# The Cyber Shield

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

*10 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


*April 5, Chicago Tribune* – (Illinois) **Chicago-area doctors' group announces data breach.** Midwest Orthopaedics located in Rush University Medical Center in Chicago announced April 4 that surgical information for 1,256 patients may have been compromised in February when an individual accessed a doctor's Gmail account. All affected patients were notified and the doctor's group has since eliminated use of outside physician email accounts in their domain. Source: http://articles.chicagotribune.com/2014-04-05/news/chi-chicagoarea-doctors-group-announces-data-breach-20140404_1_midwest-orthopaedics-advocate-medical-group-data-breach

*April 9, Softpedia* – (International) **Companies advise users to change passwords due to possible Heartbleed attacks.** Several private companies and government organizations advised users to change their passwords in the wake of the Heartbleed vulnerability in OpenSSL that could expose usernames, passwords, and other secure communications. Security researchers also began posting analyses of the vulnerability as organizations worked to close the vulnerability on their systems. Source: http://news.softpedia.com/news/Companies-Advise-Users-to-Change-Passwords-Due-to-Possible-Heartbleed-Attacks-436704.shtml

*April 9, Softpedia* – (International) **Four vulnerabilities fixed with the release of Adobe Flash Player 13.0.0.182.** Adobe issued an update for its Flash Player, closing four security issues. Source: http://news.softpedia.com/news/Four-Vulnerabilities-Fixed-With-the-Release-of-Adobe-Flash-Player-13-0-0-182-436600.shtml

*April 9, Softpedia* – (International) **WordPress 3.8.2 addresses 2 vulnerabilities, includes 3 security hardening changes.** A new version of WordPress was released for download containing fixes for two security vulnerabilities and three changes that enhance security. Source: http://news.softpedia.com/news/WordPress-3-8-2-Addresses-2-Vulnerabilities-Includes-3-Security-Hardening-Changes-436613.shtml

*April 8, Threatpost*– (International) **Last call for XP, Office 2003 updates: April Patch Tuesday fixes 11 vulnerabilities.** Microsoft released its monthly Patch Tuesday round of updates April 8, including the final updates for Windows XP and Office 2003, with 4 bulletins closing 11 vulnerabilities. Source: http://threatpost.com/last-call-for-xp-office-2003-updates-april-patch-tuesday-fixes-11-vulnerabilities/105329

*April 8, IDG News Service* – (International) **Cybercriminals use sophisticated PowerShell-based malware.** Researchers at Symantec identified a new malicious PowerShell script that contains several ways to hide itself and can inject malicious code into rundll32.exe. The finding follows the discovery of another malicious PowerShell script by Trend Micro researchers known as CRIGENT or Power Worm during March. Source: http://www.networkworld.com/news/2014/040814-cybercriminals-use-sophisticated-powershell-based-280521.html

*April 8, Threatpost* – (International) **Google patches 31 flaws in Chrome.** Google released a new version of its Chrome browser, closing 31 vulnerabilities, 19 of which were rated as high priority. Source: http://threatpost.com/google-patches-31-flaws-in-chrome/105326

*April 8, Softpedia* – (International) **2013 threat report: 8 mega data breaches, 552 million identities exposed.** Symantec published its Internet Security Threat Report for 2013, showing a 62 percent increase in data breaches from organizations during the year, with 552 million identities exposed, among other findings. Source: http://news.softpedia.com/news/2013-Threat-Report-8-Mega-Data-Breaches-552-Million-Identities-Exposed-436508.shtml

*April 8, IDG News Service* – (International) **Yahoo email anti-spoofing policy breaks mailing lists.** Security researchers reported encountering an issue with mailing lists after Yahoo introduced a new Domain-based Message Authentication, Reporting, and Conformance (DMARC) policy to prevent email spoofing. Source: http://www.networkworld.com/news/2014/040914-yahoo-email-anti-spoofing-policy-breaks-280500.html

**Fake "Vital Newsletter" Emails Lead to Phishing Website**

SoftPedia, 9 Apr 2014: Phishers are trying to trick users into handing over their email account username and password with the aid of bogus newsletter emails. The malicious notifications spotted by Hoax Slayer carry the subject line "Vital Newsletter" and they read something like this: "Hello, I uploaded this vital newsletter using my google doc. For immediate access CLICK HERE. Sign in with your email." The link doesn't point to a legitimate email service, but to a phishing website where internauts are asked to enter their credentials. The cybercriminals are not targeting a certain type of email account. Instead, they allow victims to select between several services, including Yahoo, Gmail, Windows Live and AOL. The information entered on the phishing site is sent to a server controlled by the attackers. The cybercrooks can later use the information to hijack accounts and abuse them for other malicious operations. If users don't have two-factor authentication (2FA) enabled, their accounts can be easily compromised. On the other hand, most of those who fall for such a phish probably don't know much about security, so they most likely don't have 2FA enabled. A similar phishing scam was spotted last week by experts from Trusteer. It's clear that these types of schemes are still successful, which is why users are advised to be cautious when they come across suspicious emails. To read more click **HERE**

**Here's What You Need to Know About the 'Heartbleed' Bug That's Attacking Millions of Websites**

Tom's Guide, 8 Apr 2014: Millions of websites may have been leaking critically sensitive data for the past two years, thanks to a devastating flaw in the OpenSSL software many sites use to encrypt and transmit data. The Heartbleed bug, as it's called by the researchers who discovered it, would let anyone on the Internet get into a supposedly secure Web server running certain versions of OpenSSL and scoop up the site's encryption keys, user passwords and site content. Once an attacker has a website's encryption keys, anything is fair game: Instead of slipping through a proverbial crack in the wall, he can now walk in and out the front door. All websites that ever used the affected versions of OpenSSL should be considered compromised. Websites that are currently vulnerable to Heartbleed exploits include Yahoo, Comixology, Flickr, Imgur and OculusVR. Many other top sites — including Facebook, Google, Wikipedia, Amazon, Twitter, Apple and Microsoft — are not currently vulnerable, though some may have been in the past. Most secure websites encrypt traffic to and from their servers using a protocol called SSL/TLS. There are several different encryption "libraries" that can be used in this protocol, and one of the most widely used is an open-source library called OpenSSL. The Heartbleed bug is in versions of OpenSSL issued from December 2011 onward, not in SSL/TLS itself. Not every instance of SSL or TLS encryption across the Internet is compromised. But OpenSSL is the default encryption library in Apache and Nginx server software, which power two-thirds of all websites. An attack exploiting the Heartbleed bug would leave no trace in an

attacked Web server's logs. It's impossible to tell how many sites, if any, may have been exploited, and how many may have been vulnerable over the past two years. Neel Mehta of Google Security and a team of engineers at Oulu, Finland-based security company Codenomicon first discovered the Heartbleed bug, though they haven't specified when. They've created a FAQ page at heartbleed.com with full details. The bug's name refers to a handshake (process of connecting to a network) in OpenSSL's code called the "heartbeat extension," which sets a limit on how long an encrypted session stays valid. A coding error meant that the extension was missing a necessary verification (called a bounds check), thus giving an attacker access to additional information about the server and creating the vulnerability. The most recent version of OpenSSL, 1.0.1g, patches the flaw, so any websites running OpenSSL should upgrade to the newest version immediately. However, the damage has been done. Versions of OpenSSL with the bug have been in use for more than two years. If an attacker used the Heartbleed bug to get into a Web server, he would have access to the website's "crown jewels": its encryption keys. With the keys, attackers could decrypt traffic to and from the server; impersonate the server so that users who think they're visiting a given website are actually visiting a fraudulent site disguised as the correct one; or decrypt the server's databases, including their users' personal information, such as usernames, passwords, email addresses, payment information and more. Web servers that use or used vulnerable versions of OpenSSL need to do more than upgrade to the latest version of OpenSSL; they also need to revoke and reissue all of their encryption certificates. It's no use boarding up a hole in the wall if the intruders can now let themselves in through the front door. Administrators of websites using Apache or Nginx server software need to evaluate whether they have, or had used, vulnerable versions of OpenSSL. Such websites should be considered compromised. OpenSSL is also incorporated into email servers using the SMTP, POP and IMAP protocols; chat servers using the SMPP protocol; and most virtual private networks (VPNs) that use SSL to protect their networks. Want to check if an individual Web domain is affected? Cloud security company Qualys' SSL Labs hascreated a test. "Ironically, smaller and more progressive services, or those who have upgraded to the latest and best encryption, will be affected most," wrote the Codenomicon researchers in a thorough write-up on the Heartbleed bug. Many large consumer sites are not vulnerable to the Heartbleed bug, the researchers said, because those sites tend to be slow to adopt new security measures and have failed to upgrade to modern Web architecture. (They might, of course, be vulnerable to other kinds of attacks.) Unless you're a system administrator, there's not much you can do right now. We can't even recommend that you change your online passwords — not yet, at least. If a website hasn't upgraded its OpenSSL library and changed its encryption certificates, then a new password would be just as compromised as an old one. The vulnerable versions of OpenSSL are 1.0.0 through 1.0.1f. If you're a website administrator and can't upgrade to the newest version, then you can manually disable the heartbeat function and then recompile OpenSSL's code. To read more click **HERE**

**Heartbleed "Author" Denies Malicious Intentions, Says Bug Was a Programming Error**

SoftPedia, 10 Apr 2014: Everyone that has any type of interest in their security as they browse the Internet has heard about Heartbleed by now – the famous OpenSSL bug that has ruined Internet safety for the entire world. Robin Seggelmann, a German software developer, is the one who unknowingly allowed this to happen, making what's been dubbed as a rookie's mistake. In an interview for the Sydney Morning Herald, Seggelmann explains his mistake and how a moment of negligence ended up being such a serious issue. The developer says he did not insert the bug with the intent to do so. "I was working on improving OpenSSL and submitted numerous bug fixes and added new features. In one of the new features, unfortunately, I missed validating a variable containing a length," he explained. The error wasn't noticed by the reviewer either and so Heartbleed ended up in the released version of OpenSSL. Prior to this, Seggelmann was commonly fixing OpenSSL bugs and trying to contribute to the project. While he admits that it can be easy to believe that the bug was inserted maliciously, that wasn't the case. "It was a simple programming error in a new feature, which unfortunately occurred in a security relevant area," he said. The developer says that it is quite possible for intelligence agencies to have made use of the bug in the past two years, admitting that it's always better to assume the worst than best case scenario in security matters. That being said, he urged more people to keep an eye over the code going into open source software, especially with something like OpenSSL, mentioning that the more people look at

it, the better. The encryption bug, called Heartbleed, has caused quite a bit of trouble. The problem exposed large parts of the Internet that were supposed to be protected against anyone knowing where to look. The protocol is used by some two thirds of the world's websites, which means that there are a lot of unsafe sites out there that you need to be careful with, especially when inputting personal data, including passwords and bank account information. Not only was information exposed, but a server's private encryption keys were also up for grabs. These could then be used by criminals to decrypt data sent between a user of the website and the server. This is the most severe security issues to hit the Internet in a very long while. To read more click **HERE**

**Windows 8.1 Update Cannot Be Installed, Returns Error Code 80073712**

SoftPedia, 10 Apr 2014: As compared to Windows 8.1, the new Windows 8.1 Update is being delivered through Windows Update in order to avoid any potential downloading and installation issues, but it seems that plenty of users are actually stuck with some weird error codes that do not say anything about what went wrong. As we reported to you yesterday, a number of users are provided with error code 80070020 when trying to install Windows 8.1 Update, but today it has emerged that another message pops up when attempting to deploy the new OS version. This time, users are provided with a message saying, "Couldn't complete the updates. Undoing changes" and then with error code 80073712 which, again, doesn't provide any other specifics on how users can actually fix the issues. Here's what one of the affected users posted on Microsoft's Community forums today: "The installation of KB2919355 proceeds quickly to 74%, becomes dead slow until 89% complete, and finally aborts without any specific error message, just stating 'Couldn't complete the updates. Undoing Changes'." Many other users have already confirmed similar problems, so it's very unlikely for this to be just an isolated issue affecting a small number of computers. At this point, there are several workarounds available, but none actually seems to be solving the problems, even though a number of users claim they have managed to install Windows 8.1 Update after performing a system refresh or reset. Microsoft is yet to provide a fix for this problem. To read more click **HERE**

**Heartbleed Affects Canada's Tax-Filing System and TurboTax**

SoftPedia, 10 Apr 2014: It's not just regular websites that have been affected by the Heartbleed bug, but also important systems aiding governments around the world. Canada, for instance, has shut down its online tax-filing service because of the bug. The move comes at a particularly bad time since Canadians must file their tax returns in the next few weeks. According to Canada's Revenue Agency, the system has been halted and will remain inactive for a few days. On the bright side, however, it seems like Heartbleed has not actually done any real damage to the Canadian system, since the agency says that this is a "preventative" measure meant to safeguard the integrity of the information it holds. It's unclear whether they're trying to cover up a system breach or if this is indeed just something they are trying to do to make sure the system is secure all around. On the same line of work, Intuit TurboTax, a service that helps people prepare their taxes, has examined its systems and secured the product against the Heartbleed bug. "Safeguarding our customers' data is our top priority. We continuously monitor our systems to improve our security capabilities in service to our customers. Taxpayers can be confident that TurboTax websites are secure and their personal and financial information are safe. They can file their return today with confidence," said "Nat" Rajesh Natarajan, chief technology officer and vice president of product development and product management for Intuit TurboTax. To read more click **HERE**

**Yes, Heartbleed Is Serious Business, Even for Apple Users**

SoftPedia, 10 Apr 2014: Security researcher and public speaker Graham Cluley has taken it upon himself to raise awareness among Apple customers about the Heartbleed SSL flaw widely covered in the media these past two days. Apparently it's more serious than you'd like to believe. Writing on the Intego Mac Security Blog, Cluley warns that "The Heartbleed Bug is a serious vulnerability that could lead to malicious hackers spying on what were thought to be secure Internet communications." He explains that "A programming bug in the widely-used OpenSSL software library could

allow information to be stolen, which—under normal conditions—would be protected by SSL/TLS encryption." Information that could be stolen through this vulnerability includes (but is not limited to) email addresses, passwords, and private communications, "data which normally you expect to be transmitted down the equivalent of a 'secure line'," writes Cluley. According to the security expert, the Heartbleed flaw (also referred to as CVE-2014-0160 in security circles) has been around for roughly two years, and "people have been able to scoop up private information" for precisely that amount of time. "Yes, it is really bad," Cluley admits. But no one knows for sure if it happened, because "exploitation of the bug leaves no trace," according to the security consultant. "However, lots of people have demonstrated in the last couple of days that the bug can be exploited, and they've proven that it works," he adds. Apple customers asking whether or not they're exposed to any kinds of risks, either on OS X or iOS, are told that Heartbleed doesn't discriminate based on the platform you're using. It's basically an Internet flaw, so yes, any Mac or iPhone that you take to the web is vulnerable. "Unfortunately this bug doesn't care what kind of device you are using to communicate via the Internet. This means that iPhones, iPads and Macs are just as much at risk as, say, a computer running Windows 8.1." Except for Mavericks computers, though. There is a version of OpenSSL that shipped with OS X Mavericks 10.9 and is unaffected by the bug, according to multiple reports from security researchers. A new version of OpenSSL is available with a fix and you can test whether or not a web site is impacted by Heartbleed. Apple's own web sites are secure, Cluley says. Visit the related links below to learn more about the emergence of the flaw and the response from the IT community. To read more click **HERE**

**Man Who Got Raided After Hacking University of Maryland Does Reddit AMA**

SoftPedia, 10 Apr 2014: David Helkowski, a software engineer who got raided by the FBI and the Secret Service after hacking into the systems of the University of Maryland, has decided to share his story on Reddit. The expert had found a vulnerability in the University of Maryland's systems while working for Canton Group, a software company contracted by the university. He reported the vulnerability, which could have allegedly been leveraged to gain access to a lot of sensitive information. However, after his reports were ignored, he decided to take matter into his own hands. He exploited the vulnerability from his home computer and downloaded a small number of information records, which he anonymously posted on Pastebin on March 15. He used a VPN to protect his identity, yet, shortly after, he returned home from dinner to find his house being raided by FBI and Secret Service agents. Since he claims he didn't mean to cause any harm, and since his wife witnessed the entire raid, Helkowski decided to fully cooperate with authorities in their investigation. He even handed over the password for his system encryption and his Keepass password. The man says no charges have been brought against him so far, but he no longer works for the Canton Group. Although he tried to cover his tracks when he hacked into the university's systems, he did share his plans with some people, including on a Steam chat, which might explain how law enforcement tracked him down so fast. The FBI appeared to have a printout of the Steam chat log, which Helkowski believes was obtained directly from Steam or from someone in the chatroom. His friends and even his parents were questioned by authorities before the raid. Helkowski says he might also be a suspect in the recent data breach in which the details of hundreds of thousands of individuals have been stolen. He claims to have gained more access than the cybercriminals who stole data from the organization, but he says he didn't do "anything bad with that information or access." However, in a statement they published regarding the man's case last month, University of Maryland representatives said the two breaches were unrelated. "The FBI has informed the University that the intrusion resulted in no public release of any information and no damage to the institution, except for the release of personal data of one senior University official, who has been notified. We are unable to comment further on the intrusion at this time. This matter is unrelated to the data breach of February 18, 2014," said Interim Vice President and Chief Information Officer Ann G. Wylie. To read more click **HERE**