[redacted] Cyber-Threat Newsletter – 22 Feb 16

(b)(3) 10 USC 424

Patches & Updates of the Week:

(U) Mozilla fixes critical vulnerabilities in Firefox browser and Extended Support Release
Mozilla yesterday issued two security advisories announcing key updates to its Firefox browser and the Firefox Extended Support Release (ESR), both of which fixed vulnerabilities that the open-source developer labeled as critical. The latest iteration of the Firefox browser, version 44.0.2, has addressed a critical vulnerability surrounding the ability of service workers to intercept responses to plug-in network requests. Plug-ins responsible for making security decisions were susceptible to forged, malicious responses that would allow websites to override same-origin policies -- an important security measure that forbids web pages from accessing sensitive data on other web pages unless they share the same origin. Meanwhile, version 38.6.1 of the Firefox ESR has patched a vulnerability associated with a malicious Graphite 2 smart font capable of triggering an arbitrary code execution. According to Mozilla, the malicious font "could circumvent the validation of internal instruction parameters in the Graphite 2 library using special CNTXT_ITEM instructions," potentially resulting in code execution. Mozilla addressed issue by integrating more updated version of Graphite 2 into its ESR. (scmagazine.com, 12Feb16)

(U) New Windows flaws allow the removal of 2FA
Following in the wake of Patch Tuesday, three additional flaws with Microsoft products have been revealed, two of which could remove the two-factor authentication (2FA) protocol from any Windows products. The vulnerabilities were found in Microsoft ASP.NET and Microsoft Visual Studio. In both cases a remote user could conduct a cross-site request forgery attacks that would allow the removal of 2FA. Essentially the attacker uploads malware to the victim though a web page or malicious URL which removes the phone number associated with the 2FA with that account making it inoperative. Password authentication is not affected. The third flaw impacts Windows 2008 R2 and 2012 R2. A vulnerability was found in Windows Network Policy Server allowing a remote user to block Radius authentication on the targeted system. This is done by sending specially crafted username strings to the target network policy server to prevent Remote Authentication Dial-In User Service. Microsoft has issued patches for all three vulnerabilities. (scmagazine.com, 12Feb16)

Threats & Vulnerabilities of the Week:

(U) JavaScript analytics code can be used to compromise US banks
Hungarian security expert Gabor Szathmari has analyzed the login pages of 21 major US banks and found that 9 load third-party JavasCript assets, exposing users to unnecessary dangers. Theoretically, bank login pages should be the safest places on the Internet. In practice, they are far from being so, and there are multiple reasons this happens. As Mr. Szathmari has discovered in his research, some US banks fail to protect this page and unwittingly load JavaScript resources from third-party sites. But loading JavaScript files is not a problem, since websites need JavaScript files to work properly these days. The danger relies in the fact that some of these files are stored on another company's server. If that company gets compromised, attackers could very well alter these third-party scripts and deliver malicious code, which is executed right on the bank's login page. Thanks to many new HTML5 APIs, malicious JavaScript code now allows you to log keystrokes, steal data entered in forms, take screengrabs, steal browser cookies, and even communicate with Flash to exploit many of its security loopholes. A simple analytics script can break down a bank's complex security policy. No matter how many multi-million dollar deals banks sign with cyber-security vendors, by continuing to allow third-party analytics code to load on login pages, or even the user's banking dashboard, banks are leaving a backdoor wide open to attacks, thanks to their analytics provider. As Mr. Szathmari explains, the solution is quite simple. Removing analytics code from these pages is the quickest way to neutralize the threat. Additionally, implementing Subresource Integrity (SRI) is also another way to allow these scripts to load but remain safe in case the third-party service gets compromised. (Softpedia, 17Feb16)

(U) Poseidon cybergang infects victims, then blackmails them
A cyberespionage group is infecting firms with malware and then blackmailing the firm into giving them an IT contract, according to a researcher at Kaspersky Lab. The gang known as "Poseidon" infects its victims using spearphishing emails that deliver "state-of-the-art custom malware" to ensure easy and silent entry and efficient data acquisition, in line with their patrons' requirements, researcher Oleg Gorobets said in a post. Once the gang has harvested valuable information from its victim, it uses a front-end security company to blackmail its targets into contracting with the gang to remove the infection, he said. Afterwards, the gang would either retain an illegitimate presence within the "secured" system or quietly remain in the firm's network after supposedly removing the malware. Poseidon's malware is focused on Windows-based systems and is capable of embedding itself in a firm's system for years without being detected, the researcher said. (scmagazine.com, 17Feb16)

(U) Several bugs detected in IBM Java Runtime
Multiple vulnerabilities that could enable a remote attacker to launch a denial-of-service attack have been detected in the IBM Runtime Environment Java Technology Edition v6, according to an IBM Security Bulletin posted on Tuesday. The integrated software is used by Tivoli Composite Application Manager for SOA, a platform which provides management for services, applications and middleware. These bugs, which include the vulnerability popularly known as "SLOTH," were reported by IBM when it updated Java SDK in January 2016. "The TLS protocol could allow weaker than expected security caused by a collision attack when using the MD5 hash function for signing a ServerKeyExchange message during a TLS handshake," the bulletin stated. Employing man-in-the-middle techniques, a saboteur could exploit this flaw to mimic a TLS server and glean credentials, IBM wrote. No workarounds or mitigations have yet been provided. (scmagazine.com, 17Feb16)

(U) Major bug exposes thousands of Linux apps and IoT devices to hacks
Google's security team and Red Hat have found a flaw in a widespread computer code library that leaves hundreds of thousands of devices vulnerable to malware when performing domain-name lookups. The bug was found in the GNU C Library, colloquially known as glibc, which offers developers a collection of open source code to act as the foundation of an app and can be found in many uses of Linux. A buffer overflow bug, which causes programs to try to read and write more data than their allocated memory allows, was located in the getaddrinfo () function of glibc, which performs searches for IP addresses using domain name servers (DNS). Google's security team explained that when the getaddrinfo () function tries to communicate with a web domain or server controlled by a malicious party, or if the query is intercepted by a hacker, it is possible for malicious code to be inserted into vulnerable devices or cause them to crash. Versions of glibc above 2.9 are vulnerable to the bug. The bug has since been patched by the maintainers of glibc. But given that it was introduced in 2008 and has avoided detection until now, the number of machines and devices that may have been infected by malware making use of the bug could be vast. This is further compounded by the fact that Linux is used as the foundation operating system for many smart and Internet of Things (IoT) devices, notably routers. These devices are not updated as often as laptops, PCs and smartphones, so the vulnerability may difficult to wipe out. The bug serves as a warning that, while open source tools offer an affordable and flexible way to build apps and embed functional operating systems into devices, they are also reliant on the community that maintains them. Google explained that the bug was identified several years ago but appeared not to have been patched. "To our surprise, we learned that the glibc maintainers had previously been alerted of the issue via their bug tracker in July 2015," the security team said. It also highlights security concerns around the IoT and the increase of internet-connected devices. (v3.co.uk, 17Feb16)

(U) Russian cyberspy group uses simple yet effective Linux Trojan
A cyberespionage group of Russian origin known as Pawn Storm is infecting Linux systems with a simple but effective Trojan program that doesn't require highly privileged access. Pawn Storm, also known as APT28, Sofacy or Sednit, is a group of attackers that has been active since at least 2007. Over the years, the group has targeted governmental, security and military organizations from NATO member countries, as well as defense contractors and media organizations, Ukrainian political activists and Kremlin critics. The group is known for using zero-day exploits -- exploits for previously unknown vulnerabilities -- as well as other infection techniques like spear-phishing emails with malicious attachments. Its primary tool is a Windows backdoor program called Sednit, but the group also uses malware programs for Mac OS X, Linux and even mobile operating systems. Its preferred malware tool for Linux is a Trojan program called Fysbis, according to researchers from security firm Palo Alto Networks. It has a modular architecture allowing attackers to expand its functionality as needed through plug-ins that get pushed down to individual victims. As a cyberespionage tool, Fysbis is primarily designed for data theft. As such, even if it doesn't gain control over the whole system, it can still achieve its primary goal of stealing potentially sensitive documents that the user has access to, or spying on the user's Web browsing and other activities. Fysbis shows that Advanced Persistent Threat (APT) actors often don't require advanced methods to reach their objectives, the Palo Alto researchers said. "Despite the lingering belief (and false sense of security) that Linux inherently yields higher degrees of protection from malicious actors, Linux malware and vulnerabilities do exist and are in use by advanced adversaries," they said. (IDG News Service, 15Feb16)

(U) Netflix-themed phishing, malware supply black market with stolen credentials
As the Netflix movie streaming service spreads all over the world, the number of users rises, as well as the number of those who wish to use it but don't want to pay for it or want to pay less than the set price. With such a wide (and widening) pool of potential targets, it's no wonder that some cyber crooks are opting to concentrate on them. Unsurprisingly, legitimate Netflix users are targeted with phishing emails impersonating the service, using one pretext or another to lure them to a fake Netflix site where they are directed to update their account, i.e. to enter their login credentials, personal info and credit card details. "Netflix subscriptions allow between one and four users on the same account. This means that an attacker could piggyback on a user's subscription without their knowledge," Symantec researcher Lionel Payet explains. Stolen Netflix login credentials are often sold on the black market, to users who wish to access Netflix for free or a reduced price. "These accounts either provide a month of viewing or give full access to the premium service." Payet explains. "In most advertisements for these services, the seller asks the buyer not to change any information on the accounts, such as the password, as it may render them unusable. This is because a password change would alert the user who had their account stolen of the compromise." A similar approach is taken by cyber criminals offering Netflix account generators. The software provides stolen login credentials to users or login credentials of accounts that have been created by using stolen payment card details. That list is often updated, as some accounts are shut down either because the legitimate users stopped using them or because the compromise was detected. Finally, potential users can be and sometimes are tricked into downloading malicious files posing as Netflix software. In Brazil, for example, users have been tricked into downloading a banking Trojan masquerading as Netflix software, after clicking on fake ads offering free or cheaper access to the streaming service. (net-security.org, 12Feb16)

(U) Critical bug found in Cisco ASA products, attackers are scanning for affected devices
Several Cisco Adaptive Security Appliance (ASA) products -- appliances, firewalls, switches, routers, and security modules -- have been found sporting a flaw that can ultimately lead to remote code execution by attackers. The vulnerability (CVE-2016-1287) is critical, as it can be exploited by an unauthenticated, remote attacker by sending crafted UDP packets to the affected system. Cisco ASA Software is affected if the system is configured to terminate Internet Key Exchange (IKE) v1 or IKE v2 VPN connections, and not if the system is configured to terminate Clientless SSL and AnyConnect SSL VPN connections. A full list of affected products can be found in this security advisory, and includes Cisco ASA 5500-X Series Next-Generation Firewalls and Cisco ISA 3000 Industrial Security Appliances. "The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory," the company pointed out. SANS ISC CTO Johannes Ullrich says that the exploit would likely arrive over UDP port 500 or possibly 4500, and that they are seeing a large increase in port 500/UDP traffic. Luckily, Cisco has released patched firmware for affected devices, and admins are advised to patch them as soon as possible, as there are no workarounds available. "To determine whether the Cisco ASA is configured to terminate IKEv1 or IKEv2 VPN connections, a crypto map must be configured for at least one interface. Administrators should use the show running-config crypto map | include interface command and verify that it returns output," the company helpfully explained. For more technical details about the flaw and its possible exploitation, check out this blog post by the three Exodus Intelligence researchers who unearthed it. (net-security.org, 11Feb16)

Incidents of Interest:

[redacted]

OGA

(U) Hackers hold Hollywood hospital's computer network hostage for $5M
A hospital in Southern California is currently without access to email, digital patient records, and some internet-connected medical devices following a cyberattack that saw hackers take its computer networks clear offline -- before demanding more than $5 million US in ransom. NBC LA reports that an "internal emergency" was declared at the Hollywood Presbyterian Medical Center in Los Angeles after staff began experiencing "significant IT issues" around 5 February. Hospital CEO and president Allen Stefanek confirmed the attack on Friday as both The Los Angeles Police Department and The FBI launched investigations into the case, noting that "the shutdown has not affected patient care." It has, however, resulted in emergency room delays, 911 patients being diverted to other hospitals, and the need for all registrations and medical records to be written by hand on paper. Patients themselves are being told they must pick up medical test results in person as opposed to having them delivered electronically, according to BBC News. While Stefanek described the attack as random, he didn't expand on the type of malware being used, how the hospital's system became infected, or how much money was being demanded for access to be restored. Computer forensics expert Eric Robi, whose clients include both the State of California and the US federal government, told FOX 11 Los Angeles that hackers have asked Hollywood Presbyterian Medical Center for approximately 9,000 bitcoin (just over $5 million) in relation to a ransomware attack. Several employees at the hospital echoed this while speaking to NBC4, reportedly saying that "hackers would send back the key codes to restore the system" in exchange for a bitcoin ransom. After working on half a dozen similar attacks against LA businesses over the past year, Robi said that "most of the time it's cheaper to pay the ransom than to pay to fix the problem" -- though he did note that this particular ransom was higher than any he'd seen before. What's happening to Hollywood Presbyterian Medical Center may be part of a larger trend predicted for this year by Forrester Research, in which ransomware is being used to target the medical sector. (CBC News, 16Feb16)

(U) Kaspersky researcher hacked a hospital while sitting in his car
Sergey Lozhkin, a security researcher for Kaspersky, gave a talk at the Security Analyst Summit (SAS 2016) held these days in Tenerife, Spain, where he presented a case study during which he hacked a local hospital. Lozhkin's experiment started when he accidentally discovered unprotected medical equipment available online through Shodan. Digging deeper into the results, he found that a few of the exposed devices were actually from a local nearby hospital. The researcher contacted a friend working at that hospital and brought the issue to the institution management's attention. He explained the problem to the people in charge and eventually agreed to carry out a security audit to test if he could hack into their network. Since IoT equipment is known to have lots of security issues, Lozhkin was sure he'd eventually get in. During his initial hacking attempts, he discovered that he couldn't access any equipment from a remote connection, which means that basic and properly configured firewalls are more than enough to keep low-skilled hackers away. Lozhkin did manage to crack into the hospital's network, but only after he drove near the actual building, close enough to reach its WiFi network from his laptop. From there, he managed to hack and steal the local network key, which then allowed him to access various medical equipment that was connected to the building's internal WiFi network. Using the network key, he accessed a tomographic scanner, from where he extracted patient records. The records were dummy data since management knew he was supposed to carry out a test, but the experiment proved its point and showed hospital management that their network was woefully insecure. (Softpedia, 12Feb16)

(U) 'Crackas with Attitude' suspect arrested in UK
A teen believed to be the mastermind behind the cybergang "Crackas with Attitude," a group that hacked US officials, including CIA Director John Brennan, was arrested Tuesday in the UK. The unnamed teen is suspected of most recently leaking the personal information of more than 20,000 FBI employees and 9,000 Department of Homeland Security (DHS) employees. He also stands accused of an embarrassing series of cyberattacks against Brennan, FBI Deputy Director Mark Giuliano and other US government officials. Authorities in the US were shocked that a teenaged "computer nerd" had covered his tracks so well, according to CNN, and it is unclear what charges he will face domestically. In the U.K., the teen will be charged with several counts of suspicion of conspiracy to commit unauthorized access to computer material, The South East Regional Organised Crime Unit told The Daily Dot. (scmagazine.com, 12Feb16)

(U//~~FOUO~~) ISIL's Cyber Caliphate Army hacks Indian travel, media entities, US firm
(U//~~FOUO~~) On 10 February, the ISIL-affiliated Caliphate Cyber Army (CCA) hacktivist group—as part of its "#AbuHussainRevenge" campaign—claimed responsibility for compromising several websites, including Indian airline booking company Fly Mantra, India-based news service Maharashtra, and a US industrial gas distributor, according to a CrowdStrike report. The CCA posted screenshots via its social media channels to prove its compromise of Fly Mantra, published Fly Mantra customer account information—including usernames, passwords, and phone numbers—and claimed to have disrupted scheduled flights. However, the attacks probably were not very sophisticated, according to CrowdStrike, and the screenshots suggest the CCA only gained access to Fly Mantra's administrative portal and altered customer reservations. The CCA said it was targeting Indian entities in response to recent Indian news reports claiming ISIL was recruiting Indian hackers and had offered $10,000 for Indian Government data. The CCA announced the "#AbuHussainRevenge" campaign in January to avenge ISIL hacker Junaid Hussain, who was killed in a drone strike in August 2015, according to the report. (intel.crowdstrike.com, 11Feb16)

Items of Interest

(U) US Department of Defense will put Windows 10 on 4 million computers
The US Department of Defense is going to standardize 4 million computers on Windows 10, a significant endorsement for Microsoft's latest operating system. It marks the largest announced deployment of Windows 10 in an enterprise setting to date. The goal is to have all of the DoD's computers that are currently running older versions of Windows upgraded to Microsoft's new OS within a year. That's an incredibly fast timeline for an organization of the Defense Department's size, especially since Windows 10 hasn't yet been on the market for a year. It's a move to streamline the department's IT infrastructure, which is increasingly important as a key means of protecting from digital attacks. Wednesday's news is also a sign of the government's confidence in Windows 10, and will be a signal to other organizations about where the enterprise PC market is going. It's unclear yet how much the migration will cost the Defense Department, which spends around $44 billion every year on IT and cybersecurity. In addition to the deployment news, Microsoft's Surface line of products has been certified to meet the Defense Department's security and interoperability requirements. That means it's easier for the tablets to be worked into government deployment plans for new technology, and could mean more business for Microsoft, especially as the DoD upgrades to Windows 10. Those 4 million DoD devices will help Microsoft reach its goal of getting 1 billion devices worldwide running Windows 10 by late summer of 2018. (IDG News Service, 17Feb16)

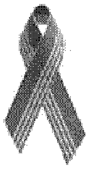
(U) DHS rethinks privacy in cyber analytics
DHS wants to track cyber threats in real time across network environments using machine algorithms that can detect strange traffic patterns associated with malicious reconnaissance, compromised accounts or data exfiltration. It also wants to insure the capabilities adhere to privacy rules. Algorithmic analytics track the behavior of network traffic. 'That differentiates the technique from signature-based programs like Einstein. And, according to DHS, it could improve detection rates and speeds, as well as boost responses to hostile network activity in federal agency and protected networks. The program was detailed in an 8 February public meeting of the DHS Privacy Office as the agency sought to insure protection of personally identifiable information as analytic tracking technology moves forward at the agency. During the meeting, committee members stressed the data collected by algorithmic analytics was only a "piece of a piece" of netflow traffic -- just the portion that showed anomalous behavior, and not all traffic going in and out. They also noted that the technology did not track the behavior of people using a network, but rather traffic behavior patterns. The DHS Privacy and Integrity Advisory Committee adopted privacy recommendations that include limiting personnel who work with the data generated, developing control for accessing both the logs and underlying data, notifying users of the technology's use, and making the criteria for what is being collected transparent. (fcw.com, 12Feb16)

(U) Obama to sign bill combating counterfeit chips
US President Barak Obama indicated Thursday (11 February) that he will sign into law a customs bill passed by the US Senate that includes a provision to combat counterfeit semiconductors. The bill, known as the Trade Facilitation and Trade Enforcement Act of 2015 (H.R. 644/S.1269), mandates that US Customs and Border Protection share information and samples of suspected counterfeit parts for rapid identification of counterfeits. The bill, which passed the US House of Representatives last year, had been bogged down in the Senate in a fight over the extension of a ban on Internet taxes included in the legislation. But it passed Thursday by a 75-20 vote. The circulation of counterfeit semiconductors has drawn increased attention in recent years, with organizations such as the Semiconductor Industry Association (SIA) lobbying for policies and legislation designed to improve identification of fake parts and crack down on those responsible for their circulation. In 2011, the SIA estimated that counterfeiting costs US-based semiconductor companies more than $7.5 billion per year. In addition to the SIA, other trade groups, including the US Chamber of Commerce and the National Association of Manufacturers, also supported the legislation. (EE Times, 12Feb16)

[redacted]

(b)(3) 10 USC ⊥ 424

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



[redacted]

(b)(3) 10 USC ⊥ 424