[redacted] Cyber-Threat Newsletter – 29 Feb 16 (b)(3) 10 USC § 424

Patches & Updates of the Week:

(U) Google fixes Chrome critical flaw, researcher snags $25K
An anonymous researcher picked up a $25,633 bug bounty for discovering a critical vulnerability in Chrome (CVE-2016-1629), which Google has now patched in version 48.0.2564. While Google won't release details of the bug until the majority of users have had time to update, the company noted that it was a "same-origin bypass in Blink and Sandbox escape in Chrome." Google said it "will also retain restrictions if the bug exists in a third-party library that other projects similarly depend on, but haven't yet fixed." Earlier this year, with the release of Chrome 48.0.2564.82 Google promoted Chrome 48 into the stable channel for Linux, Mac and Windows. (scmagazine.com, 19Feb16)

Threats & Vulnerabilities of the Week:

(U) MouseJack vulnerability in RF-based dongles can result in computer takeovers
Researchers have uncovered a wide-ranging vulnerability in the way non-Bluetooth dongle devices interact with wireless mice and keypads, which could enable a nearby hacker to take over a victim's computer using radio frequency signals. According to a white paper from Internet of Things security company Bastille, hackers looking to exploit this flaw, dubbed MouseJack, need only their own inexpensive dongle, a few lines of malicious code, and to be within a 100-meter range of the machine they intend to compromise. The vulnerability can be exploited by ostensibly tricking the targeted computer's dongle into thinking it is receiving transmissions from its corresponding wireless device, when it's actually receiving packets from the hacker's dongle. "It's a new class of attack that affects potentially billions of devices, said Chris Rouland, founder and CTO of Bastille, in an interview with SCMagazine.com. Bastille uncovered the flaw using software-defined radio, a technology that sniffs out vulnerabilities in RF airwaves, an attack surface that "has been largely unexplored," Rouland added. An attack of this nature can happen so fast that even if the victim realizes someone has accessed their machine, it's probably too late. The implications are grave, as hackers could leverage this flaw to steal credentials and sensitive data, or infect a machine with malware that can quickly spread across a connected enterprise. "They can even bypass an air-gapped network by turning a PC into a WiFi hotspot," said Rouland. Bastille discovered the vulnerability in products manufactured by all seven of the wireless vendors it tested -- AmazonBasics, Dell, Gigabyte, HP, Lenovo, Logitech and Microsoft. MouseJack actually consists of a series of related vulnerabilities. All involve finding a way to circumvent the encryption process that is supposed to occur when authorized users press keys on their computer keyboards. This encryption normally prevents an attacker from spoofing the keyboard and then typing in malicious codes and commands. Unfortunately, Bastille found several exploitable workarounds. For starters, some dongles don't require wireless keyboards to transmit packets using encryption. In those instances, the hacker can easily spoof the keyboard and then inject unencrypted keystrokes and commands. If the dongle does require encryption protocols when communicating with a keyboard, attackers can instead focus on the wireless mouse, because mouse click packets are unencrypted. Moreover, dongles often do not have a mechanism to verify if a packet it receives matches the type of device that transmitted it. This means hackers can use a malicious dongle to spoof the wireless mouse, but trick the computer into thinking its receiving keyboard commands -- again allowing the attacker to execute code. Users with only a wireless mouse but no wireless keyboard installed are not necessarily safe either, because in some instances attackers can force the victim's dongle to pair with their own wireless keyboards. If the victim's dongle doesn't require keyboards to use encryption, then the computer is susceptible to attack. (scmagazine.com, 23Feb16)

(U) Linux Mint operating system maliciously hacked
The Linux Mint operating system software download has been hacked on the community-driven distribution's own website. The Linux Mint ISO 'disk image' data contents were maliciously altered, meaning than anyone downloading and installing the software over the weekend of 20/21 February 2016 will find that their machine has been compromised. The Linux Mint operating system, a 'variant' based upon Debian and Ubuntu (two other popular Linux OS distributions), has enjoyed popularity as a result of its combination of packaged software, focus on desktop functionality and appealing graphical user interface (GUI). In what can be regarded as something of a setback for fans of free and open source software (FOSS) distributions, the only compromised version was Linux Mint 17.3 Cinnamon edition. The team points out that users who downloaded another release or another edition are not affected. Users who downloaded Linux Mint via torrents or via a direct HTTP link are also not affected. The Linux Mint blog is currently visible and details the specific technical reasons behind the attack. However, the Linux Mint website itself is offline at the time of writing. The process for checking whether an ISO file installation has a valid MD5 signature is detailed at the aforementioned blog link. As Tim Anderson explains, "The infected ISOs installed the operating system complete with the IRC (Internet Relay Chat) backdoor Tsunami, giving miscreants access to infected systems via IRC servers." Creator of Linux Mint, Clem Lefebvre, has said that the hack is connected to Sofia, Bulgaria and his team has pinpointed the names of three possible perpetrators. It later transpired that this might simply be the location of the file server used to store the hack's details. This is not the only element in the Linux Mint hack story. Lefebvre has also confirmed that hackers have stolen a complete copy of the site's forum login details. Members' passwords, addresses, birthdates and profile pictures are all thought to have been copied. If the Linux Mint team remains clueless then they should perhaps talk to ZDNet's Zack Whittaker who claims to have already had an encrypted chat with the hacker responsible, who goes by the name 'Peace'. Peace told Whittaker on Sunday that a "few hundred" Linux Mint installs were under his control and that this is 'a significant portion' of the thousand-plus downloads during the day. According to ZDNet's Whittaker, "Peace declined to give their name, age, or gender, but did say they lived in Europe and had no affiliations to hacking groups. The hacker, known to work alone, has previously offered private exploit services for known vulnerabilities services on private marketplace sites he is associated with." Peace was apparently 'just poking around' on the Linux Mint site when he or she found the vulnerability granting unauthorised access. At the time of writing SCMagazineUK.com has not been able to confirm when the Linux Mint project will be fully functional again. (scmagazine.com, 22Feb16)

(U) IRS warns of a 400 percent rise in tax-related phishing emails

The US Internal Revenue Service (IRS) has issued a public advisory, warning US citizens of an avalanche of tax-related malicious emails that are looking to harvest personal user information through phishing campaigns or to spread malware via malicious attachments. According to the IRS, the situation is quite bad and only in the month of January 2015, the agency received 1,026 reports of tax-related malicious emails, a 400 percent increase compared to last year when the IRS received only 254 reports of the same type. Barely reaching the middle of the tax season, the trend set in January continued in the first 16 days of February, IRS officials saying they've received 363 reports, compared to the 201 recorded in the entire month of February 2015. In total, until the middle of February 2016, the IRS says it received 1,389 complaints of tax-themed phishing and malware reports, a number that's unbelievably high for US officials. The number is so large that it already surpassed 2014's total of 1,361 incidents, and is almost halfway through 2015's total of 2,748. If complaints continue to come at the same rate, the IRS would be collecting more than 11,100 tax-related phishing and malware reports by the end of 2016. (Softpedia, 19Feb16)

(U) Locky ransomware grows rapidly in prominence, infamy, warn researchers

As industry research continues to pour in on Locky -- the newly emerging ransomware responsible for locking out Hollywood Presbyterian Medical Center, it is becoming clear that the malicious code is propagating rapidly in the US and across the globe. Locky's accelerated distribution was noted in recent advisories from leading security firms Heimdal Security and Palo Alto Networks. The latter, in a 16 February blog post, said it "observed approximately 446,000 sessions for this threat, over half of which targeted the United States (54 percent)." But Locky's global reach is expanding as well, as evidenced by today's Heimdal blog post, which analyzes an email spam campaign designed to trick German-language targets into downloading the ransomware. In this instance, the spoofed emails appear to come from MPSMobile, a mobile device accessory wholesaler. MPSMobile's homepage today features a prominent security advisory warning customers not to fall for the email-based scam. The spam emails spread Locky via malicious Word attachments as well as via macros that, upon activation, connects a victim's PC to a malicious web page. Researchers have also noted a distinct link between Locky and the known banking malware Dridex, believing them to be the handiwork of the same bad actors. (scmagazine.com, 18Feb16)

OGA

Incidents of Interest:

(U) Sensitive child profiles, private messages exposed online

Security researcher Chris Vickery has discovered another database containing sensitive user data exposed online (i.e. accessible via Internet). Leveraging Shodan, he unearthed a database compiled and used by US-based uKnowKids, a company that helps parents monitor what their kids do online and on the mobile phone. "In violation of the Children's Online Privacy Protection Act (COPPA), uKnowKids.com gave public access to over 6.8 million private text messages, nearly 2 million images (many depicting children), and more than 1,700 detailed child profiles. This includes first and last names, email addresses, dates of birth, gps coordinates, social media access credentials, and more," Vickery noted in a blog post, adding that the "databases was configured for public access, requiring no level of authentication or password and providing no protection at all for this data." Vickery notified the company about this problem mere minutes after he accessed the database, and according to uKnowKids CEO Steve Woda, the company's "technology team patched the database vulnerability within 90 minutes of discovery." But even though Woda initially thanked Vickery for the heads-up, he's obviously not satisfied with the fact that Vickery accessed the database, took screenshots, and downloaded it -- all without permission. "The vulnerable database included proprietary intellectual property including customer data, business data, trade secrets, and proprietary algorithms developed to power some of uKnow's most important technology," says Woda. He confirmed that names, communications, and URL data for about 0.5 percent of the kids that uKnowKids has helped protect were exposed, but that no financial information or unencrypted password credentials were vulnerable. After patching the flaw that let Vickery in, the company analyzed its systems for other flaws and to check who else might have obtained unauthorized access to their systems. Among several other security measures implemented in the wake of the breach, the company has also hired two third-party security firms to try to breach their systems "on an ongoing and continuous fashion," so they can identify any future vulnerabilities as quickly as possible and prevent future breaches. "The lesson to learn here is that, if you're a parent, be wary of services that offer to monitor your child's online behavior. These services collect unnerving amounts of data on your child and, when a breach occurs, all of that data can be exposed to untold numbers of people". (helpnetsecurity.com, 23Feb16)

OGA

(U) US school agrees to pay $8,500 to get rid of ransomware

Administrators of the Horry County school district (South Carolina, US) have agreed to make a $8,500 / €7,600 payment to get rid of a ransomware infection that has affected the school's servers. The ransomware took root during the past week, on Monday, 8 February, and affected 25 servers that stored information for Horry County elementary schools, WBTW reports. Immediately after school employees noticed problems accessing their data, its IT personnel took down all servers to prevent the ransomware from spreading to more computers. Shutting down the servers affected the school's online services. School officials discovered that the ransomware asked 0.8 Bitcoin per computer, for a total of 20 Bitcoin. The school's IT staff said the ransomware penetrated their network through an older server running outdated equipment. Local South Carolina law enforcement and the FBI were brought in to investigate, but as in many similar cases, they could do little to help. After spending countless hours trying to find a way around the ransomware's encryption, and failing, the school's administration has approved Monday, 15 February, a payment that would cover the ransom demand. About the same time this was happening on the East Coast, a similar, more high-profile incident was in full swing on the West Coast. On the same day, 15 February, the Hollywood Presbyterian Medical Center in Los Angeles approved a $17,000 payment to free its IT network of a ransomware infection that almost shut its operations in the previous week. (Softpedia, 19Feb16)

OGA

(U) Hospital pays $17,000 ransom to get access back to its encrypted files

A Los Angeles hospital has paid $17,000 to cyberattackers who crippled its network by encrypting its files, a payment that will likely rekindle a fierce debate over how to deal with a problem known as ransomware. Hollywood Presbyterian Medical Center issued a statement saying that its systems were restored on Monday, 10 days after malware locked access to its systems. The hospital contacted law enforcement as well as computer experts, wrote Allen Stefanek, president and CEO of Hollywood Presbyterian, in a statement on Wednesday. But it is apparent those efforts did not help in recovering files. "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," Stefanek wrote. "In the best interest of restoring normal operations, we did this." The cyberattackers requested 40 bitcoins, or about $17,000, not 9,000 bitcoins, worth about $3.4 million, as reported in the media, Stefanek wrote. Paying the attackers likely encourages the schemes. Hollywood Presbyterian may face criticism for paying, but it appears the hospital had little choice. Companies have paid ransoms to cyberattackers before and come under fire. Last November, ProtonMail, a Switzerland-based encrypted email service, paid a ransom to a group that was crippling its network with distributed denial-of-service attacks. ProtonMail wrote a blog post saying it paid a ransom in bitcoins, but the DDoS attack didn't stop. A second group began attacking the company. Later, ProtonMail said it regretted paying and that it "was clearly a wrong decision so let us be clear to all future attackers -- ProtonMail will never pay another ransom". (IDG News Service, 17Feb16)

Items of Interest

OGA

(U) DHS releases guidelines for CISA-sanctioned cybersecurity information sharing

The US Department of Homeland Security has published guidelines on how the private sector and federal entities can share cyber threat indicators (CTIs) with the US federal government. The Department has also provided interim policies and procedures for how federal entities can receive and use CTIs, how privacy and civil liberties can receive, store, use and disseminate them, and how federal agencies can share information in the government's possession. These guides are to make sure that the entities that want to take advantage of the Cybersecurity Information Sharing Act (CISA), signed into law last December, can do so in a simple and standardized manner, and that those who receive the information know exactly how to use it and disseminate it. Among other things, CISA allows companies to share information (CTIs, defensive measures) about cyber attacks they suffered with government agencies, without having to worry about getting sued by users for breach of privacy. The sharing will be executed through the Department's Automated Indicator Sharing (AIS) initiative, and will result in the its National Cybersecurity and Communications Integration Center (NCCIC) receiving CTIs from the various entities, anonymizing them, and disseminating them to some or all of the above mentioned federal, non-federal and private sector entities. Those who, for whatever reason, don't want to join the AIS, can still share CTIs and defensive measures via email or web form. (helpnetsecurity.com, 19Feb16)

(U) Dark web honeypot shows how quickly leaked passwords attract hackers

A simple experiment carried out by cloud security provider Bitglass has shown how quickly a compromised account that had its password leaked can attract hackers. Bitglass' experiment revolved around a fake identity created for a fictitious bank employee. Researchers created a fake banking portal, a dummy Google Drive account, and added boobytrapped files that were monitored through the Bitglass service. Once researchers created the fake service, they leaked it on the Dark Web as phished credentials for a Google Drive account. Within a day after posting the data online, Bitglass detected three logins on the Google Drive account, and another five on the fake banking portal. After two days, hackers had already downloaded files, and within a month, Bitglass recorded more than 1,400 login attempts from 30 different countries, with many hackers returning many times over the course of multiple days. The hackers also tried to use the leaked credentials for the victim's other accounts, showing exactly why password reuse is such a dangerous habit to have. The experiment, dubbed Project Cumulus, also showed that once inside the Google Drive account, some attackers didn't stay idle, and attempted to download sensitive files. Bitglass says that 12 percent of the hackers that managed to log in attempted to download files, and some even managed to open encrypted documents. This was the second time that Bitglass carried out this study, after doing the same thing back in April 2015. The company looked over the last experiment's data once again and was surprised to find out that after hackers avoided downloading and accessing data from the first experiment in the beginning, eight months later, over 200 people accessed those particular booby-trapped files. The Bitglass 'Where's Your Data?' report is available for download on its site. (Softpedia, 19Feb16)

(U) Obama creates cyber panel

President Barack Obama on Wednesday appointed his former national security adviser, Tom Donilon, to lead a new commission on cybersecurity that will make detailed recommendations on how the nation should better protect itself against computer attacks. Donilon will serve as chairman of the Commission on Enhancing National Cybersecurity. Obama will appoint former IBM chief executive Sam Palmisano to serve as vice chairman. Their task, Obama said, is to produce a report by 1 December that will guide future presidents on the infrastructure necessary to confront long-term computer challenges. The commission that Donilon and Palmisano will lead will consist of up to 12 members and make detailed recommendations dealing with the public and private sectors. Obama said Donilon will come at the job from a national security perspective, while Palmisano brings perspective from the private sector and non-profits. Obama said the commission will examine several challenges, including how to keep huge government databases secure, how to provide timely information to the public about best practices to keep their information safe, and how the government can improve its procurement process and attract the best computer personnel. (AP, 18Feb16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424