Cyber-Threat Newsletter – 18 Jul 16

Patches & Updates of the Week:

(U) Microsoft's Patch Tuesday updates led by rare print spooler bug

(U) Microsoft's July Patch Tuesday offering includes 11 security updates with six rated critical covering almost 50 individual bugs. MS16-084, MS16-085, MS16-086, MS16-087, MS16-088 and MS16-093 were all given a critical rating by Microsoft with MS16-087 being specifically called out by several industry experts as particularly interesting. This bulletin contains CVE-2016-3238 and CVE-2016-3239, which if exploited could allow an attacker to execute a man-in-the-middle attack on a workstation or print server allowing remote code execution. "One of the new appearances this month is Windows Print Spooler; we haven't seen a bulletin related to it in 3 years. Luckily, many enterprises will already have printers installed on their images, which should help to mitigate risk from this," said Tyler Reguly, manager of Tripwire's Vulnerability and Exposure Research Team, told SCMagazine.com in an email. Bobby Kuzma, CISSP, systems engineer at Core Security, agreed the risk of exposure from this particular vulnerability was low, but cited a different reason than Reguly. "It's been a while since we've seen remote code execution in the print spooler of all places. It fails to validate printer drivers, so an attacker would need to be in a position to coerce users into installing the drivers, and the users would need permissions to do so," Kuzma wrote in an email to SCMagazine.com. However, Günter Ollmann, CSO of Vectra Networks, said in an emailed statement to SCMagazine.com, that this vulnerability makes printers a prime threat vector. "This makes printers one of the most powerful threat vectors on a network," Ollmann said. "Rather than infecting users individually, an attacker can effectively turn one printer into a watering hole that will infect every Windows device that touches it." Amol Sarwate, director of engineering and head of vulnerability research at Qualys, pointed out M16-084, MS16-085 and MS16-088 as requiring immediate attention as all three will allow remote code execution and he pointed out that MS16-093 referred to dozens of vulnerabilities related to Adobe's Flash Player. Adobe today issued fixes for these problems "This update affects Windows, Mac, Linux and ChromeOS. As many vulnerabilities fixed by the update allow attackers to take complete control of the victim machine we recommend applying the Flash and Reader update immediately," he wrote in a blog. The five bulletins rated as important by Microsoft contain vulnerabilities that can allow elevation of privilege, information disclosure, security feature bypass and remote code execution if exploited. (scmagazine.com, 12Jul16)

(U) Serious flaw fixed in widely used WordPress plug-in

(U) If you're running a WordPress website and you have the hugely popular All-in-One SEO Pack plug-in installed, it's a good idea to update it as soon as possible. The latest version released Friday fixes a flaw that could be used to hijack the site's admin account. The vulnerability is in the plug-in's Bot Blocker functionality and can be exploited remotely by sending HTTP requests with specifically crafted headers to the website. The Bot Blocker feature is designed to detect and block spam bots based on their user agent and referrer header values, according to security researcher David Vaartjes, who found and reported the issue. If the Track Blocked Bots setting is enabled -- it's not by default -- the plug-in will log all requests that were blocked and will display them on an HTML page inside the site's admin panel. Because the plug-in fails to properly sanitize the requests before displaying them, attackers can inject malicious JavaScript code in the request headers, allowing the code to end up as part of the HTML page. This allows for a persistent cross-site scripting (XSS) attack, where the rogue code will be executed every time a user views the log page. Because that page is in the admin panel, that user will likely be the administrator, and the code can steal their session tokens. These tokens are values stored inside the browser that allows a website to identify a logged in user. By placing these values in their own browsers, attackers could access the website as an administrator without having to authenticate. The rogue code could also force the administrator's browser to perform an action that they haven't authorized. The All in One SEO Pack developer, a company called Semper Fi Web Design, has released version 2.3.7 Friday in order to fix this vulnerability. Users are advised to upgrade to this version as soon as possible or to make sure they don't have the Track Blocked Bots setting enabled. (IDG News Service, 11Jul16)

(U) SQLite vulnerability could expose sensitive data from Chrome, Firefox, and more

(U) SQLite 3.13.0, released at the end of May, contained a fix for a potentially dangerous vulnerability that could be used to leak sensitive data from SQLite temporary files. While SQLite is not the first name that comes to mind when you say "database," this is one of those crucial projects that are used all over the place in various desktop or Web-based products from companies like Adobe, Google, Microsoft, Mozilla, but also many others. According to security researchers from KoreLogic, all SQLite versions prior to 3.13.0 contained an information disclosure issue that originated in the way the database selected the directory where to store temporary files, used to save data that's in transit through the database. Researchers say that SQLite would carry out a series of checks on the app's desired location to store temporary files. If these checks failed, SQLite would store temporary files in the "". path, which was the app's current folder. "[T]his [vulnerability] could lead to insecure behavior by some application using SQLite under these conditions," KoreLogic said. Researchers explain that SQLite-based applications could write temporary files on NFS or SMB network shares, making data capture possible, or on removable drives, which can be taken out of the user's physical control. These temporary files can, in theory, contain sensitive data not meant to be shared outside the original application's scope. For example, Web traffic for browsers or details about downloaded files for a BitTorrent client. Updating all apps using older SQLite databases should take a while. In the meantime, developers should review their code based on KoreLogic's findings. (Softpedia, 07Jul16)

Threats & Vulnerabilities of the Week:

(U) Irongate heralds new cyber threat to industry

(U) The FireEye Labs Advanced Reverse Engineering (FLARE) team has identified a type of malware that can attack industrial control systems (ICS), but hide itself from conventional antivirus software. The malware family, which FireEye has dubbed "Irongate," appears to target specific industrial processes running under a Siemens control system and allows an outside agent to step between the edge node PLC and the operator's HMI system and send false information to both. While the analysis by FireEye and Siemens concludes that the currently-known versions of the malware would not work in a standard Siemens system environment and pose no increased risk to process operators, the code's characteristics seem to indicate an avenue of attack on ICS is developing that may need countering in the long term. According to a report from FireEye, the Irongate code first appeared in 2014, but anti-virus software did not immediately identify it as malicious. FLARE found several Irongate samples in the latter half of 2015 while researching malware "droppers" and began analyzing its operation, issuing its report last month. FireEye concluded that the code examples it has analyzed are a test case, proof of concept, or research activity, not an actual attempt to compromise an ICS, but recommends that industrial systems consider taking steps to counter its attack techniques. The Irongate malware appears to look for and replace DLLs in an ICS with a corrupted version. The malware then acts as a man-in-the-middle between process IO and operator software, capturing legitimate traffic and replaying it to the operator while sending its own commands to the process. The malware also sought to evade detection and resist casual analysis by exiting early when running in a sandbox environment. The specific code samples analyzed targeted user-generated DLLs interacting with a system simulation, such as are used during development to test process control code, and did not threaten deployed systems. Still, Irongate possessed several characteristics unique in ICS malware, and similar to characteristics of Stuxnet. These characteristics include being targeted to a single, specific process, replacing DLLs to achieve process manipulation, recording and playing back process data to hide its manipulation, and detecting anti-malware environments. (EE Times, 13Jul16)

(U) CuteRansomware using Google Docs as a launch platform

(U) Despite its benign nickname, a new strain of malware called cuteRansoware has been uncovered that uses a Google Doc generated by the cybercriminal to host the decryption key and command-and-control functionality, according to a blog post from Netskope. The specific case cited uses Google Docs, but Ravi Balupari, Netskope's director of engineering and cloud security research, told SCMagazine.com in an email on Wednesday that any cloud-based system could be substituted. CuteRansomware was spotted in the latter half of June. Balupari called it rather rudimentary in design and possibly an early version, and believed it was most likely authored in China to target Chinese citizens. The ransomware so far has only been spotted using Google Docs, but Balupari said it is not limited to this cloud app. "This can happen in any cloud app and, in fact, we have seen other ransomware and general malware transferred via other cloud apps. For example, last week we reported on Cerber ransomware being transferred via Microsoft Office 365," he told SCMagazine.com. Using Google Docs specifically creates a host of issues from a cybersecurity standpoint. Netskope noted that Google docs uses HTTPS by default and the network data transmission over SSL can easily bypass normal security measures, such as a firewall. In addition, since the victimized company uses Google Docs as part of its productivity software suite, it is almost impossible to block malicious docs. "We believe this is critical," Netskope wrote. "As malicious actors make increasing use of the cloud for both delivering malware and exfiltrating data via command-and-control, traditional detection tools' lack of visibility into SSL becomes a huge benefit to them." But the most interesting aspect of the threat, the company believes, is how the Google Doc is actually used during the attack. First the ransomware creates a mutex with the name cuteRansomware, encrypts the files and then writes several text files stored under percentTEMP percent directory. A pop-up ransom note is then shown telling the user the files have been encrypted. "Then comes the interesting part: The binary captures the computer name of the victim and uploads it and the RSA key for encrypting/decrypting files to the malicious actor-controlled Google Docs form," Netskope wrote. This malware is being spread mostly through drive-by downloads, Balupari said. CuteRansomware's existence could be a harbinger of things to come. Netskope researchers said hackers may turn to cloud services as an attack platform to store keys and to be an integral part of their command-and-control system. (scmagazine.com, 13Jul16)

(U) Sophisticated nation-state sponsored malware could shut down electric grid

(U) SentinelOne researchers discovered what they believe to be a sophisticated nation-state sponsored malware campaign targeting at least one European electric company. The researchers believe the malware originated in Eastern Europe and a dropper tool is most likely being used to first gain access to targeted network users, and then to introduce a payload designed to extract data or potentially shut down an energy grid, according to a 12 July blog post. The malware appears to be targeting facilities that not only have software security in place, but physical security as well and that the exploit affects all versions of Microsoft Windows and is known to exploit the CVE-2014-4113 and CVE-2015-1701 vulnerabilities, the post said. SentinelOne said it is unknown which attack vector is used by the malware and it is possible that infection is spread via physical access or phishing emails. Researchers said the malware is designed to bypass traditional antivirus solutions, next-generation firewalls, and even more recent endpoint solutions that use sandboxing techniques to detect advanced malware. "The sample evasion and the technique this malware uses to remove the antivirus is not common -- it runs at a very early stage in the boot process, before the antivirus software is loaded," Sentinel One Chief Security Officer Udi Shamir told SCMagazine via emailed comments. "Also, steps have to be taken before the reboot to remove any antivirus that would be running during this early boot time." The payload used in the attack was a simple data exfiltrator that can efficiently send data to an outside adversary and he said the sample obtained by researchers most likely exploits old vulnerabilities in unpatched systems. Shamir noted that the infection doesn't spread on its own and that there is no concern for infection by this variant, however he said it is very possible for attackers to use this technique outside of Europe. The energy industry requires substantial investment to tilt the playing field towards defense, Tim Erlin, Senior Director of IT Security and Risk Strategy at Tripwire told SCMagazine.com via emailed comments. "We've already seen that the industrial systems controlling the power grid can be vulnerable to cyber attacks," he said. "It's no surprise that governments are investing in an expanding arsenal of tools to leverage these weaknesses. Tripwire Chief Technology Officer Dwayne Melancon agreed and added that it pays to make a cyber cooks' lives more difficult. "For example, implementing multi-factor authentication to prevent access using only a password is crucial," Melancon said. "Additionally, organizations should segment their networks to limit the amount of sensitive information that can be accessed by a single account". (scmagazine.com, 13Jul16)

(U) An online market that offered cheap hacked servers returns

(U) A website that offered access to hacked servers for as little as $6 is back online. The market, called xDedic, went down 15 June, right after security firm Kaspersky Lab publicly exposed it. Access to more than 70,000 compromised servers from governments, businesses and universities had been sold through the site, in the two years it was in operation. Kaspersky Lab, however, reported its finding to law enforcement agencies and said that "several major" internet service providers helped shut the site down. But after a brief hiatus, the makers of xDedic have been quick to revive the marketplace, security firm Digital Shadows said on Tuesday. On 24 June, an anonymous user named xDedic was spotted sharing the site's new address on a Russian hacking forum, according to Digital Shadows. The new xDedic site was found to be identical to the original one, although none of the previous user accounts were carried over. The domain was also shared on a French language criminal website located on the dark web. It's still unknown how many users the revived xDedic site currently has, but the previous site attracted 30,000 users a month, Digital Shadows said. Once more hackers become aware of the site, it may only be a matter of time before it becomes popular again, the security firm added. The new xDedic site has opened user registration to all, but at the cost of paying $50. (IDG News Service, 13Jul16)

(U) 92 percent of Internet-available ICS hosts have vulnerabilities

(U) Kaspersky, the first major antivirus vendor to provide security software specifically aimed at ICS/SCADA equipment, has published a report today that details the sad state of security in the field of Industrial Control Systems (ICS). The company's experts say that, following an Internet-wide scan, they found 188,019 hosts connected to ICS equipment, in 170 countries around the globe. Of these, 92 percent, or 172,982, contained vulnerabilities that can be exploited to attack, take over, or even harm devices and their normal mode of operation. While ICS hacking is not as widespread as IoT hacking, which has become a core component of DDoS botnets, malicious groups would find no difficulties in attacking critical infrastructure if they ever chose to. Cyber-attacks on ICS systems, in general, are at an all-time high, according to a Booz Allen report released in June. According to Kaspersky, most of the vulnerable devices are located in the US (57,417), followed at a long distance by Germany (26,142), Spain (11,264), France (10,578), and Canada (5,413). Most of these devices are available to external connections via the HTTP protocol (116,900), Telnet (29,586), Niagara Fox (20,622), SNMP (16,752), or Modbux (16,233). A large number of devices are from vendors such as Tridium (24,446), Siera Wireless (17,908), Beck IPC (14,837), Digi International (12,367), and SMA (11,904). The vulnerability encountered the most, by far in ICS/SCADA equipment was Sunny WebBox Hard-Coded Credentials (CVE-2015-3964), found in 11,904 devices. The vulnerable devices were found in almost all major critical industries: electricity, aerospace, transportation (including airports), oil and gas, metallurgy, chemical, agriculture, automotive, utilities, drinks and food manufacturing, construction, liquid storage tanks, and smart city technology. Internet-available and vulnerable devices were found in both the public and the private sectors. Kaspersky experts say that 17,042 ICS components on 13,698 different hosts likely belonged to very large organizations that had failed to properly secure ICS devices. The high percentage of vulnerable equipment that security researchers discovered shows that companies are failing to update their critical infrastructure in due time, leaving exploitable holes through which malicious actors could carry out economic sabotage. The large number of countries in which vulnerable ICS equipment was discovered shows that attacks on critical network infrastructure are possible against almost any state around the globe. For more in-depth and technical details, Kaspersky provides two reports, one detailing ICS availability statistics and one detailing ICS vulnerabilities. (Softpedia, 11Jul16)

(U) Cerber developers create new ransomware called Alfa

(U) The developers behind the Cerber ransomware released their latest creation upon the Interwebs, and it's a new ransomware variant named Alfa, Bleeping Computer reported last week. Cerber is one of today's most active and widespread ransomware families, alongside Locky, CryptXXX, and Jigsaw. Security researchers did not crack its encryption, so it is quite odd to see the group creating a new and different version without an apparent reason. Since Alfa is new on the scene, security researchers still don't know how this threat spreads, but they are aware that Alfa is linked to Cerber's devs and that it features a rock-solid encryption routine that currently can't be broken. The ransomware targets 142 different file types, and after the encryption process ends, it drops text and HTML-based ransom notes on the user's Desktop and other locations. The ransom note is improperly worded and may need some work. Also, the ransom note uses the "Alpha" term instead of Alfa, which is used only on the Tor-based website where users are told to go to decrypt their files. The name Alfa ransomware will likely be used in future versions because there was already an Alpha ransomware that appeared at the start of May 2016, for which security researchers created a free decrypter. The Cerber devs would likely want to distance themselves from the term "Alpha ransomware" as much as possible since they may not want victims thinking they can recover files after googling the ransomware's name. Alfa asks 1 Bitcoin (~$650) from each infected user. (Softpedia, 10Jul16)

(U) Kovter malware masquerades as Firefox update

(U) Kovter malware, packaged as a legitimate Firefox browser update, is being delivered to unsuspecting victims via drive-by-download attacks. Kovter, which also occasionally installs other malware, has been around for a few years now, and has gone through many changes that keep it a current threat. "What makes this new variant particularly nasty is that it's the later fileless version of Kovter, and it's now using an apparently legitimate certificate," Barkly researchers have discovered. "That's bad news because a legitimate certificate causes plenty of traditional antivirus/endpoint solutions to give the software a pass." As the company shared their insight with other AV vendors, many of them are now able to detect this variant. Comodo, the CA that signed the certificate misused by the malware, has also been notified and will hopefully soon -- if they haven't already -- revoke it. Users are advised always to be wary of random pop-ups telling them some software needs an update. Most software by now -- and popular browsers especially -- have in-software mechanisms for downloading and implementing updates. If, for whatever reason, they don't want to use it, updates should be picked up directly from the vendors' official websites or from well-reputed download sites. "Good user education can generally go a long way to reducing attacks, but as this particular attack demonstrates, even the best of us can be tricked into installing something that appears to be legitimate, or accidentally doing something we wish we could undo," the researchers noted. (helpnetsecurity.com, 08Jul16)

(U) New "Patchwork" cyber-espionage group uses copy-pasted malware for its attacks

(U) Since December 2015, a new cyber-espionage group has been launching attacks aimed at several governments and other related organizations working on military and political assignments linked to issues surrounding Southeast Asia and the South China Sea. This APT (Advanced Persistent Threat) stands apart from all other recent cyber-espionage groups because it doesn't seem to be using its own malware, like, for example, the Pacifier APT. Instead, the group has been copy-pasting malware source code from GitHub and hacking forums to create a "patchwork" of new threats, hence its name of the Patchwork APT. Security firm Cymmetria says the group has targeted and infected at least 2,500 machines in several countries since December 2015 alone, but there are clues that the group may have been active since 2014. For their attacks, the group has used spear-phishing emails that contained PowerPoint files as attachments. Most of these emails used subject lines relating to China's activity in the South China Sea, but sometimes even pornography. The PowerPoint file contained the Sandworm exploit (CVE-2014-4114) that allowed crooks to infect the underlying operating system with their malware. Cymmetria says crooks used an assortment of copy-pasted code from known malware and malware kits such as PowerSploit, Meterpreter, AutoIt, and UACME. This malware jumble effectively created a backdoor trojan, which, in theory, should have been easy to pick up, since most antivirus vendors were well aware of this code and its mode of operation. Unfortunately, the attacks went undiscovered until May 2016, when Cymmetria's security product was the first to catch them. As for attribution for these attacks, things aren't that clear. Cymmetria experts say: "Many of the primary targets of this campaign are regional neighbors of India, and other targets seem to be targeted (by their interests, occupation, and by the content of the spear phishing) to issues affecting India. Circumstantially, this targeting correlates with intelligence requirements necessary for a pro-Indian entity". Evidence includes the times of day when the malware was edited and the times of day when the C&C servers were active, while also indicating that all of India's neighbors were among the targets. India is not known as a hotbed for cyber-espionage campaigns. The low technical ability displayed in the crafting of the malware, which uses publicly available code, may support the conclusion of an Indian actor entering the APT stage. Nevertheless, the same experts say that this evidence could be very well planted to make it look like it's an Indian threat actor behind this campaign. Until further evidence surfaces, 100 percent attribution will have to wait. An in-depth analysis of the Patchwork APT's activities, malware, spear-phishing tactics, and more is available via Cymmetria's Unveiling Patchwork the Copy-Paste APT report. (Softpedia, 07Jul16)

(U) Over 6,000 Redis database servers ready for the taking

(U) The total disregard for any security features in the creation of the Redis database server has come around to haunt the project years after, as Risk Based Security (RBS) reports discovering 6,338 compromised Redis servers. Redis is a NoSQL database server that's ideal for storing data in the key-value format, using an in-memory system for handling the data and subsequent queries. According to statistics from DB-Engines, Redis ranked tenth in terms of usage and popularity in 2015. Because Redis was created with performance in mind, in a default configuration, the database doesn't feature any type of authentication or other hardened security features. This means that anyone can access its content just by knowing its IP and port. Even worse is that, towards the end of 2015, an exploit appeared that allowed a third-party to store an SSH key in the authorized_keys file of any Redis server that doesn't have an authentication system put in place. There are over 30,000 Redis database servers without any authentication available online. According to RBS researchers, 6,338 of these servers were compromised. The company reached this conclusion after performing a non-intrusive scan using Shodan. Scanning Shodan for open Redis servers that featured non-standard SSH keys, researchers found 5,892 instances of SSH keys tied to the email address ryan@exploit.im. They also found 385 keys for root@chickenmelone.chicken.com and 211 keys for root@dedi10243.hostsailor.com. As for compromised Redis database versions, researchers found 106 different versions, ranging from the very early 1.2.0 version up to the latest release, 3.2.1. "While we were unable to get anyone to go on the record, it appears from our analysis that we have confirmation of two things, the first being that this is not a new issue, and second, some servers are sitting out there infected and are not being utilized for anything malicious," RBS researchers explained. The security firm recommends that webmasters update their Redis databases to the most recent version and activate "protected mode," a security feature introduced in Redis with version 3.2. These 6,338 servers are still exposed today, meaning that new threat actors can easily re-compromise them. (Softpedia, 07Jul16)

(U) D-Link flaw affects 400,000 devices

(U) The pre-authentication flaw, discovered by Senrio security researchers, was initially found in the D-Link DCS-930L, a wireless IP surveillance camera that is controlled remotely. A web camera's code vulnerability discovered by researchers last month was reused across the manufacturer's product lines, affecting more than 120 products and 400,000 individual devices. The pre-authentication flaw, discovered by Senrio security researchers, was initially found in the D-Link DCS-930L, a wireless IP surveillance camera that is controlled remotely. The stack overflow vulnerability allows for remote code execution of the device. The researchers discovered that the software component appeared across the company's product lines, although it initially appeared that some of the products did not utilize the software component in the default settings. However, this estimation unfortunately proved to be overoptimistic. D-Link conducted its own analysis of the company's network routers, IoT devices, and home security devices and informed Senrio that more than 120 devices are affected. "It constitutes a fairly sizable portion of their product line," said Stephen A. Ridley, CTO and founder at Senrio. The Taiwan-based manufacturer has not yet released a patch for the flaw. In January, Vectra Networks hacked D-Link's consumer-grade WiFi webcam and used the web camera to create a persistent access point into corporate networks. "While the thought of strangers watching your sleeping baby is disturbing, the implications for enterprise and infrastructure environments are downright scary," the Senrio blog post noted in June. Manufacturers often opt to reuse firmware code across products to create cost savings and cut development time. However, code reuse can make it easier for attackers to exploit a small firmware component to launch attacks against multiple products. The problem is especially dangerous in medical device and industrial control components, according to Ridley. "Code reuse is vulnerability reuse," he said. (scmagazine.com, 07Jul16)

(U) New malware targets Macs

(U) After yesterday security researchers from Bitdefender discovered the Eleanor trojan targeting Macs and opening a backdoor using Tor, today it's ESET's turn to reveal the existence of a similar backdoor trojan that also uses a Tor2Web service to steal Keychain passwords. Named Keydnap and detected as OSX/Keydnap, this trojan is a new arrival on the Mac malware scene, first seen this past May (internal version 1.3.1), and later in June (version 1.3.5). The malware's mode of operation is very simple, even if the infection chain is drawn out in several steps. Everything starts when users receive an email that contains an archive. Unzipping this file drops at first glance either an image or a text file. In reality, there's a space after the file's extension, meaning the file will run in the Mac terminal. This file is a Mach-O executable that uses a fake icon. When executed, this file runs its malicious behavior and then shows an image if it's trying to pose as a picture, or a text pad, if it's trying to pose as a text file. The malicious behavior is a series of operations ran in the console. The file first downloads another component, which is the actual Keydnap backdoor. It then executes the backdoor, which installs itself as LaunchAgent to get boot persistence, and then it downloads the image/text file it was posing as and shows that to the user. After this, the malicious behavior moves to Keydnap, which runs under the current user, but also tries to get root privileges by asking the user for their credentials using a popup. Keydnap then dumps the content of the Mac Keychain using the code of a GitHub project called Keychaindump and opens a link to a Tor website employing the onion.to Tor2Web proxy. The Keychain's content is sent to the C&C server via HTTPS. ESET has detected two C&C servers until now and says that, based on the decoy images the trojan shows to users in its early stages of infection, Keydnap might be after security researchers. The decoy images, in many Keydnap instances, are pictures of botnet C&C control panels, something that only infosec professionals would be interested in. Besides stealing passwords from the infected Mac, Keydnap can also download and execute files from a remote URL, download and execute Python scripts, execute shell commands and report back results, and update the backdoor with a new version. (Softpedia, 06Jul16)

~~(U//FOUO)~~ Researchers describe hardware-level backdoor in computer chips

~~(U//FOUO)~~ University of Michigan researchers have published a technical concept for a chip-level backdoor; according to a 4 June *Softpedia* report. Instead of working like a transistor, the backdoor would work as a capacitor and store energy with every new command it receives. Malicious code can target that area of the chip to start the capacitor's loading process and, after a certain threshold is reached, direct the system to switch into a privileged execution mode. Attackers could then run code on the infected device with system-level privileges. When the attacker stops the malicious code, the capacitor loses all charge and automatically closes itself. According to the researchers, most chip design companies outsource chip fabrication to a third party—often overseas—and rely on post-fabrication testing to guard against malicious modifications. However, since attackers can craft attack triggers that require a sequence of unlikely events, even the most diligent tester can never detect all possible modifications. Nation states would only need one or two strategically placed employees at a company to guarantee access to all devices containing the malicious chip. To counter the threat, the researchers recommended specific new testing technologies for the affected companies. (news.softpedia.com, 04Jun16)

Incidents of Interest:

OGA

OGA

(U) HHS issues ransomware guidance

(U) Hospital systems, medical practices and others that deal with sensitive health information are required to protect that information under health privacy law. Typically in the event of a cyber breach, health providers are required to notify patients that their information has been potentially compromised. But ransomware attacks are different from other kinds of breaches, and the notification rules have not been clear. The Office of Civil Rights at the Department of Health and Human Services is attempting to clarify things with long-anticipated guidance released 11 July. HHS is telling providers that under the Health Insurance Portability and Accountability Act, responses to ransomware attacks should include processes to detect and contain the impact of a ransomware attack, to recover lost data, revive operations and conduct post-incident analysis to determine whether any of the regulatory triggers to report to patients have been tripped. Unless providers can demonstrate that there is "a low probability" that protected health information has been compromised, they must comply with HIPAA requirements to notify affected individual and the HHS secretary "without unreasonable delay". In instances of breaches affecting more than 500 individuals, the media must be notified as well. To demonstrate a low probability of compromise, a provider can identify and mitigate the damage from the attack, by showing a "robust" disaster recovery plan that includes frequent data backups, and by showing that data has not been stolen from the victimized system. The guidance also suggests that best way to protect data on such systems is to keep it encrypted in transit and at rest. The "unsecured protected health information" guidelines under HIPAA do not apply to encrypted data. (fcw.com, 12Jul14)

(U) White House accelerates cyber hiring

(U) The federal government hired 3,000 cybersecurity and IT workers during the first six months of fiscal 2016, and hopes to make an additional 3,500 new hires by January 2017. The hiring spree is part of the Cybersecurity National Action Plan, a $19 billion effort that includes the proposed $3.1 billion IT modernization revolving fund. While pieces of the effort are stalled in Congress, the White House is pushing ahead with the workforce piece of the strategy, according to a 12 July White House blog post. The governmentwide recruitment effort includes the use of special pay authorities, the addition of a cybersecurity cadre to the Presidential Management Fellows program and increased outreach to diversify the cybersecurity and IT workforce. Officials hope to improve recruitment and training and to identify workforce needs by dividing the cyber field into 31 specialty areas. The plan also includes a single program to orient new cyber workers to the government workforce, with an eye toward improving information sharing and career advancement opportunities. (fcw.com, 12Jul16)

(U) Increasing power grid cybersecurity

(U) Cybersecurity experts Jamie Van Randwyk of Lawrence Livermore National Laboratory (LLNL) and Sean Peisert of Lawrence Berkeley National Laboratory (Berkeley Lab) are leading a new program to develop new data analysis methods better to protect the nation's power grid. The project, "Threat Detection and Response with Data Analytics," is part of a $220 million, three-year Grid Modernization Initiative launched in January 2016 by the Department of Energy to support research and development in power grid modernization. LLNL says that the goal of this project is to develop technologies and methodologies to protect the grid from advanced cyber and threats through the collection of data from a range of sources and then use advanced analytics to identify threats and how best to respond to them. Specifically, the project team hopes to be able to distinguish between power grid failures caused by cyber attacks and failures caused by other means, including natural disasters, "normal" equipment failures, and even physical attacks. In addition to LLNL and Berkeley Lab, DOE's Idaho, Oak Ridge, Pacific Northwest, and Sandia national laboratories are also participating in the project. To make the scientific results more realistic and more usable by the power industry, the group is also partnering with the Electric Power Board and the National Rural Electric Cooperative Association, which will help provide data and collaborate in transferring the technology to the power industry. The Energy Department's Grid Modernization Initiative represents a comprehensive effort to help shape the future of our nation's grid and solve the challenges of integrating conventional and renewable sources with energy storage and smart buildings, while ensuring that the grid is resilient and secure to withstand growing cybersecurity and climate challenges. (homelandsecuritynewswire.com, 12Jul16)

(U) CryptoDrop gives users hope to prevent ransomware infections in the future

(U) In the near future, there might be a simple way to stop ransomware infections from locking your files, if we are to believe a team of researchers from the University of Florida and Villanova University. This team presented the CryptoDrop project to the world at the recently concluded IEEE International Conference on Distributed Computing Systems that took place on 29 June in Nara, Japan. CryptoDrop is a computer application currently working only on Windows that keeps an eye on the user's file system for signs and operations specific to ransomware infections. This includes a surge in encryption operations, a drop in available entropy (random data, used to power encryption operations), file type changes (ransomware changes file type extensions), and a few other more. When CryptoDrop makes a detection, it will stop the process and alert the user that something suspicious is happening. The application is not designed to work like an antivirus but alongside one. The researchers say that CryptoDrop will not be able to detect or stop ransomware before encrypting files, but after it already started, so using a powerful antivirus software is still recommended, in order to prevent and block common ransomware threats from taking root on a PC, to begin with. The good news is that, during testing on a computer with 5,100 available files, CryptoDrop detected and stopped ransomware infections in its early stages. They tested their system against 492 ransomware variants, got a 100 percent true positive rate, and ransomware families encrypted on average around ten files before being detected and stopped. The project is similar to what Sean Williams had built this winter via his Cryptostalker project, which worked in a similar way, but for Linux systems. Just like Cryptostalker, CryptoDrop has issues with false positives at the process level. More details can be found in the research paper presented at the IEEE conference, called CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. (Softpedia, 11Jul16)

(U) Avast to acquire antivirus rival AVG

(U) Although Avast and AVG both offer paid security tools, they are best known for their free antivirus software. Some people confuse the two firms because of the similarity of what they do, and the fact their names begin with the same letters, they were founded at around the same time, and originated in the Czech Republic. But that confusion soon won't be an issue as today Avast announces it is set to acquire AVG. Avast is offering $25 per share, about $1.3 billion in total, for its rival and is awaiting AVG shareholder approval (Avast, unlike the public and listed AVG, is itself a private company). As to what this means for users of AVG and Avast products it's hard to say for certain until the deal is finalized. (BetaNews, 07Jul16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424