# The Cyber Shield

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

*20 May 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




**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



*May 15, Threatpost* – (International) **Five year old security vulnerability patched in Linux kernel.** A patch was issued for a serious vulnerability in the Linux kernel that could allow attackers to cause denial of service issues or obtain administrator privileges. The vulnerability has reportedly been present for 5 years, and a proof-of-concept exploit was made available. Source: http://threatpost.com/five-year-old-security-vulnerability-patched-in-linux-kernel/106104

*May 16, IDG News Service* – (International) **'Elderwood' hackers continue to set pace for zero-day exploits.** Symantec released research into the Elderwood hacking platform showing that the attackers using it may be more numerous and diverse than previously thought, with several groups or subgroups using that platform to attack defense, IT, supply chain, and human rights organizations. The Elderwood platform is linked to several cyberespionage campaigns including the Operation Aurora and Icefog attacks, among others. Source: http://www.networkworld.com/news/2014/051614-39elderwood39-hackers-continue-to-set-281662.html

*May 15, CNET News* – (International) **Adobe restores Creative Cloud login service after day-long outage.** Adobe restored service to users of its Creative Cloud service May 15 after a 24-hour outage that left users unable to use some aspects of the service and unable to use the service if not already logged in. Source: http://www.cnet.com/news/adobe-restores-creative-cloud-login-service-after-day-long-outage/

**Email Malware Masquerades as 'Important' Update**

Tom's Guide, 19 May 2014: Email Malware Masquerades as 'Important' Update.Are you a Windows user who recently received an email about an "important company update" for your computer? Whatever you do, don't install that update; it's really a Trojan that, once installed, appears to sneakily download more malware onto your computer. These malicious emails use forged headers to pretend to originate from whatever email domain your own address is from. So if your company's email address is "jdoe@acmecorp.com," the email message will seen to come from "administrator@acmecorp.com." Attached to the emails is a ".gadget" file, a type of program that runs in the Windows sidebar. Once the gadget is installed, a program within it called "main.exe" connects to the Internet and downloads another file with an ".enc" ending. It's not clear what this file is, but Jonathan French of Gulf Breeze, Fla.-based email and Web security firm AppRiver, who discovered the malware this morning (May 16), observed that this process is similar to the way the prolific Gameover malware, a variant on the eternally adaptable Zeus banking Trojan, often infects computers. French said on the AppRiver blog that the company has already blocked more than 70,000 of these infected emails. According to the malware tracking website VirusTotal, the antivirus program MalwareBytes was the first to be able to flag the ".gadget" file as malicious. To read more click **HERE**

**Linux Kernel 2.6.32.62 LTS Released After One-Year Hiatus**

SoftPedia, 20 May 2014: The latest version of the stable Linux kernel, 2.6.32.62, is out, marking yet another release in this particular branch of the software, which is also the oldest one still in existence. The latest build of this kernel features quite a few patches and fixes, covering numerous aspects. The interesting thing about it is that the latest update for this branch was released almost a year ago, which makes this the oldest kernel still updated. Linux kernel maintainer Willy Tarreau announced a few days ago that he was pulling patches for this old version and numerous developers agreed. "This is the start of the long-term review cycle for the 2.6.32.62 release. All patches will be posted as a response to this one. If anyone has any issue with these being applied, please let me know," Willy Tarreau said in the email announcement. Keep in mind that this is an LTS release, which means that it's going to be around for a very long time. If you feel adventurous, you can ditch the LTS branch and go for the latest 3.14 version or even the latest 3.15 RC. A complete list of commits in this branch of the kernel can be found in the official announcement. You can download Linux kernel 2.6.32.62 right now from Softpedia. To read more click **HERE**

**Half of security pros fail to secure data**

Heise Security, 20 May 2014: Research conducted at Infosecurity Europe 2014 (**link**) has revealed that 50% of security professionals do not secure data on portable storage devices such as USBs and external hard drives. This finding comes despite 91% of respondents to the same survey expressing concerns about the potential damage that data loss could bring to their organizations. These statistics have been revealed following a survey of over 500 security professionals conducted by iStorage. Despite half of respondents admitting to not encrypting data, the survey revealed that 67% were aware that a maximum fine of £500,000 could be imposed on businesses and Government bodies for serious breaches of the Data Protection Act. Under this Act, a breach constitutes failing to keep data secure against unlawful or unauthorized processing, accidental loss or erasure. The other 33% of respondents were aware of fines but believed them to be far less, with the majority understanding the maximum fine to be £250,000. According to a recent national data survey, the third-biggest source of data breaches in the country is people losing USB keys, laptops, and external hard drives. Further research states the average cost of a data security breach for companies in the UK ranges from £160,000 to £4.8 million. Along with the issue of financial costs that comes with data loss, reputational damage is also a big factor as it can have serious implications. "In today's fast-moving business environment and the era of big data, it is deeply concerning that 50% of security professionals do not encrypt data while on the move," states John Michael, CEO and Founder of iStorage. "Data loss can have a sizeable negative impact on business productivity, reputation and future revenue. To ensure critical business data remains confidential, it is imperative that businesses take the necessary precautions to guarantee data does not end up in the wrong hands." To read more click **HERE**

**Fitness apps are a "privacy nightmare", shedding personal data to the highest bidder Sophos**

Naked Security, 20 May 2014: The Washington Post quotes Deborah Peel, the executive director of Patient Privacy Rights, has called the growing fitness data marketplace a "privacy nightmare", given that the vast majority, if not all, of the health data these apps collect has "effectively zero" protection. Take, for example, Facebook's recently acquired fitness and activity tracking app, Moves. Moves describes itself as an "activity diary" for iPhone and Android mobile devices. It does things like count how many steps you take every day, and then presents it in a slick interface on your mobile phone. It gets that information by mixing data from mobile phones' motion sensors with GPS information to track a user's location and activity throughout the day. Moves's algorithms can differentiate between different types of exercise, such as biking or running, and can calculate distances traveled and calories burned. That means the app knows not only a user's location, pinpointed down to an exact building, but also whether he or she got there on foot, bike or bus. The data-rich landscape being created by the proliferation of this type of fitness app has tech heavyweights drooling. Apple, for one, has been on a hiring spree in the biomedical field, Reuters recently found when rifling through LinkedIn profile changes, with much of the hiring being centered on sensor technology that could feed into its development of the iWatch and other wearable technology. Google, for its part, has been working not just on wearable

tech such as Glass, but also on other medical products, such as contact lenses for diabetics that read tears to ascertain glucose levels, the Post reports. Google pre-briefed Lorenzo Hall, chief technologist at the Center for Democracy & Technology, before its January announcement about the contact lenses. Google assured Hall that data collected by the contacts would be kept out of the wealth of personal data collected by the company through its other services, Hall told the Post. So who's keeping an eye on the sensitive data collected by fitness apps? Unfortunately, we can expect little oversight by traditional medical watchdogs. The data isn't protected by the Food and Drug Administration, given that fitness apps or gizmos don't generally qualify as medical devices. Nor does it merit the privacy protection of the US's Health Insurance Portability and Accountability Act (HIPAA), which covers privacy with regards to information handled by medical professionals. As the Post reports, fitness apps seem to be falling through an FDA loophole: A list of examples of types of apps that fall into this category on the FDA Web site appears to encompass features commonly found in fitness tracking apps, but a footnote includes a potential loophole -- saying that when these type of apps "are not marketed, promoted or intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, or do not otherwise meet the definition of medical device, FDA does not regulate them." The FDA for now is pretty much steering clear of regulating health-related apps unless they pose a clear and present medical danger to consumers. The Federal Trade Commission, for its part, hosted a public conference about consumer-generated health data earlier this month as it tries to figure out where it fits into this new regulatory scene. But the FTC has limited means to punish companies if they break their promises to consumers, lacking the power to issue fines over first offenses. That leaves it up to consumers to watch their own backs when it comes to reading the privacy policies for these apps. To read more click **HERE**