The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

23 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

April 21, SC Magazine – (International) **Critical update makes P2P Zeus trojan even tougher to remove.** Fortinet researchers found that the peer-to-peer (P2P) Zeus banking trojan recently received an update that also installs a rootkit driver, making the trojan difficult to remove from infected systems. Source: http://www.scmagazine.com/critical-update-makes-p2p-zeus-trojan-even-tougher-to-remove/article/343551/

April 22, Help Net Security – (International) **Supposedly patched router backdoor was simply hidden.** A security researcher who discovered a backdoor vulnerability in several popular home routers found that the firmware update issued by manufacturer Sercomm does not close the vulnerability but instead hides the backdoor. The backdoor can then be opened after sending a specific network packet to the router from the local area network (LAN) or the Internet service provider (ISP), allowing attackers reset the device's configuration, username, and password to default settings. Source: http://www.net-security.org/secworld.php?id=16721

April 22, Softpedia – (International) **Django 1.6.3 released to address 3 security issues.** The developers of the Django framework for Python released new versions of the framework, closing three security vulnerabilities. Source: http://news.softpedia.com/news/Django-1-6-3-Released-to-Address-3-Security-Issues-438666.shtml

April 21, Threatpost– (International) **Oracle gives Heartbleed update, patches 14 products.** Oracle released updates for five products April 21, closing vulnerabilities related to the Heartbleed vulnerability in OpenSSL. Source: http://threatpost.com/oracle-gives-heartbleed-update-patches-14-products/105576

SharePoint users are breaching security policies

Heise Security, 17 Apr 2014: A study, conducted amongst attendees at last month's Microsoft's SharePoint Conference in Las Vegas, has found that at least 36% of SharePoint users are breaching security policies, and gaining access to sensitive and confidential information to which they are not entitled. It also found that, of the 19% of respondents whose organizations do not allow sensitive information to be stored within SharePoint environments, nearly a quarter of them later confessed they knew of individuals who had accessed content that they were not entitled to, demonstrating that users were ignoring this directive. Most alarmingly of all, the majority of administrators perceive their 'permission' to be unrestricted - responding with comments anecdotally that included 'I am entitled to see everything' and 'Administration access is God mode'. This incomprehension is testament that, albeit unintentionally, many SharePoint administrators are in fact abusing their privileged access rights, ultimately putting confidential data at risk. The results reveal many are struggling, with some even failing completely. Hakan Saxmo, CTO at Cryptzone, clarifies, "Of the people spoken to during our survey, 19% recognize there are risks and try to limit them by banning sensitive information from being stored within SharePoint. I say 'try', because it turns out that just 18% actually use technical controls with 73% instead relying on a written policy or an 'understanding' with their workforce. And we all know how many people actually 'do as they're told'." "It's hardly

surprising that sensitive information is not only finding its way into SharePoint repositories, but that users are discovering and accessing it too. It's my opinion that the 23% that put their hand up to sensitive information being accessed is conservative and others either didn't want to confess or, perhaps even worse, are oblivious that it's even happening," added Saxmo. The study found that interest in salary details had dropped, by over 50%, in 2014 to just 22%, but there was a marked increase in accessing other types of employee details – from 15 to 22%. Valuable data assets - such as insider information and Intellectual Property, also saw significant rises of around 50%. Saxmo adds, "While it is unclear why there's less interest in what others earn, one hypothesis is that the recent economy has encouraged people to consider changing employment, and are therefore looking for information that could prove useful securing a new role." With compliance high on many organizations' agendas, it's perhaps surprising that 36% of organizations do not audit their system, and therefore can't be sure if they're putting sensitive and confidential data at risk or not. Interestingly, a higher percentage of organizations undertake an internal compliance audit of their SharePoint environments (53%) than an external compliance audit (28%) – of which 25% perform both. Findings this year show that a greater percentage of organizations no longer allow third party access to their SharePoint environment. While it is unclear why this appears to have tightened, it could be related to the high percentage of organizations (79%) storing sensitive and confidential information in their SharePoint environments and the fear of exposing it to others. Over half of respondents (56%) reported that mobile access to SharePoint applications and data is an issue within their organizations. Saxmo concludes, "Users won't follow the rules, just because they are there!" To read more click **HERE**

3M payment cards compromised in Michaels Stores/Aaron Brothers breach

Heise Security, 18 Apr 2014: In the wake of the highly publicized Target and Neiman Marcus breaches, Texas-based arts and crafts store chain Michaels has stated in January that it has been targeted by cyber crooks that were after their customers' payment card data. The breach has now definitely been confirmed, and the impact is huge: approximately 3 million payment cards were potentially compromised. Since the January announcement, Michaels has retained two independent security firms to investigate the breach and has worked closely with law enforcement authorities. "After weeks of analysis, the company discovered evidence confirming that systems of Michaels stores in the United States and its subsidiary, Aaron Brothers, were attacked by criminals using highly sophisticated malware that had not been encountered previously by either of the security firms," the company stated in the press release. The affected systems contained payment card numbers and expiration dates, but it seems that the customers' name, address or PIN weren't compromised. "Regarding Michaels stores, the attack targeted a limited portion of the point-of-sale systems at a varying number of stores between May 8, 2013 and January 27, 2014. The analysis conducted by the security firms and the company shows that approximately 2.6 million cards may have been impacted, which represents about 7% of payment cards used at Michaels stores in the US during the relevant time period," they stated, and offered a list of stores that were affected (**link**). A similar list has been compiled of the Aaron Brothers stores (**link**) affected by the malware between 26, 2013 and February 27, 2014, when some 400,000 cards are thought to have been impacted. "The company has provided data about potentially affected payment cards to the relevant card brands so they can take appropriate action," the press release says. To read more click **HERE**

Heartbleed attacker hijacked VPN active user sessions

Heise Security, 22 Apr 2014: As the number of the most popular websites that still haven't patched their servers against the Heartbleed exploit continues to diminish (go here for an up-to-date list of those that are still vulnerable), researchers from cybersecurity firm Mandiant have reported that have identified successful attacks in the wild by targeted threat actors exploiting the Heartbleed bug. In a blog post published on Friday, they detailed a particular attack they investigated that involved the exploitation of the Heartbleed vulnerability in a SSL VPN concentrator - a device that handles a large number of incoming VPN tunnels. "Beginning on April 8, an attacker leveraged the Heartbleed vulnerability against a VPN appliance and hijacked multiple active user sessions. Specifically, the attacker

repeatedly sent malformed heartbeat requests to the HTTPS web server running on the VPN device, which was compiled with a vulnerable version of OpenSSL, to obtain active session tokens for currently authenticated users," they shared. "With an active session token, the attacker successfully hijacked multiple active user sessions and convinced the VPN concentrator that he/she was legitimately authenticated. The attack bypassed both the organization's multifactor authentication and the VPN client software used to validate that systems connecting to the VPN were owned by the organization and running specific security software." If you are wondering how they know for sure that the Heartbleed bug was exploited in the attack, the answer is that the victim organization implemented a set of IDS signatures to identify Heartbleed network activity, and the IDS alerts were triggered over 17,000 times. Also, the VPN logs showed VPN connections of multiple users speedily "flip flopping" between users' IP address and malicious IP addresses tied to different ISPs. "The attack was spotted in its later stages, when the attacker tried to "move laterally and escalate his/her privileges within the victim organization." The researchers have several recommendations for organizations worrying about being hit with this type of exploit: patch/upgrade your infrastructure, implement appropriate network intrusion detection signatures to spot the attacks, and check out VPN logs "for instances where the IP address of a session changed quickly and repeatedly between two IP addresses from different network blocks, geographic locations, or from different service providers." To read more click **HERE**

Nine patterns make up 92 percent of security incidents

Heise Security, 23 Apr 2014: Verizon security researchers have found that 92 percent of the 100,000 security incidents analyzed over the past ten years can be traced to nine basic attack patterns that vary from industry to industry. "After analyzing 10 years of data, we realize most organizations cannot keep up with cybercrime – and the bad guys are winning," said Wade Baker, principal author of the Data Breach Investigations Report series (**link**). "But by applying big data analytics to security risk management, we can begin to bend the curve and combat cybercrime more effectively and strategically. "Organizations need to realize no one is immune from a data breach. Compounding this issue is the fact that it is taking longer to identify compromises within an organization – often weeks or months, while penetrating an organization can take minutes or hours," Baker said. The DBIR identifies the nine threat patterns as: miscellaneous errors such as sending an email to the wrong person; crimeware (various malware aimed at gaining control of systems); insider/privilege misuse; physical theft/loss; Web app attacks; denial of service attacks; cyberespionage; point-of-sale intrusions; and payment card skimmers. This year's report found that on average, just three threat patterns cover 72 percent of the security incidents in any industry. For example, in the financial services sector, 75 percent of the incidents come from Web application attacks, DDoS and card skimming, while 54 percent of all manufacturing attacks are attributed to cyberespionage and DDoS. In the retail sector, the majority of attacks are tied to DDoS (33 percent) followed by point-of-sale intrusions (31 percent). Key findings include:

- Cyberespionage is up again in the 2014 report, representing a more than three-fold increase compared with the 2013 report, with 511 incidents. (This is partially due to a bigger dataset.) In addition, these attacks were found to be the most complex and diverse, with a long list of threat patterns. As it did last year, China still leads as the site of the most cyberespionage activity; but the other regions of the world are represented, including Eastern Europe with more than 20 percent.
- For the first time, the report examines distributed denial of service attacks, which are attacks intended to compromise the availability of networks and systems so that, for example, a website is rendered useless. They are common to the financial services, retail, professional, information and public sector industries. The report points out that DDoS attacks have grown stronger year-over-year for the past three years.
- The use of stolen and/or misused credentials (user name/passwords) continues to be the No. 1 way to gain access to information. Two out of three breaches exploit weak or stolen passwords, making a case for strong two-factor authentication.

• Retail point-of-sale (POS) attacks continue to trend downward, exhibiting the same trend since 2011. Industries commonly hit by POS intrusions are restaurants, hotels, grocery stores and other brick-and-mortar retailers, where intruders attempt to capture payment card data. While POS breaches have been in the headlines lately, they are not indicative of the actual picture of cybercrime.
• While external attacks still outweigh insider attacks, insider attacks are up, especially with regard to stolen intellectual property. The report points out that 85 percent of insider and privilege-abuse attacks used the corporate LAN, and 22 percent took advantage of physical access.

Eric Chiu, President of HyTrust, said: "As we see in the report, everyone is vulnerable to some type of security incident, whether external attacks or insider misuse and errors that harm systems and expose data. The number one threat method was stolen user credentials. Also startling is the widening gap between the time to compromise and time to discover breaches. Both of these points underscore that breaches are happening more and more from the inside where attackers are using stolen credentials, and once on the network, are almost impossible to detect." To read more click **HERE**

Apple Releases Security Update 2014-002 for OS X

SoftPedia, 23 Apr 2014: Apple has released Security Update 2014-002 for OS X 10.7 (Lion), OS X 10.8 (Mountain Lion), and OS X 10.9 (Mavericks) addressing over a dozen distinct bugs in the operating system, some shared with the iOS mobile operating system. Security researcher Antoine Delignat-Lavaud of Prosecco at Inria Paris informed Apple of a CFNetwork HTTPProtocol flaw where an attacker in a privileged network position could obtain web site credentials. According to the description, “Set-Cookie HTTP headers would be processed even if the connection closed before the header line was complete. An attacker could strip security settings from the cookie by forcing the connection to close before the security settings were sent, and then obtain the value of the unprotected cookie.” Apple addressed this flaw by instructing CFNetwork HTTPProtocol to ignore incomplete HTTP header lines. The issue was also found and patched in iOS 7 (with the release of iOS 7.1.1). A format string issue was found in the handling of URLs by Lukasz Pilorz of runic.pl and Erik Kooistra. Affecting CoreServicesUIAgent, “This issue was addressed through additional validation of URLs,” Apple says. OSes other than Mavericks are unaffected. iOS 7.1.1 patches the same bug for users of iPhones, iPod touch players, and iPads. A FontParser vulnerability is also disclosed in the advisory. Impacting only Mountain Lion computers, the bug (once exploited) would lead to unexpected application termination or arbitrary code execution by opening a maliciously crafted PDF file. The problem stemmed from a buffer underflow in the handling of fonts in PDF files. Apple patched the bug through additional bounds checking after learning of its existence from Will Dormann of CERT/CC. Power Management on OS X Mavericks 10.9.2 suffered from a vulnerability that prevented the screen from locking. Apple explains: “If a key was pressed or the trackpad touched just after the lid was closed, the system might have tried to wake up while going to sleep, which would have caused the screen to be unlocked. This issue was addressed by ignoring keypresses while going to sleep. This issue does not affect systems prior to OS X Mavericks.” Other flaws were found in areas like Heimdal Kerberos, ImageIO, Intel Graphics Driver, IOKit Kernel, Kernel, Ruby, Security – Secure Transport and WindowServer. There are separate versions of Security Update 2014-002 that customers can download (tailored specifically for their OS version). For instance, the Lion version only patches a handful of bugs. To read more click **HERE**

Iowa State University Servers Containing SSNs of 30,000 Students Hacked

SoftPedia, 23 Apr 2014: The Iowa State University’s IT staff has discovered unauthorized access to a total of five servers. The machines in question contained some sensitive information, but the university believes that the attackers were simply trying to use their computing power to mine Bitcoins. According to the university, the compromised servers stored the social security numbers of close to 30,000 students who had enrolled between 1995 and 2012. No financial information was exposed and there’s no evidence that the files containing the SSNs have been accessed. “We don’t

believe our students' personal information was a target in this incident, but it was exposed," stated Iowa State University Senior Vice President and Provost Jonathan Wickert. "We have notified law enforcement, and we are contacting and encouraging those whose Social Security numbers were on the compromised servers to monitor their financial reports," he added. In addition to those whose SSNs have been exposed, the university is also contacting close to 19,000 students whose university ID numbers were stored on the breached servers. This information can only be used on campus and it poses no financial risk. Those whose SSNs could have been compromised are being offered one year of free credit monitoring services through AllClear. The targeted servers are made by Synology, and they're popular among cybercriminals who use compromised computers to mine for Bitcoins. The breached machines have been destroyed. Other similar servers will be replaced in the upcoming period. In the meantime, software updates have been installed to keep hackers out. "Iowa State has always taken information security very seriously, and we will continue to take every possible action to safeguard the personal information of those who learn and work here," Wickert added. "We have well-regarded cyber defense experts here who not only protect university data, but educate others on how to prevent computer attacks. Unfortunately, Iowa State is not immune to hacking, but we are disappointed and sorry for the inconvenience this incident may cause." Meanwhile, the university warns students, faculty, staff and alumni about phishing attempts. The university, the ISU Foundation, and the ISU Alumni Association do request information from their members. However, none of these bodies ever asks for SSNs over phone or via email. Those who come across suspicious emails can check if they're legitimate by contacting the ISU Foundation, the ISU Alumni Association or the university's IT security team at "serverbreach [at] iastate.edu." To read more click **HERE**

Amazon and HP Cloud Services Vulnerable Due to Unpatched Windows Server Installations

SoftPedia, 23 Apr 2014: Security researchers from Bkav warn that many cloud customers are vulnerable to cyberattacks because their services are running unpatched versions of Windows Server. With auto update disabled, some of them haven't been patched in years. Experts started investigating cloud environments after one of their customers using Amazon EC2 noticed traces of malware on his server. Upon a closer investigation, researchers discovered that the service was running Windows Server 2003. Windows Server 2003 still receives security updates from Microsoft. The problem was that auto updates were turned off and the last patches were applied in October 2009, making the server highly vulnerable. To test their findings, experts exploited MS12-020, a critical remote desktop vulnerability that can be leveraged for remote code execution. The security hole was patched by Microsoft in the spring of 2012, but as the server wasn't updated since October 2009, the vulnerability could have been exploited. Microsoft's cloud services have auto update enabled, so the installations are more secure. However, there are other cloud providers, like HP and GoGrid, that also have auto update disabled, leaving customers vulnerable to cyberattacks. In the case of HP's Public Cloud, the last patches were applied in July 2013. Server installations from GoGrid were last updated in April 2012. MS12-020 is just one of the many vulnerabilities that can be exploited by cybercriminals. Over the past years, Microsoft has released tens or maybe hundreds of security bulletins for various versions of Windows Server operating systems. However, if the automatic update feature is disabled and customers neglect this aspect, they can end up handing all their valuable data over to cybercriminals. Experts believe that hackers could be scanning the cloud provider's IP ranges in search for vulnerable installations which they can easily breach. "Amazon, HP, GoGrid are among the biggest cloud IaaS providers in the world with big number of users and, sadly, big vulnerability in their service. Problem in updating security patches for their cloud servers might have contributed to the leaks of credit card information, trade secrets that occur frequently in recent years," explained Ngo Tuan Anh, Bkav VP of Internet Security. "It's time for attitude towards security for cloud servers to be changed. Cloud computing is different from conventional world in this, being connected to the Internet right after it is 'born', rather than being fully patched before saying hello to the world." To read more click **HERE**

Apple Patches Heartbleed Bug with AirPort Base Station Firmware Update 7.7.3

SoftPedia, 23 Apr 2014: Despite letting out a statement that said "key Web-based services were not affected" by the Heartbleed bug, Apple today offers a firmware update for AirPort base stations, incorporating a patch meant to specifically address the OpenSSL flaw. In a statement provided to Re/code earlier this month, a company spokesperson said, "Apple takes security very seriously. IOS and OS X never incorporated the vulnerable software and key Web-based services were not affected." Admittedly, AirPort is neither an OS, nor a web-based service (such as iCloud), but that doesn't mean it's not a key Apple service. The company has released AirPort Base Station Firmware Update 7.7.3 which is "recommended for all AirPort Extreme and AirPort Time Capsule base stations with 802.11ac." According to a brief support document, "It provides security improvements related to SSL/TLS. Other AirPort base stations do not require this firmware update." A more comprehensive advisory is then offered. The second document outlines that said firmware update patches a flaw where "an attacker in a privileged network position may obtain memory contents." The Mac maker doesn't specifically mention the Heartbleed flaw, but it does provide a detailed enough description which confirms that Firmware Update 7.7.3 indeed patches the infamous vulnerability that affected half of the Internet. "An out-of-bounds read issue existed in the OpenSSL library when handling TLS heartbeat extension packets. An attacker in a privileged network position could obtain information from process memory. This issue was addressed through additional bounds checking. Only AirPort Extreme and AirPort Time Capsule base stations with 802.11ac are affected, and only if they have Back to My Mac or Send Diagnostics enabled. Other AirPort base stations are not impacted by this issue." Apple credits Riku, Antti, and Matti of Codenomicon and Neel Mehta of Google Security as the people who discovered and reported the flaw. The Mac maker insists that firmware version 7.7.3 goes onto "AirPort Extreme or AirPort Time Capsule base stations with 802.11ac using AirPort Utility for Mac or iOS." Softpedia readers can download the utilities at the links supplied below. On OS X, customers are advised to employ AirPort Utility 6.3.1. On iOS, AirPort Utility 1.3.1 or later is to be used. Apple has also released standard security updates for OS X Lion, Mountain Lion, and Mavericks, as well as iOS 7.1.1 and Apple TV firmware 6.1.1 to address bugs. To read more click **HERE**

Two Alleged Members of Anonymous Cambodia Arrested

SoftPedia, 22 Apr 2014: A couple of 21-year-old students believed to be members of Anonymous Cambodia have been arrested. Local authorities collaborated with the FBI on the investigation. According to The Phnom Penh Post, the suspects are students at a private university, the SETEC Institute in Phnom Penh. They've been charged with computer hacking and they face up to two years in prison. Bun King Mongkolpanha, aka "Black Cyber" or "Machine," and Chu Songheng, aka "Zoro," were arrested on April 7. They're currently in prison awaiting trial. Authorities have been targeting them for eight months before obtaining a warrant for their arrest. "These are the first members of the Anonymous hacker group who have been arrested by the [Cambodian] police, and we found no [evidence] of any [planned] terrorist attack," said Major General Chhay Sinarith, director of the Ministry of Interior's internal security department. Sinarith said that both admitted taking part in hacking operations. However, a statement issued by the police says that Zoro has denied being involved in cyberattacks. Others are being investigated for their alleged connection to cyber operations against the Cambodian government. Interestingly, the official Anonymous Cambodia Twitter account hasn't mentioned anything about hackers being arrested. Instead, the hacktivists have already announced their plans to launch more attacks after a draft of the new cybersecurity law was leaked on April 9. Anonymous Cambodia has breached and disrupted numerous government and government-affiliated websites since September 2013. To read more click **HERE**

SMS Trojan FakeInst Targets Users in 66 Countries

SoftPedia, 23 Apr 2014: Security researchers from Kaspersky continue to analyze pieces of malware designed to target Android devices. One interesting threat is Trojan-SMS.AndroidOS.FakeInst.ef, an SMS Trojan that's designed to target users in 66 countries. The Trojan was first spotted in February 2013 and over a dozen new versions have been released since then. The first variants were only designed to send SMSs to premium rate numbers in Russia. However,

cybercriminals kept adding more and more countries to the list, until they reached 66. While most of the infections have been observed in Russia and Canada, countries like the US, Germany, Lithuania, France, Finland, Norway, Ukraine, the UK, Malaysia, Hungary, Switzerland, Indonesia, Spain, Israel, Portugal, Ireland, China, the Czech Republic, the Netherlands, New Zealand, and Brazil are also impacted. Cybercriminals distribute the Trojan by disguising it as an app that allegedly allows users to access adult videos. The configuration file contains a list of phone numbers and prefixes. Based on the victim's location, messages are sent from the infected devices to premium rate numbers. For each message, victims are charged around $2 (€1.5). In addition to sending SMSs, the malware is also capable of intercepting incoming text messages. Experts believe the threat has been developed by Russian-speaking cybercriminals. To read more click **HERE**

Microsoft to Release Large Windows Updates Twice a Year

SoftPedia, 23 Apr 2014: With Windows 8.1 Update rolled out this month and another major pack of improvements prepared for this fall, Microsoft has fully changed its Windows release cadence to embrace the rapid release approach that Steve Ballmer has talked about one year ago. Windows 8 was officially launched in October 2012 and approximately one year after that, Redmond officially introduced the new Windows 8.1, a new set of improvements that brought users the Start button and some other important changes. Fast forward to April 2014 and we get Windows 8.1 Update, another large pack of changes that makes the modern platform more mouse-friendly and marks another step towards a broader mix of the Modern UI and the traditional desktop. This fall, Microsoft is planning to launch a second Windows 8.1 update, followed by the debut of Windows 9 in early 2015. 'Why the rush?' you might ask. This rapid release cycle is part of Microsoft's new strategy of providing users with improvements and new features for their devices, be they PCs, tablets, or smartphones. The company previously introduced new Windows versions every three years, but it appears that the company is now planning to launch large Windows updates twice a year, followed by a major release every 24 months. Former Microsoft CEO Steve Ballmer said at the BUILD developer conference in 2013 that this new strategy is a key priority for the company, as it struggles to keep users up to date with the innovations coming out of Redmond. "And that's not even so much about the conference, but it's about the rapid pace of innovation. If there's not one other message that I reach you with in my opening remarks, it's about the transformation that we are going through as a company to move to an absolutely rapid release cycle -- rapid release, rapid release," Ballmer said. "I've talked externally about the transformation that we're going through as a company who's a software company to a company that is building software-powered devices and software-powered services. And the only way in which that transformation can possibly be driven is on a principle of rapid release." With the new CEO Satya Nadella at the helm of the company, Microsoft seems fully prepared to switch to this kind of strategy, but also to a more consumer-shaped business that would in the end tweak the Windows platform in such a way that it could better address feedback. To read more click **HERE**

FileMaker Pro 13 Updated with Heartbleed Fix

SoftPedia, 22 Apr 2014: Apple subsidiary FileMaker Inc. has released version 13.0.2.228 of its cross-platform database software to combat the Heartbleed OpenSSL flaw reported two weeks ago. A serious vulnerability that could expose user-sensitive data, including credit card information, the OpenSSL bug was deemed critical by numerous security researchers, which prompted many website administrators and software vendors to release updates and / or implement an updated version of the OpenSSL architecture to thwart potential outside attacks. FileMaker Inc. has done the same, albeit at a much slower-than-expected pace. FileMaker Pro 13.0.2.228 "Includes OpenSSL 1.0.1g, which is not vulnerable to the Heartbleed bug. In addition, the TLS heartbeat in OpenSSL is disabled, which removes the attack method used by the Heartbleed bug." The update theoretically includes all the changes implemented in version 13.0.2.228 (released on April 3), which adds a great deal of new functionality, fixes, and various tweaks. For example, Mac users in particular will notice that FileMaker has addressed an issue where data entry could appear slower when a large number of windows

were open. The system requirements remain unchanged, and Softpedia readers can grab the new updates at the links below, as usual. To read more click **HERE**

DEFT 8.1 Is a Forensic Distro Used by Law Enforcement to Catch Bad Guys

SoftPedia, 22 Apr 2014: DEFT, a Linux distribution based on Linux kernel 3.x and the DART (Digital Advanced Response Toolkit) with the best freeware Computer Forensic tools, is now at version 8.1. DEFT stands for Digital Evidence & Forensic Toolkit and is based on Lubuntu. It's a set of tools used by law enforcement agencies during computer forensic investigations. "Computer Forensics software must be able to ensure the integrity of file structures and metadata on the system being investigated in order to provide an accurate analysis. It also needs to reliably analyze the system being investigated without altering, deleting, overwriting or otherwise changing data," reads the official website. This means that it has to have a number of important features. DEFT does not use the swap partitions on the system being analyzed, during the system startup there are no automatic mount scripts, there are no automated systems for any activity during the analysis of evidence, and all the mass storage and network traffic acquisition tools do not alter the data being acquired. All these conditions must be fulfilled because the obtained data must be presented in a court of law and it must stand to rigorous testing. A number of aspects of this Linux distribution have been improved with the latest release. For example, the disk mount's status is now shows in the file manager, full support for Bitlocker encrypted disks has been implemented, Sleuthkit has been updated to version 4.1.3, Digital Forensics Framework has been upgraded to version 1.3, and full support for Android and iOS 7.1 logical acquisitions has been implemented. Also, the JD GUI has been added, Skype Extractor (a forensic software utility for reading and extracting information from the Skype Internet telephone software user data files) has been upgraded to version 0.1.8.8, Maltego 3.4 Tungsten has been implemented, a new version of the OSINT browser has been added, a bug in the /etc/apt/sources.list has been fixed, and full suite updates of the deft packages and DART 2 software and tools have been implemented. You can download DEFT Linux 8.1 right now from Softpedia (**link**). To read more click **HERE**

Russia Suspects Google of Violating the Law with Email Scanning Update to Terms of Service

SoftPedia, 22 Apr 2014: One Russian legislator is suspecting that Google's brand new changes to the Terms of Service are actually violating the country's law regarding personal data. As Softpedia reported last week, Google has now put it in writing that the company scans your emails in order to better target ads. The Internet giant doesn't exactly read the content of your emails, but it does pick up on key words so it can refine the ads you're being served, but also in order to weed out spam and malware. "Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored," reads Google's new Terms of Service. Lyudmila Bokova, Russian senator, has already addressed the search giant and the Russian consumer rights agency regarding this matter. Due to the wording of this specific paragraph in the Terms of Service, Bokova fears that the corporation won't just store and transfer user information, but it will also modify it by translating, distributing and publishing it. "I think that these terms of service are creating a potential for violating the Russian law, in particular the law on personal data. I want to get an answer on how the company itself appraises this threat," Bokova said. The State Duma Committee for Information Policy supports the move. Andrey Tumanov, a member of the committee, said that personal data can be used to harm users and the effect from using such information can be worse than a nuclear bomb. The American Internet giant is already facing some troubles over its scanning practices, which aren't exactly new. In fact, Google has been doing this for years, even though it never really hid what it was doing. The company is currently going to court over this exact issue as it is being accused of violating several laws, including the federal anti-wiretapping statuses. Google has managed to avoid a class action on this topic as non-Gmail users were also trying to get involved. Identifying those affected would have taken an unprecedented (and impossible) effort because Google would have to send an email notice to all non-Gmail addresses that have made it into the company's systems. Google is likely to face inquiries like the one in Russia in numerous countries. To read more click **HERE**