# Cyber-Threat Newsletter – 21 Mar 16



*Patches & Updates of the Week:*

**(U) Adobe releases emergency Flash Player patch**
(U) Adobe Systems released new versions of Flash Player in order to fix 18 critical vulnerabilities that could be exploited to take over computers, including one flaw that's already targeted by attackers. "Adobe is aware of a report that an exploit for CVE-2016-1010 is being used in limited, targeted attacks," the company said in a security advisory. The flaw stems from a heap overflow condition and was reported to Adobe by researchers from antivirus firm Kaspersky Lab. Adobe advises users to upgrade their Flash Player installations to version 21.0.0.182 for Windows or Mac and version 11.2.202.577 for Linux. The extended support release of Flash Player has also been updated to version 18.0.0.133. The Flash Player plug-ins bundled with Google Chrome, Internet Explorer, and Microsoft Edge will automatically be updated through those browsers' update mechanisms. Adobe has also released version 21.0.0.176 of AIR Desktop Runtime, AIR SDK, AIR SDK & Compiler and AIR for Android, which contain Flash Player components. (IDG News Service 10Mar16)

*Threats & Vulnerabilities of the Week:*

**(U) Cyber criminals snap up expired domains to serve malicious ads**
(U) Expired domain names are becoming the latest route for cyber criminals to find their way into the computers of unsuspecting users. Cyber criminals launched a malicious advertising campaign this week targeting visitors of popular news and entertainment websites after gaining ownership of an expired web domain of an advertising company. Users visiting the websites of the New York Times, Newsweek, BBC and AOL, among others, may have installed malware on their computers if they clicked on the malicious ads. Bresntsmedia.com, the website used by hackers to serve up malware, expired on 1 January and was registered again on 6 March by a different buyer, security researchers at Trustwave SpiderLabs wrote in a blog. Buying the domain of a small but legitimate ad company provided the criminals with high quality traffic from popular web sites that publish their ads directly, or as affiliates of other ad networks, the researchers said. New York Times spokesman Jordan Cohen said the company was investigating if the attack had any impact. "To be clear, this is impacting ads from third parties that are beyond our control." Newsweek, BBC and AOL could not be immediately reached for comment. (Reuters, 16Mar16)

**(U) Malvertising campaign hits MSN, NYT, BBC, AOL, and NFL websites**
(U) A large malvertising campaign has been detected by three major cyber-security vendors, affecting multiple websites that have a total monthly viewership that goes well over 2.4 billion users. According to Trend Micro, Trustwave, and Malwarebytes, crooks have managed to show malicious ads using four different advertising networks. These ads have hijacked the user's browsing experiences and led them to malicious sites hosting the Angler EK (exploit kit). In some of these cases, security researchers from Trustwave have reported that they've seen Angler distribute the TeslaCrypt ransomware instead of the Bedep malware, but the overwhelming majority of infections has been with Bedep. The four advertising platforms through which the malicious ads were delivered are Google, AOL, Rubicon, and AppNexus. Some of the biggest sites on which the malicious ads have been displayed include Microsoft's MSN portal, the New York Times, the BBC, AOL, Comcast's Xfinity, NFL, Realtor, the Weather Network, The Hill, and Newsweek. Security researchers from Malwarebytes also noted that in the past few weeks, malvertising, in general, was seen in far smaller numbers than before, but this changed during the past day, when this massive campaign was first spotted. The same company also released an interesting report regarding the most recent tactics used in malvertising campaigns. (Softpedia, 16Mar16)

**(U) Mac and Windows users threatened by rampant domain 'typosquatting'**
(U) Mac and Windows users could end up in some bad Internet neighborhoods by not typing the "c" in ".com" websites. As reported by Threatpost, Security vendor Endgame recently discovered widespread "typosquatting" with the ".om" domain name, in which bad actors attempt to dupe people who mistype common URLs. In this case, more than 300 malicious URLs have latched onto the Country Code Top-Level Domain for Oman, which users might accidentally enter instead of .com". Some examples include samsung.om, delta.om, and netflix.om. The danger is particularly acute for Mac users, who according to Endgame might be bombarded with pop-ups to update a new version of Adobe Flash Player. While tech-savvy users may recognize this type of attack -- or know to stop using Flash Player entirely -- users who are follow through on the update prompts may be unknowingly installing adware on their machines. This adware, called Genieo, will then attempt to inject targeted advertising into the user's web browser. That's not to say Windows users aren't at risk. Visiting one of the affected sites with a Windows machine may redirect users to various scareware, adware, or survey sites, several of which try to coerce users into installing harmful or unnecessary programs. Typosquatting is not a new phenomenon, and brands generally do a good job of protecting users against obvious misspellings. The abuse of .om appears to be an anomaly, in which hundreds of popular sites now have bad actors sitting on not-so-unlikely typos. With any luck, the exposure will prompt those sites to take action, but users should be extra careful with their URL spellings in the meantime. (Macworld, 15Mar16)

**(U) Chinese hackers behind US ransomware attacks**

(U) Hackers using tactics and tools previously associated with Chinese government-supported computer network intrusions have joined the booming cyber crime industry of ransomware, four security firms that investigated attacks on US companies said. Ransomware, which involves encrypting a target's computer files and then demanding payment to unlock them, has generally been considered the domain of run-of-the-mill cyber criminals. But executives of the security firms have seen a level of sophistication in at least a half dozen cases over the last three months akin to those used in state-sponsored attacks, including techniques to gain entry and move around the networks, as well as the software used to manage intrusions. "It is obviously a group of skilled of operators that have some amount of experience conducting intrusions," said Phil Burdette, who heads an incident response team at Dell SecureWorks. Burdette said his team was called in on three cases in as many months where hackers spread ransomware after exploiting known vulnerabilities in application servers. From there, the hackers tricked more than 100 computers in each of the companies into installing the malicious programs. The victims included a transportation company and a technology firm that had 30 percent of its machines captured. Security firms Attack Research, InGuardians and G-C Partners, said they had separately investigated three other similar ransomware attacks since December. Although they cannot be positive, the companies concluded that all were the work of a known advanced threat group from China, Attack Research Chief Executive Val Smith told Reuters. Asked about the allegations, China's Foreign Ministry said on Tuesday that if they were made with a "serious attitude" and reliable proof, China would treat the matter seriously. But ministry spokesman Lu Kang said China did not have time to respond to what he called "rumors and speculation" about the country's online activities. The security companies investigating the advanced ransomware intrusions have various theories about what is behind them, but they do not have proof and they have not come to any firm conclusions. Smith said some government hackers or contractors could be out of work or with reduced work and looking to supplement their income via ransomware. It is also possible, Burdette said, that companies which had been penetrated for trade secrets or other reasons in the past were now being abandoned as China backs away, and that spies or their associates were taking as much as they could on the way out. Dell said that some of the malicious software had been associated by other security firms with a group dubbed Codoso, which has a record of years of attacks of interest to the Chinese government, including those on US defense companies and sites that draw Chinese minorities. (Reuters, 15Mar16)

**(U) Documents with malicious macros deliver fileless malware to financial-transaction systems**

(U) Spammed Word documents with malicious macros have become a popular method of infecting computers over the past few months. Attackers are now taking it one step further by using such documents to deliver fileless malware that gets loaded directly in the computer's memory. Security researchers from Palo Alto Networks analyzed a recent attack campaign that pushed spam emails with malicious Word documents to business email addresses from the US, Canada and Europe. The emails contained the recipients' names as well as specific information about the companies they worked for, which is not typical of widespread spam campaigns. This attention to detail lent more credibility to spam messages and made it more likely that victims would open the attached documents, the researchers said. The documents contained macros that, if allowed to run, execute a hidden instance of powershell.exe with special command-line arguments. Only systems that match what the attackers are looking for are flagged and reported back to a command-and-control server. For those systems, the script downloads a malicious encrypted DLL (dynamic link library) file and load it into memory. "Due to the target-specific details contained within the spam emails and the use of memory-resident malware, this particular campaign should be treated as a high threat," the Palo Alto researchers said in a blog post. A similar combination of PowerShell and fileless malware was observed last week by researchers from the SANS Institute's Internet Storm Center. That malware creates a registry key that launches a hidden PowerShell instance at every system start-up. The PowerShell command executes an encoded script that's stored in a separate registry key. Its goal is to decrypt and load an executable file directly into memory without ever writing it to disk. "By using PowerShell the attackers have been able to put malware that might otherwise be detected on a hard drive into the Windows Registry," senior SANS instructor Mark Baggett, said in a blog post. Storing malicious code in the system registry, abusing the Windows PowerShell and adding malicious macros to documents are not new techniques. However, their combination can make for very potent and hard-to-detect attacks. (IDG News Service, 14Mar16)

**(U) Vulnerability in torrent portal software exposes user private information**

(U) An anonymous security researcher is sounding the alarm on a security flaw in popular torrent portal software that can be leveraged to expose details about a site's users. In terms of piracy and torrent-related news, the TorrentFreak blog is the place you'd want to check out on a daily basis. Taking advantage of the blog's huge following, a security researcher who did not want to disclose his name contacted the site and revealed details about an exploit he had recently discovered. The problem lies in a software package used by torrent site administrators to set up their portals. The researcher declined to name the software package since the flaw was not yet patched. This software comes with support for BBcode (Bulletin Board Code), a system that replaces certain text patterns with text, images, or other types of dynamic information. According to the researcher, there's a flaw in one of the built-in BBcodes packed with that particular software package. The BBCode is [you], which, when used, prints the user's name. The researcher discovered that, by nesting the [you] BBcode inside an image URL, he could log details about a site's users. The researcher explained that an attacker, or a law enforcement agency, could register on torrent portals, open forum threads or send a private message to the users it wants to target. When the user accesses the thread or private message, the BBcode is automatically executed, loading the image, and recording the user's IP address on the attacker's server without the user even noticing there was an image on the page. Users who don't use VPN or proxies to access torrent sites can be logged via this technique and later identified in logs, tying their real IP address to piracy-related activities. As of now, the researcher told TorrentFreak that one of the affected sites is SceneAccess, a private torrent portal. (Softpedia, 14Mar16)

**(U) Two-year-old Java flaw re-emerges due to broken patch**

(U) A patch for a critical Java flaw released by Oracle in 2013 is ineffective and can be easily bypassed, security researchers warn. This makes the vulnerability exploitable again, paving the way for attacks against PCs and servers running the latest versions of Java. The flaw, tracked as CVE-2013-5838 in the Common Vulnerabilities and Exposures (CVE) database, was rated by Oracle 9.3 out of 10 using the Common Vulnerability Scoring System (CVSS). It can be exploited remotely, without authentication, to completely compromise a system's confidentiality, integrity and availability. According to researchers from Polish security firm Security Explorations who originally reported the flaw to Oracle, attackers can exploit it to escape from the Java security sandbox. On Thursday, Security Explorations revealed that the Oracle patch for the vulnerability is broken. The fix can be trivially bypassed by making a four-character change to the proof-of-concept exploit code released in 2013, Security Explorations CEO Adam Gowdiak wrote in a message sent to the Full Disclosure security mailing list. Gowdiak's company published a new technical report that explains how the bypass works in more detail. The company's researchers claim that their new exploit was successfully tested on the latest available versions of Java: Java SE 7 Update 97, Java SE 8 Update 74 and Java SE 9 Early Access Build 108. In order to exploit the vulnerability on an up-to-date Java installation, attackers would need to find a separate flaw that allows them to bypass the security prompts or to convince users to approve the execution of their malicious applet. The latter route is more likely. Security Explorations has not notified Oracle about the CVE-2013-5838 bypass before disclosing it. According to Gowdiak the company's new policy is to inform the public immediately when broken fixes are found for vulnerabilities that the company has already reported to vendors. "We do not tolerate broken fixes any more," he said. It's not clear whether Oracle will push out an emergency Java update just to patch this vulnerability, or if it will wait until the next quarterly Critical Patch Update, which is scheduled for 19 April. (IDG News Service, 11Mar16)

**~~(U//FOUO)~~ New Mac malware from HackingTeam suggests firm still viable**

~~(U//FOUO)~~ As of 29 February, researchers had discovered what appears to be newly developed Mac malware from Italian firm HackingTeam (HT), according to an online press report. The malware was uploaded on 4 February to the Google-owned Virus Total scanning service, indicating it had avoided detection by major antivirus (AV) programs, and as of 29 February, only 10 of 56 AV services had detected it. The sample installs a copy of HT's signature Remote Control System (RCS) platform and mostly relies on old, unexceptional source code. It is unclear how the malware is installed. A Mac security expert at a US IT firm examined the malware and assessed that while the sample appears to install a new version of the old HT implant, it uses several advanced tricks to evade detection and analysis. For example, it uses Apple's native encryption scheme to protect the binary file's contents, possibly making it the first malicious implant installer to do so, according to the expert. (arstechnica.com, 29Feb16)

***Incidents of Interest:***

**(U) An inventory of what was taken in the Staminus data breach**

(U) An analysis of the leaked files reveals the true extent of the devastating Staminus data breach that took place last week after an unknown hacker had managed to access the company's network, shut down some of its infrastructure, and then steal most of its data, dumping it online. The data breach took place between 10 March and 11, and because the hacker hosted the data via Tor servers, which have a notoriously slow download speed, it took some time before security experts managed to download all 30 GBs of the leaked information so they could examine it in depth. An analysis of all the Staminus data was carried out by researchers from Risk Based Security (RBS), a cyber-intelligence firm from Richmond, Virginia, USA. According to their investigation, the hackers managed to get their hands on quite a lot of information, also validating the hacker's initial claim that credit card details were stored in cleartext. Analysts are saying that the leaked data contained the personal information of 4,415 of the company's customers. This included full addresses, contact details, company details, emails, and encrypted passwords. For 2,042 of these customers, the Staminus database also contained full credit card details. Additionally, RBS researchers also uncovered 141,403 entries of account billing details from various types of purchases Staminus clients made since the company started its activity. Outside financial details, researchers also found the source code of most of the company's applications and a full configuration file for the company's OpenVPN client. Among other information included in the leaked documents are details about Staminus sales, site configuration, billing tracking, DDoS reporting, and full ticket history. The ticket history included more data as well, such as user details, ticket content, and the Staminus responses. Researchers also discovered data relating to Staminus' servers configuration, along with information on its staff members, such as encrypted passwords, email addresses, and OAuth credentials in the form of tokens and generated user keys. RBS also came across certificates used by Staminus for some of its services, along with site configurations for various internal or public-facing services. All of this was possible because, as the hacker claimed, Staminus used the same root password for most of its servers. (Softpedia, 15Mar16)

OGA

**(U) Hackers botched $1 billion bank heist because of a misspelled word**

(U) Hackers that breached Bangladesh's central bank account at the US Federal Reserve Bank of New York have botched a bank heist which would have pocketed them nearly $1 billion. What was known was that a group of unknown hackers had accessed an account at a US bank belonging to the country of Bangladesh, which its central bank was using for international payments, said to contain over $20 billion. The hackers initiated a series of transactions, which were at some point detected and stopped, but not before the intruders managed to move a large amount of money to the Philippines. Ever since the heist came to light, more details have been uncovered by Reuters journalists, which have now found out that the attack actually took place on the night between 4 February and 5, 2016. The hackers logged into Bangladesh's account at the US Federal Reserve Bank of New York and initiated three dozen bank transfers to different banks across the world. The first four transactions went through to bank accounts belonging to several casinos in the Philippines and totaled $81 million. Problems appeared at the fifth operation, which was sent to the bank account of an NGO in Sri Lanka. Reporters are saying, quoting US bank officials, that the hackers misspelled the name of the NGO writing "Shalika Fandation" instead of "Shalika Foundation." Because the money had to move through a series of intermediary banks before it could reach Sri Lanka, the misspelled name triggered alarm bells at German bank Deutsche Bank, but not before forwarding the money to Sri Lankan bank Pan Asia Banking Corp. By the time Deutsche Bank realized there is no Shalika Fandation registered in Sri Lanka, the money was already in the country. Fortunately, Pan Asia was also investigating, because it was unusual for them to receive such a large sum of money. About the same time, US Federal Reserve officials were also noticing a big queue of large transfers from Bangladesh's account and also contacted the country's central bank officials. At this point, Federal Reserve employees intervened and stopped the transfers, realizing what was happening. US bank officials are saying that they've managed to stop transactions worth of over $870 million, which would have easily meant this was the biggest cyber-heist in history. All of this seems to be a case of where the hackers used spear-phishing and social engineering tactics to get hold of some Bangladesh central bank employee's login credentials. Currently, the Bangladesh central bank is busy recovering its funds with the help of Filipino authorities. (Softpedia, 11Mar16)

*Items of Interest*

**(U) Denmark's intelligence agency creates 'hacker academy'**

(U) Denmark's military intelligence agency says it's creating "a hacker academy" to train IT specialists who, if they graduate, will be offered employment. In a statement, the secretive Danish Defiance Intelligence Service (DDIS) says the small group who will be enrolled are "already are among the best in their field." DDIS said Wednesday the academy "will not teach them how to hack" but will "target their mindset and skills so that they can be used" by the agency which spies outside Denmark's border. (AP, 16Mar16)

**(U) Opera becomes first big browser maker with built-in ad-blocker**

(U) Norwegian company Opera is introducing a new version of its desktop computer browser that promises to load web pages faster by incorporating ad-blocking, a move that makes reining in advertising a basic feature instead of an afterthought. Faster loading, increased privacy and security and a desire for fewer distractions are behind the growing demand for ad-blockers. However, their popularity is cutting into the growth of online marketing for site publishers and corporate brands, which rely on reaching web and mobile users to pay for their content rather than restricting access to paid subscribers. Opera has a history of introducing innovations that later become common in major browsers such as tabbed browsing and pop-up blocking, which helped users control an earlier generation of in-your-face ads and malware disguised as advertising. Opera said it can cut page-loading times by as much as 90 percent by eliminating the complex dance that occurs behind the scenes in a user's browser as various third-party ad networks deliver promotional messages to users. Opera sees no contradiction in the fact that it relies on advertising for a big chunk of its own revenue but is introducing ad-blocking control features in its products. Because it is building the features directly into its browser, page delivery times are 40 percent faster than existing ad-blocker plug-ins, or browser extensions. Top plug-in providers include AdBlock, AdMuncher and Ghostery that run on top of existing browsers. A study published by PageFair and Adobe estimated online ad revenue lost to blockers in 2015 would amount to $21.8 billion and those losses could almost double to $41.4 billion in 2016. Ad-placement firm Carat forecasts global digital and mobile advertising will near $150 billion this year. (Reuters, 10Mar16)

---

(b)(3) 10 USC ⊥ 424

Note: This is not original product but is consolidated from various sources.

(b)(3) 10 USC ⊥ 424