[redacted] Cyber-Threat Newsletter – 12 Aug 16 (b)(3) 10 USC ⊥ 424

Patches & Updates of the Week:

(U) Microsoft patches 27 flaws

(U) Microsoft released another batch of security patches Tuesday, fixing 27 vulnerabilities in Windows, Microsoft Office, Internet Explorer, and its new Edge browser. The patches are organized in nine security bulletins, five of which are rated critical and the rest important, making this Microsoft patch bundle one of the lightest this year in terms of the number of patches. All of the issues resolved this month are in desktop deployments, but Windows servers might also be affected depending on their configuration. On the desktop side, administrators should prioritize the Microsoft Office and browser patches: MS16-099 (Office), MS16-095 (IE) and MS16-096 (Edge).These vulnerabilities are critical and could be exploited remotely through web pages or Office documents to execute malicious code. Another critical security bulletin that applies to Windows, but also to Microsoft Office, Skype and Lync is MS16-097. It covers patches for three vulnerabilities in the Windows Graphics Component that allow for remote code execution through malicious web pages and documents. The MS16-102 bulletin should also be on the priorities list because it addresses a critical remote code execution flaw in the Windows PDF Library that's bundled with Windows 8.1, Windows RT 8.1, Windows 10, Windows Server 2012, and Windows Server 2012 R2. On Windows 10 with Edge, attackers could exploit the vulnerability by hosting a malicious PDF document on a website and then tricking users into loading that file in their browser. On other systems, attackers would have to trick users to download the document locally and then open it, for example through an email attachment. Even though flagged as important and not critical, the MS16-101 bulletin also stands out because it addresses two vulnerabilities in Windows authentication protocols -- Kerberos and NetLogon. These flaws require the attacker to already be in control of a domain-joined machine or to be in a man-in-the-middle position on the network between a domain-joined computer and its domain controller. The MS16-100 and MS16-098 bulletins, both rated as important, could also get some attention from hackers because they cover flaws that could be used to further their attacks. The flaw described in MS16-100 allows attackers to bypass the Windows Secure Boot feature and to disable code-integrity checks. This allows the loading of test-signed executables and drivers into the OS, a technique that could prove useful for the deployment of system-level rootkits. Meanwhile, MS16-098 fixes four privilege escalation flaws in the Windows kernel-mode drivers. "Overall it's a regular sized Patch Tuesday which will keep Windows desktop administrators busy," said Amol Sarwate, director of Vulnerability Labs at Qualys, in a blog post. (IDG News Service, 10Aug16)

(U) Updated Firefox browser, now with bolstered security

(U) Version 48 of the Mozilla's web browser Firefox has just been released offering new features intended to improve the stability and security of the browsing experience. It is available for Windows, Mac, Linux and Android platforms. The updated browser includes "multiprocess for Firefox for Desktop," in which the rendering engines work in a separate process from the browser shell, freeing up memory so screens won't freeze up. Other browsers have long offered this. The developers at Firefox created a new extension system and created shim layers that enable developers to still support their old extensions. Another security improvement is that Firefox 48 now requires extension signing. Any add-on that has not been verified and signed by Mozilla will not load. The rollout of v48 is available to only around half of the user base at this point, with full rollout expected to increase gradually. (scmagazine.com, 04Aug16)

Threats & Vulnerabilities of the Week:

~~(U//FOUO)~~ Microsoft Windows 10 "golden key" backdoor revealed

~~(U//FOUO)~~In early August, security researchers revealed a major flaw in the Windows 10 Unified Extensible Firmware Interface (UEFI) that could enable attackers to bypass the Windows 10 Secure Boot process and install malware and rootkits at the deepest software level of any device, according to *ZDNet*. When functional, Secure Boot uses a cryptographically signed "boot policy" to validate each component of the Windows boot process and prevents users from installing non-Windows operating systems. However, the design flaw in Secure Boot could enable attackers to apply a policy disabling all operating system checks and install any software—including self-signed binaries—during the boot process, effectively creating a backdoor to any Windows 10 device. According to the researchers, the flaw exemplifies the potential danger of "backdooring" cryptosystems with a "secure golden key." Microsoft issued two patches, in June and July, to address the vulnerability, but the researchers deemed the fixes "inadequate" and said Microsoft could not remediate the vulnerability on all systems without "breaking" installed media, recovery partitions, and backups. A third update is expected in September. (ZDNet.com, 11Aug16)

(U) Linux trojan mines for cryptocurrency using misconfigured Redis database servers

(U) Security researchers have discovered a new self-propagating trojan targeting Linux system, which uses unsecured Redis database servers to spread from system to system. Discovered by Russia-based antivirus maker Dr.Web, the trojan, named Linux.Lady, is one of the few weaponized Go-based malware families. Researchers say that Linux.Lady is written using Google's Go programming language and mostly relies on open source Go libraries hosted on GitHub. The trojan infects systems by connecting to misconfigured Redis database servers for which administrators have forgotten to set a password. According to a recent Risk Based Security report, there are over 30,000 Redis servers available online without a password. The initial entry point is not the Linux.Lady trojan, but a smaller trojan called Linux.DownLoader.196, which, in turn, downloads the main payload after securing a foothold on the infected machine. After the smaller trojan launches Linux.Lady into execution, this latter malware collects information about the infected system and sends it to a C&C server. The collected data includes details such as the computer's current Linux version, the Linux OS family name, the number of CPUs, the number of running processes, and their names. Once the C&C server is informed of the creation of a new bot, it sends over a configuration file, which Linux.Lady uses to start a cryptocurrency mining program that generates digital currency for the crook's account. The trojan mines for a cryptocurrency named Monero, the same one used by the author of the PhotoMiner worm that self-propagated through vulnerable FTP servers. (Softpedia, 09Aug16)

(U) Study highlights serious security threat to many Internet users

(U) Researchers at the University of California, Riverside have identified a weakness in the Transmission Control Protocol (TCP) of all Linux operating systems since late 2012 that enable attackers to hijack users' internet communications completely remotely. Such a weakness could be used to launch targeted attacks that track users' online activity, forcibly terminate a communication, hijack a conversation between hosts or degrade the privacy guarantee by anonymity networks such as Tor. Led by Yue Cao, a computer science graduate student in UCR's Bourns College of Engineering, the research will be presented on Wednesday (10 August) at the USENIX Security Symposium in Austin, Texas. The project advisor is Zhiyun Qian, an assistant professor of computer science at UCR whose research focuses on identifying security vulnerabilities to help software companies improve their systems. To transfer information from one source to another, Linux and other operating systems use the Transmission Control Protocol (TCP) to package and send data, and the Internet Protocol (IP) to ensure the information gets to the correct destination. For example, when two people communicate by email, TCP assembles their message into a series of data packets -- identified by unique sequence numbers -- that are transmitted, received, and reassembled into the original message. Those TCP sequence numbers are useful to attackers, but with almost 4 billion possible sequences, it's essentially impossible to identify the sequence number associated with any particular communication by chance. The UCR researchers didn't rely on chance, though. Instead, they identified a subtle flaw (in the form of 'side channels') in the Linux software that enables attackers to infer the TCP sequence numbers associated with a particular connection with no more information than the IP address of the communicating parties. This means that given any two arbitrary machines on the internet, a remote blind attacker, without being able to eavesdrop on the communication, can track users' online activity, terminate connections with others and inject false material into their communications. Encrypted connections (e.g., HTTPS) are immune to data injection, but they are still subject to being forcefully terminated by the attacker. The weakness would allow attackers to degrade the privacy of anonymity networks, such as Tor, by forcing the connections to route through certain relays. The attack is fast and reliable, often taking less than a minute and showing a success rate of about 90 percent. The researchers created a short video showing how the attacks work. Qian said unlike conventional cyber attacks, users could become victims without doing anything wrong, such as downloading malware or clicking on a link in a phishing email. Qian said. Qian said the researchers have alerted Linux about the vulnerability, which has resulted in patches applied to the latest Linux version. (UCR Today, 09Aug16)

(U) Researchers crack open unusually advanced malware that hid for 5 years

(U) Security experts have discovered a malware platform that's so advanced in its design and execution that it could probably have been developed only with the active support of a nation state. The malware -- known alternatively as "ProjectSauron" by researchers from Kaspersky Lab and "Remsec" by their counterparts from Symantec -- has been active since at least 2011 and has been discovered on 30 or so targets. Its ability to operate undetected for five years is a testament to its creators, who clearly studied other state-sponsored hacking groups in an attempt to replicate their advances and avoid their mistakes. Because of the way the software was written, clues left behind by ProjectSauron in so-called software artifacts are unique to each of its targets. That means that clues collected from one infection don't help researchers uncover new infections. Unlike many malware operations that reuse servers, domain names, or IP addresses for command and control channels, the people behind ProjectSauron chose a different one for almost every target. "The attackers clearly understand that we as researchers are always looking for patterns," Kaspersky researchers wrote in a report published Monday. "Remove the patterns and the operation will be harder to discover. We are aware of more than 30 organizations attacked, but we are sure that this is just a tiny tip of the iceberg". Part of what makes ProjectSauron's so impressive is its ability to collect data from air-gapped computers. To do this, it uses specially prepared USB storage drives that have a virtual file system that isn't viewable by the Windows operating system. To infected computers, the removable drives appear to be approved devices, but behind the scenes are several hundred megabytes reserved for storing data that is kept on the air-gapped machines. The arrangement works even against computers in which data-loss prevention software blocks the use of unknown USB drives. Kaspersky researchers still aren't sure precisely how the USB-enabled exfiltration works. The presence of the invisible storage area doesn't in itself allow attackers to seize control of air-gapped computers. The researchers suspect the capability is used only in rare cases and requires use of a zero-day exploit that has yet to be discovered. In all, Project Sauron is made up of at least 50 modules that can be mixed and matched to suit the objectives of each individual infection. "Once installed, the main Project Sauron modules start working as 'sleeper cells,' displaying no activity of their own and waiting for 'wake-up' commands in the incoming network traffic," Kaspersky researchers wrote in a separate blog post. The main purpose of the malware platform was to obtain passwords, cryptographic keys, configuration files, and IP addresses of the key servers related to any encryption software that was in use. Infected groups include government agencies, scientific research centers, military organizations, telecommunication providers, and financial institutions in Russia, Iran, Rwanda, China, Sweden, Belgium, and possibly in Italian-speaking countries. Kaspersky researchers estimate that development and operation of the Sauron malware is likely to have required several specialist teams and a budget in the millions of dollars. The researchers went on to speculate that the project was funded by a nation state, but they stopped short of saying which one. (ars technical, 08Aug16)

(U) Researchers infect IoT thermostat with ransomware

(U) Ken Munro and Andrew Tierney of Pen Test Partners have demonstrated at the DEF CON 24 security conference in Las Vegas that it is possible to run ransomware on an IoT device such as a thermostat. The two took an IoT thermostat that features a large screen, to show their ransom note, and hacked its underlying codebase, which was running a modified version of Linux. They were able to hack the thermostat because it allowed them to connect an SD card to the device. Additionally, it seemed that every process inside the thermostat software ran with root privileges, meaning they didn't need any special privilege escalation flaws to compromise the device. Because everything was executed with root privileges, the researchers had no problem bringing down the thermostat UI, locking the screen and showing a classic ransom note. "It heats to 99 degrees, and asks for a PIN to unlock which changes every 30 seconds," Munro told Infosecurity Magazine. "We put an IRC botnet on it, and the executable dials into the channel and uses the MAC address as the identifier, and you need to pay one Bitcoin to unlock". The two acknowledged that installing the ransomware is somewhat difficult at the moment. Currently, this requires the crook to have physical access to the device or somehow trick the user into loading malicious files on the device. Munro and Tierney said it took them two evenings to hack the thermostat and that they did it just before the DEF CON conference, so they had no time to file a bug report with the thermostat manufacturer, but they plan to do so today, on Monday. As such, they did not reveal the make and model of the hacked thermostat during their DEF CON presentation. The most important problem the vendor has to fix is to stop code from running as root and move processes into less-privileged user accounts. (Softpedia, 08Aug16)

(U) Researcher hides stealthy malware inside legitimate digitally signed files

(U) A new technique allows attackers to hide malicious code inside digitally signed files without breaking their signatures and then to load that code directly into the memory of another process. The attack method, developed by Tom Nipravsky, a researcher with cybersecurity firm Deep Instinct, might prove to be a valuable tool for criminals and espionage groups in the future, allowing them to get malware past antivirus scanners and other security products. The first part of Nipravskys research, which was presented at the Black Hat security conference in Las Vegas this week, has to do with file steganography -- the practice of hiding data inside a legitimate file. While malware authors have hidden malicious code or malware configuration data inside pictures in the past, Nipravskys technique stands out because it allows them to do the same thing with digitally signed files. That's significant because the whole point of digitally signing a file is to guarantee that it comes from a particular developer and hasn't been altered en route. If an executable file is signed, information about its signature is stored in its header, inside a field called the attribute certificate table (ACT) that's excluded when calculating the files hash -- a unique string that serves as a cryptographic representation of its contents. This makes sense because the digital certificate information is not part of the original file at the time when it is signed. It's only added later to certify that the file is configured as intended by its creator and has a certain hash. Such an addition will modify the overall file size on disk, which includes its header fields, and this file size is checked by Microsoft's Authenticode technology when validating a file signature. However, the file size is specified in three different places inside the file header and two of those values can be modified by an attacker without breaking the signature. The problem is that Authenticode checks those two modifiable file size entries and doesn't check the third one. According to Nipravsky, this is a design logic flaw in Authenticode. The second part of Nipravskys research was to develop a stealthy way to load the malicious executable files hidden inside signed files without being detected. He reverse engineered the whole behind-the-curtain process that Windows performs when loading PE files to memory. This procedure is not publicly documented because developers don't typically need to do this themselves; they rely on the OS for file execution. Nipravskys loader can be used as part of a stealthy attack chain, where a drive-by download exploit executes a malware dropper in memory. The process then downloads a digitally signed file with malicious code in its ACT from a server and then loads that code directly into memory. The researcher has no intention of releasing his loader publicly because of its potential for abuse. However, skilled hackers could create their own loader if they're willing to put in the same effort. The researcher tested his reflective PE loader against antivirus products and managed to execute malware those products would have otherwise detected. (IDG News Service, 05Aug16)

(U) Voting machines, many in swing states, less secure than iPhones

(U) A group of Princeton professors found that many voting machines across the country are less protected than iPhones and are becoming less secure each year. The researchers examined a design called Direct Recording Electronic, or DREs, for more than a decade and found that several machines still in use in hundreds of precincts around the country, many in swing states, can be "jerry-rigged" to vote more than once, have poor encryption and poor safeguards against outside manipulation, according to Politico. Despite the multiple vulnerabilities, the researchers said the threat starts with the machines that tally the votes and keep a record of them -- or, in some cases, don't. "We are in a collision course between the technology we use in election administration and the growing reality of politically motivated, state-level cyberattacks," researcher Alex Halderman said in the report. (scmagazine.com, 05Aug16)

(U) HEIST attack on SSL/TLS can grab personal info, Black Hat

(U) A new technique has been unveiled that can attack the SSL/TLS and other secure channels purely in the browser to expose encrypted email addresses, Social Security numbers and other sensitive data. The exploit of the HTTPS cryptographic scheme dupes end-users by hiding a JavaScript file in a web ad or directly on a webpage. The attack, named HEIST by its developers, Mathy Vanhoef and Tom Van Goethem, doctoral candidates at the University of Leuven in Belgium, enables the exploit of flaws in network protocols without having to sniff actual traffic. The two presented their findings at Black Hat on Wednesday. In particular, they showed how a side-channel attack could affect the way responses are sent at the TCP level, which could then grab a plaintext message. "Compression-based attacks [such as CRIME and BREACH] can now be performed purely in the browser, by any malicious website or script, without requiring network access," the researchers said. Whereas before an attacker would approach from a man-in-the-middle position, the new strategy allows bad actors to capture victims by using a website owned by a malicious party. The consequence, they explained, is that their attack can allow the theft of sensitive information from targets by penetrating services on websites. (scmagazine.com, 04Aug16)

(U) Credit card thieves could still counterfeit despite chip technology, researchers say

(U) Computer researchers have found that thieves could continue to counterfeit credit cards by making the chip security feature seem nonexistent. Researchers at NCR Corporation, a credit card processing technology company, discovered the EMV chip-based system, which has been praised for making it difficult to counterfeit credit cards, could be jeopardized by credit card thieves if they rewrite the code in the card's magnetic strip, which is supposed to tell payment machines to use the chip, to appear the card has no chip at all. "There's a common misperception EMV solves everything. It doesn't," NCR researcher Patrick Watson told CNNMoney. Banks forced many retailers to switch to using the chip as a security feature. The National Retail Federation has criticized the upgrade, which is estimated to have cost American retailers about $25 billion. Many retailers are still working to upgrade payment machines with the latest security features, such as transaction encryption, so many credit cards are still at risk. (UPI, 04Aug16)

Incidents of Interest:

(U) Hackers hit Oracle's Micros payment systems division

(U) Russian cybercriminals have infiltrated systems at Micros, an Oracle division that is one of the world's biggest vendors of point of sale payment systems for shops and restaurants, according to an influential security blogger. The hack has affected 700 computer systems at Micros and is thought to have begun with infiltration on a single machine at the company, said Brian Krebs on his Krebs on Security blog on Monday. The incident is worrying for the potential size of the hack and the systems affected. Oracle acquired Micros in 2014, when it said Micros systems are used in more than 330,000 sites in 180 countries. In an undated letter shared with IDG News Service, the company said it had "detected and addressed malicious code in certain legacy Micros systems". The letter said payment card data is encrypted "both at rest and in transit" in the Micros system. Oracle said it has "implemented additional security measures" to prevent a recurrence, but it did not describe what they are. It is requiring all Micros customers to change their passwords and the password for any account used by a Micros representative to access the payment system. Krebs quoted two researchers briefed on the investigation who said Oracle's customer support portal was monitored communicating with a server run by the "Carbanak Gang," a Russian cybercrime syndicate. (IDG News Service 08Aug16)

(U) Two crooks arrested for stealing over 100 Dodge and Jeep cars using only a laptop

(U) Houston police arrested two crooks under accusations of stealing over 100 Dodge and Jeep SUVs via high-tech methods that involved using a laptop to break into the cars software and hijack its controls. For over a year, Houston police received complaints about cars mysteriously disappearing while their owners left them parked at home or in public places. Most of these models were Dodge and Jeep SUVs, which were later spotted crossing the border into Mexico. For months, police investigators could not explain how crooks were stealing these cars without triggering alarms or damaging the vehicles. They received their first clues in April when one car owner's home video system captured the crooks in action, approaching the car using a laptop, opening the doors, getting inside the car, and using the laptop to start the vehicle and make their getaway. On 4 August, the Houston Police Department announced the arrest of Michael Arce, 24, and Jesse Zelaya, 22, for the theft of a Jeep Grand Cherokee on 30 July using the same method described above. The two are now the main suspects behind all the thefts reported until now that fit this mysterious mode of operation, according to local news media. Police said they expect this new method of high-tech car theft to proliferate among crooks as it poses less risk of getting caught and smart cars will become more affordable. (Softpedia 06Aug16)

[redacted] OGA

Items of Interest

(U) White House cyber commission wants public input

(U) The White House cyber commission wants input on how to keep Americans safe in cyberspace. The Commission on Enhancing National Cybersecurity today posted a request for information in the Federal Register for broad input about cybersecurity in the digital economy today and in the future. 'Steps must be taken to enhance existing efforts to increase the protection and resilience of the digital ecosystem, while maintaining a cyber environment that encourages efficiency, innovation and economic prosperity,' the RFI states. The commission, stood up by executive order as part of the Cybersecurity National Action Plan, is tasked with creating a road map to improve public- and private-sector cybersecurity over the next 10 years while also protecting privacy and fostering innovation. The RFI says the commission wants to hear 'from individuals and organizations of all sizes and their representatives from sector and professional associations,' as well as from government agencies, standards-setting organizations, solutions providers, industry and other stakeholders. Comments are due to the National Institute of Standards and Technology by 5 p.m. EST 9 September 2016. (NextGov 10Aug16)

(U) The Obama administration is getting ready to elevate the role of Cyber Command

(U) The United States Cyber Command is sub-unified command in the US Department of Defense, responsible for cyberspace operations and protecting US military networks. According to Reuers, the Obama administration is getting ready to elevate the organization to a unified command, which would put it on par with the other nine combat commands. The elevation of the unit signifies recognition of the importance of cyber warfare in the years to come. Cyber operations have grown in recent years, with the command conducting cyber attacks against the Islamic State. First established in 2010, Cyber Command is currently one of the subordinate units within the United States Strategic Command, which is charged with space operations, information security, strategic nuclear deterrence, and other similar tasks. The move will separate Cyber Command from the National Security Agency, which share a director. According to Reuters, the split is partially due to the evolving nature of each respective group. Where the NSA is primarily tasked with intelligence gathering, Cyber Command's role appears to be more active: stopping ongoing cyber attacks and launching counter attacks. The plan is not set in stone, with the exact nature of Cyber Command's role currently under debate at the Pentagon. (The Verge 07Aug16)

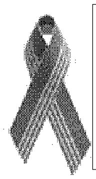
(U) White House drops final federal source code policy

(U) The White House released final policy that requires agencies to share software code with each other and with the public, according to a blog post from US Chief Information Officer Tony Scott. As part of a movement toward open source software, the White House is launching a pilot requiring agencies to share 20 percent of their custom-developed source code with the public and encouraging them to share more of it with each other to cut down on duplicative technology contracts. The White House also plans to unveil Code.gov, an inventory for that source code, in the next 90 days. The policy would apply to code custom-developed by outside contractors for the federal government -- the code federal employees write is in the public domain by default. It incorporates public feedback gathered on an earlier draft, published in March, according to Scott's post. Open source proponents argue that sharing software can slash federal spending by allowing agencies to reuse products their colleagues have developed. Supporters also believe citizen developers can examine federal source code, alerting the government to potential security vulnerabilities. Members of the General Services Administration's tech consultancy 18F, for instance, have lobbied for an "open source by default" policy, instead of just 20 percent. The policy has also found some critics in the federal government. Commenter's originally attributed to the Homeland Security Department likened open source code to "Mafia having a copy of all FBI system code" or a "terrorist with access to air traffic control software." They also suggested removing the pilot's 20 percent requirement for shared code. DHS subsequently stated those comments were published incorrectly and do not reflect official policy; CIO Luke McCormack wrote later that releasing code "can have extensive cybersecurity benefits" and that his team "strongly supports" the policy. (NextGov 08Aug16)

[redacted] OGA

[redacted] (b)(3) 10 USC ⊥ 424

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



[redacted] (b)(3) 10 USC ⊥ 424