president of HyTrust cloud control company. To read more click HERE

### New Gameover ZeuS Variant and Shylock Rebuild Botnets

SoftPedia, 1 Aug 2014: New findings from security researchers suggest a resurge in the activity of the Gameover ZeuS and Shylock malware, as the latest telemetry information indicates that a large bot crowd has been created. Israel-based security firm Seculert has found that a new variant of Gameover ZeuS (GOZ) is currently in circulation, and although it is not as prevalent as its predecessor, it still managed to infect almost 10,000 computers. Aviv Raff, CTO and lead malware researcher at Seculert, writes in a blog post that they found some changes in the latest strain of GOZ. First of all, the malware authors have dropped the pee-to-peer communication mechanism that allowed the threat actors to control and update the infected computers. This feature is what actually made the botnet difficult to dismantle in the first place. Another change observed by Raff was a new DGA (domain generation algorithm), which spews a list of 1,000 domains per day in order to hide the command and control server used by the attackers. The number of generated domains and the frequency are impressive, considering that the previous version would spew a list with the same amount of domains in a week. Since the company had previously sinkholed GOZ, it was able to compare the new telemetry and determined that during the past days more and more infected systems contacted the sinkhole system, "reaching as high as almost 10,000 infected devices." However, according to their information, the peak was recorded on July 25, and the number of communication requests dwindled to 4,000 on July 30. In the case of Shylock, Raff says that almost 10,000 bots per day tried to communicate with the sinkholed domain. Data from their systems shows that after July 29 more than 8,000 computers contacted the domain, suggesting that the number was on the rise. Although the efforts of law enforcement agencies and private security companies translate into a significant decrease of cyber-criminal activities, other threat actors with access to the same type of malware can pick up the nefarious activity and create new botnets. After the resonant action to disrupt the GameOver ZeuZ botnet, some security companies warned that the fight might not be over because of the complexity of the communication network. On July 10, Malcovery informed of a new strain that gave up the peer-to-peer mechanism and that a new DGA had been integrated. In the case of Shylock, the actors behind it are believed to be highly organized, and they are not likely to give up the malicious activity once their botnet is disrupted. To read more click HERE

### Paddy Power Historical Data Breach Affected 649,000 Customers

SoftPedia, 1 Aug 2014: On Thursday, in a statement to their customers, Paddy Power, a company that provides bookmaking services, admitted to a historical data breach that occurred in October 2010 and resulted in compromising a data sheet with details for 649,055 customers. The company said that, during the incident, no financial information or customer passwords were accessed by the hackers. However, the intruders managed to steal names, usernames, addresses, email addresses, phone contact numbers, dates of birth and security questions and answers. From a security point of view, all this information is more than enough for cybercriminals to make some money through identity theft, sending spam or phishing emails. Although Paddy Power knew about intruders hacking their systems in 2010, they were not aware of the magnitude of the incident until recently (in May), when the company "took legal action in Canada with the assistance of the Ontario Provincial Police to retrieve the compromised dataset from an individual," the statement says. It appears that the vulnerability leveraged by the intruders back in 2010 had been solved at that time, since customers making an account with the service beyond that date are not affected. Representatives of the Irish booking service inform that compromising the accounts based on the stolen information could not be possible. To further stress that no credit or debit card details and passwords were compromised, the company says that account monitoring systems did not trigger any alert of suspicious activity indicative of breaching customer accounts. "We take our responsibilities regarding customer data extremely seriously and have conducted an extensive investigation into the breach and the recovered data. That investigation shows that there is no evidence that any customer accounts have been adversely impacted by this breach. We are communicating with all of the people whose details have been compromised to tell them what has happened," says Peter O'Donovan, MD Online, Paddy Power. The company is currently issuing notifications to all affected customers, who are recommended to change the security question and answer on other sites, if the pair is the same one used for the Paddy Power account. The Data Protection Commissioner (DPC) was not informed of the incident at the time of its occurrence. In a statement for Techcentral.ie, the Office of the DPC expressed their disappointment that they were notified only when new information about the breach came to surface, four years later: "However, this Office is disappointed that Paddy Power did not report the matter to us back in October 2010 in line with best practice." To read more click HERE

### Symantec Publishes Advisory for Mitigating Zero-Day Risks

SoftPedia, 1 Aug 2014: In the wake of the zero-day threats in Symantec Endpoint Protection (SEP) suite presented by the Offensive Security team this week, Symantec has released an advisory for avoiding the risks of compromise. The problem appears to impact the Application and Device Control component in the suite, and the developer says that it received no reports of compromise. However, should the vulnerability be exploited, the consequences range from crashing the client to creating a denial of service condition and even escalation to administrator privileges and gaining control of the affected system, which was also the point made by Offensive Security in a video demonstrating the success of their exploit. Symantec also points out that the flaw is considered to have medium severity and cannot be manipulated remotely. All versions of SEP clients 11.x and 12.x running Application and Device Control component are vulnerable. At the moment, there are no patches for removing the issue, but Symantec offers solutions for mitigating the risk on the affected versions of the client In the case of 12.x, one way to avoid exploitation is to disable the driver of the vulnerable component (Application and Device Control); another is to remove the component completely by uninstalling it. On systems with version 11.x of SEP installed, the only solution provided by the developer is to withdraw the Application and Device Control policy; a restart is required for the modification to take effect. This flaw may not be of critical nature, but the simple fact that it exists in software designed to protect a computer system is quite worrying. A security researcher from Singapore-based Coseinc, a private company that offers information security services, made a presentation on the flaws available in multiple security products for consumers. In his presentation at the SysScan 360 security conference, Joxean Koret exposed how he managed to find dozens of vulnerabilities exploitable both locally and remotely, using a fuzzing test tool of his own making. Some of the glitches discovered would allow escalation of privileges and execution of arbitrary code. His opinion is that an antivirus product installed on a computer actually increases the attack surface, because such applications run with the highest privileges. "If your application runs with the highest privileges, installs kernel drivers, a packet filter and tries to handle anything your computer may do...Your attack surface dramatically increased," he said at the conference. However, from the slides of the presentation, it appears that Symantec's products were not tested by Koret. To read more click HERE

### Microsoft Fixes Three-Year Old Security Flaw in Internet Explorer

SoftPedia, 1 Aug 2014: Microsoft is making really big efforts to make its software more secure (or at least, that's what the company is saying), so every month's Patch Tuesday rollout addresses vulnerabilities in a wide array of products, including Windows, Internet Explorer, and Office. Redmond has recently fixed a vulnerability in Internet Explorer that was three years old, as it was found by the security researchers at VUPEN on February 12, 2011. Officially patched on June 17 as part of bulletin MS14-035, the glitch was disclosed by VUPEN at the Pwn2Own hacking event in March this year. "The vulnerability is caused due to an invalid handling of a sequence of actions aimed to save a file when calling 'ShowSaveFileDialog()', which could be exploited by a sandboxed process to write files to arbitrary locations on the system and bypass IE Protected Mode sandbox," the security researchers explained. The Microsoft Security Bulletin MS14-035 was released to address two publicly disclosed vulnerabilities and 58 privately reported glitches in Internet Explorer, including the one discovered by VUPEN. “The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights,” Microsoft explained. “The security update addresses the vulnerabilities by modifying the way that Internet Explorer handles objects in memory, validates permissions, and handles negotiation of certificates during a TLS session.” The security flaw found by VUPEN affected pretty much all Internet Explorer versions on the market, including the old IE6 and the newly-launched IE11 which is part of Windows 8.1. Microsoft hasn’t shared any details regarding the number of exploits that could have involved the flaw found by VUPEN, but since it was reported via private channels, users have most likely been on the safe side until the company rolled out a patch. In case you’re wondering, VUPEN has a pretty good history on finding vulnerabilities at hacking competitions, as the company has until now raised no less than $300,000 (€225,000) for flaws found in Adobe Reader, Internet Explorer, Mozilla Firefox, and Adobe Flash, according to The Register. At this point, all Internet Explorer installations should be on the safe side if all security patches delivered via Windows Update are installed. To read more click HERE