Cyber-Threat Newsletter – 14 Jun 16

Patches & Updates of the Week:

(U) Microsoft fixes critical flaws in Windows, IE, Edge, and Office
(U) Microsoft has fixed more than 40 vulnerabilities in its products Tuesday, including critical ones in Windows, Internet Explorer, Edge, and Office. The vulnerabilities are covered in 16 security bulletins, six of which are marked as critical and the rest as important. This puts the total number of Microsoft security bulletins for the past six months to more than 160, a six-month record during the past decade. Companies running Windows servers should prioritize a patch for a critical remote code execution vulnerability in the Microsoft DNS Server component, covered in the MS16-071 bulletin. Attackers can exploit this vulnerability by sending specifically crafted DNS requests to a Windows Server 2012 or a Windows Server 2012 R2 deployment configured as a DNS server. The critical bulletins for Internet Explorer and Edge, namely MS16-063 and MS16-068, should also be high on the priority list because they cover remote code execution flaws that can be exploited by simply browsing to a specially crafted website. Next on the list should be the Microsoft Office security bulletin, MS16-070, because the applications in the Office suite are a common target for attackers, particularly through malicious email attachments. Kandek believes that the most important vulnerability in the Office bulletin is a remote code execution flaw tracked as CVE-2016-0025 that stems from the Microsoft Word RTF format. Even though 10 security bulletins are marked as Important, companies should evaluate them in the context of their particular environments. Some of them might turn out to be urgent to some assets. (IDG News Service, 15Jun16)

(U) Clear path to Verizon email accounts patched
(U) A vulnerability that could have allowed attackers to hijack incoming emails from Verizon users' inboxes without their knowledge has been detected by security researcher Randy Westergren, and patched by the communications company. By substituting a friend's userID into the parameter settings of his own Verizon account, Westergren proved he was able to alter the forwarding address for any user account. "Any user with a valid Verizon account could arbitrarily set the forwarding address on behalf of any other user and immediately begin receiving his emails," he wrote. This is, he wrote, an "extremely dangerous situation" as primary email accounts are commonly used to update passwords for other accounts. After he sent Verizon a proof-of-concept, the company issued a patch, although citing a recent strike, slower than Westergren would have liked. (scmagazine.com, 15Jun16)

(U) Adobe issues Flash Player advisory, patch Tuesday updates
(U) Adobe today issued a security advisory for CVE-2016-4171, a critical vulnerability in Flash Player along with four security bulletins notifying users of issues with three other company products. The Flash Player vulnerability has been spotted in the wild being used in limited, targeted attacks, Adobe said, adding an update to address this problem will be rolled out possibly as early as 16 June. The issue was discovered by Anton Ivanov and Costin Raiu of Kaspersky Lab and successful exploitation could cause a crash and potentially allow an attacker to take control of the affected system. Wolfgang Kandek, Qualys CTO, said in a blog post that the despite the flurry of Adobe and Microsoft bulletins being issued today Adobe's Flash Player advisory should take precedence. "Pay close attention to the release and address as quickly as possible. By the way, this is the third month in a row that we are seeing a 0-day in Flash, making it most certainly the most targeted software on your organization's endpoints, Kandek wrote. Microsoft is expected to release the patch at the same time as Adobe. The four bulletins cover issues that have not been exploited in the wild, but still require user's attention. Security bulletins APSB16-19 (CVE-2016-4167) and APSB16-20 (CVE-2016-4164, CVE-2016-4165) resolve issues with Adobe's DNG Software Development Kit. The updated for CVE-2016-4167resolves a memory corruption vulnerability, while the latter two CVEs are fixes a JavaScript injection vulnerability and a vulnerability in the extension manager. Security Bulletin APSB16-21 (CVE-2016-4157, CVE-2016-4158) for Adobe Create Cloud Desktop Application has resolves an untrusted search path vulnerability in the Creative Cloud Desktop Application installer, and an unquoted service path enumeration vulnerability in the Creative Cloud Desktop Application. Adobe's released hot fixes an update for Cold Fusion, bulletin APSB16-22 (CVE-2016-4159), that repair an input validation issue that could be used in reflected XSS (cross-site scripting) attacks. (scmagazine.com, 14Jun16)

(U) Netgear removes crypto keys hard-coded in routers
(U) Qualys security researcher Mandar Jadhav has discovered two serious vulnerabilities in Netgear D6000 and D3600 modem routers, which can be exploited to gain access to the devices and to intercept traffic passing through them. The vulnerabilities reside in the devices' firmware, versions 1.0.0.47 and 1.0.0.49. The first one (CVE-2015-8288) is due to the firmware containing a hard-coded RSA private key and a hard-coded X.509 certificate and key. An attacker that discovers this information can misuse it to gain administrator access to the device, implement man-in-the-middle attacks, or decrypt passively captured packets. It can be exploited if an attacker can access the internal network, or remotely if remote management is enabled on the device. The second one (CVE-2015-8289) is an authentication bypass flaw. "A remote attacker able to access the /cgi-bin/passrec.asp password recovery page may be able to view the administrator password in clear text by opening the source code of above page," Software Engineering Institute's CERT Coordination Center warns. According to the advisory, other models and firmware versions may also be impacted, but for now Netgear has confirmed the existence of these vulnerabilities only in the aforementioned router models and firmware versions. They have provided firmware updates (v1.0.059) that fix the flaws, and urge users to implement it as soon as possible. CERT CC also suggested a workaround to minimize the possibility of an attack exploiting these flaws: "Restrict network access to the Netgear device's system web interface and other devices using open protocols like HTTP". (helpnetsecurity.com, 14Jun16)

(U) Bug in Chrome's PDF reader allows arbitrary code execution

(U) Vulnerabilities in software often arise from faulty implementations of elements developed by other code writers. Take for example CVE-2016-1681, the heap-based buffer overflow vulnerability affecting PDFium, the default PDF reader that is included in the Google Chrome web browser. The vulnerability is present in OpenJPEG, the underlying jpeg2000 parsing library. "An existing assert call in the OpenJPEG library prevents the heap overflow in standalone builds, but in the build included in release versions of Chrome, the assertions are omitted," threat researcher Earl Carter explained. The flaw can be easily exploited through a PDF file with an embedded jpeg2000 whose SIZ marker specifies 0 components, which the Talos team created as a PoC exploit. The complexity of such an attack is low, and does not require the attackers to achieve special privileges or perform any type of authentication. It does require user interaction, but users frequently browse PDF files when surfing the web and it shouldn't be too hard for attackers to trick victims into downloading and viewing such a specially crafted file. The vulnerability can be exploited to achieve arbitrary code execution on the victim's system, and can result in disruption of service, unauthorized information disclosure and modification. In this particular case, the good news is that the flaw was discovered by a security researcher (Aleksandar Nikolic of Cisco Talos) that responsibly disclosed it to the vendor (Google). They fixed it in a day, by simply changing the problematic 'assert' statement to an 'if'. Version 51.0.2704.63 of the Chrome browser, which includes the fix, has been released on 25 May. With the details about the vulnerability made public, users would do well to update to that version or the latest one (51.0.2704.79) in order to avoid potential compromise. (helpnetsecurity.com, 09Jun16)

(U) Mozilla's Firefox 47 patches 13 vulnerabilities, two critical

(U) In its latest Firefox browser release, Mozilla this week fixed two critical vulnerabilities -- a buffer overflow hazard and a set of memory safety hazards -- plus 11 other security holes ranging from low to high in severity. Discovered by the security researcher "firehack," the buffer overflow issue (CVE-2016-2819) would occur while parsing HTML5 fragments in a foreign context such as under an SVG (Scalable Vector Graphics) node. According to Mozilla in its security advisory, inserting an HTML fragment into an existing document can trigger a "potentially exploitable crash." The other severe flaw was described as miscellaneous memory safety hazards (CVE-2016-2818 and CVE-2016-2815) found in Firefox and its Extended Support Release. "Some of these bugs showed evidence of memory corruption under certain circumstances, and we presume that with enough effort at least some of these could be exploited to run arbitrary code," Mozilla wrote. Among the vulnerabilities patched in Firefox 47 that had a high level of severity was a bug that under certain circumstances created a pointerlock without user permission. This pointerlock could not be cancelled without terminating the browser, thus resulting in a persistent denial of service attack. Another was a flaw whereby the Mozilla Windows updater could be used to overwrite arbitrary files, which could have led to an unauthorized privilege escalation. Other high severity flaws that were addressed included an out-of-bounds write when using the ANGLE graphics library for WebGL (Web Graphics Library) content, and two use-after-free vulnerabilities, which are a type of memory corruption flaw that can be exploited if someone attempts to access and reuse memory after it has been freed. (scmagazine.com, 09Jun16)

Threats & Vulnerabilities of the Week:

(U) Cyber-espionage group targets US government with new malware persistence trick

(U) On 28 May 2016, a Russian-linked cyber-espionage group sent a spear-phishing email to a US government official from an infected computer in the IT network of another country's Ministry of Foreign Affairs. The email contained an RTF document called Exercise_Noble_Partner_16.rtf, referring to a joint US-Georgian military exercise. According to Palo Alto Networks, opening this file would trigger the CVE-2015-1641 exploit that would download and place two DLL files (btecache.dll and svchost.dll) on the victim's computer. Security researchers claim that these two files load a Carberp variant of the Sofacy trojan used by the Sofacy cyber-espionage group. This group has affiliations to Russian military intelligence service GRU and is also known under names like Fancy Bear, APT28, Sednit, Pawn Storm, or Strontium. Palo Alto researchers said that there was something that caught their eye during this most recent Sofacy campaign. The group had apparently come up with a never-before-seen trick to gain persistence on infected devices. While most malware adds a registry key to start its malicious process when the computer boots up, Sofacy's malware used a different technique. The hackers opted to start their malware only when the user opens a Microsoft Office product such as Word, PowerPoint or Excel. "This is the first time Unit 42 has seen the Sofacy group, or any other threat group for that matter, use this tactic for persistence purposes," Palo Alto's Robert Falcone and Bryan Lee noted. Luckily for the security researchers, there were some inconsistencies in the group's operation. First of all, the RTF document never showed any content to the user, alerting him that something was wrong. Secondly, as Palo Alto noted, the group had recycled IP addresses and C&C server domains from past campaigns. The end result is that Sofacy wasted a novel malware persistence technique that could easily evade most sandbox analysis operations, all because it didn't pay enough attention to the smaller details. Now that security firms are aware of this trick, their security products will no doubt scan for and detect this new mechanism. (Softpedia, 14Jun16)

(U) JavaScript email attachments can carry potent ransomware

(U) Attackers are infecting computers with a new ransomware program called RAA that's written entirely in JavaScript and locks users' files by using strong encryption. It's rare to see client-side malware written in web-based languages such as JavaScript, which are primarily intended to be interpreted by browsers. Yet the Windows Script Host, a service built into Windows, can natively execute .js and other scripting files out of the box. Attackers have taken to this technique in recent months, with Microsoft warning about a spike in malicious email attachments containing JavaScript files back in April. Last month, security researchers from ESET warned of a wave of spam that distributes the Locky ransomware through .js attachments. In both of those cases the JavaScript files were used as malware downloaders -- scripts designed to download and install a traditional malware program. In the case of RAA, however, the whole ransomware is written in JavaScript. According to experts from tech support forum BleepingComputer.com, RAA relies on CryptoJS, a legitimate JavaScript library, to implement its encryption routine. The implementation appears to be solid, using the AES-256 encryption algorithm. Once it encrypts a file, RAA adds a .locked extension to its original name. The ransomware targets the following file types: .doc, .xls, .rtf, .pdf, .dbf, .jpg, .dwg, .cdr, .psd, .cd, .mdb, .png, .lcd, .zip, .rar and .csv. "At this point there is no way to decrypt the files for free," said Lawrence Abrams, the founder of BleepingComputer.com, in a blog post. (IDG News Service, 14Jun16)

(U) Chinese APT targets victims with social engineering and ShimRat malware

(U) Mofang ("to imitate" in Chinese) is the name of a newly discovered cyber-espionage group that targeted various countries around the globe since February 2012, when the group's main malware, called ShimRat, was found by security firm Fox-IT. While the first attacks were recorded in February, the group sprang to life in May, when attacks with ShimRat intensified, first targeting the Ministry of Commerce in Myanmar, and then two German companies in the automotive industry. Attacks continued in January 2013, when Mofang hit a Canadian organization, then in April and August 2013, against unknown organizations. The group finished 2013 on a high note in September when they hit a US government agency, and companies in India and Singapore. 2014 was also a busy year, with the group launching attacks in February (South Korean company), April (Myanmar government entity, Canadian and US companies), June (US company), and November (unknown organization). Attacks continued in 2015 when Mofang hit Myanmar government agencies and private companies in four different incidents. Compared to other APTs, Mofang has a distinct mode of operation. The group doesn't rely on exploits to infect a target's computers, but only uses social engineering, mainly via a careful target selection and specifically crafted spear-phishing emails. Once the group compromises a target, the group sends spear-phishing emails that contain Word, PDF or Excel files. If targets open these files, then executables for legitimate applications are dropped and executed on their computers. These are legitimate apps, usually from companies such as McAfee, Symantec or Norman. Mofang uses DLL hijacking to disguise its malware within these apps. At a later stage, these apps drop the ShimRat or ShimRatReporter malware. These two leverage a UAC bypass to escalate their privileges in order to run undisturbed on infected systems. Because Mofang uses DLL hijacking, the malware runs from its parent process, which is the legitimate app, usually an antivirus. ShimRat is a basic remote access trojan and can enumerate connected drives; list, create and modify directories; upload and download files; delete, move, copy and rename files; execute programs; execute commands; and even uninstall itself. ShimRatReporter can collect information such as IP address, network info, OS info, a list of active processes, browser and proxy configurations, active user sessions, user accounts, and a list of installed software. This information is then sent to a C&C server, from where the crooks give the go-ahead for a ShimRat infection. On the matter of attribution, Fox-IT expert Yonathan Klijnsma said that Mofang "almost certainly operates out of China and is probably government-affiliated". "It is highly likely that Mofang's targets are selected based on involvement with investments, or technological advances that could be perceived as a threat to the Chinese sphere of influence," he also added. Fox-IT's report on Mofang's activities details a possible link between the cyber-attacks and the investments of a Chinese state-owned company that bid on an oil and gas pipeline project. The Myanmar government eventually awarded the project to the Chinese company. (Softpedia, 14Jun16)

(U) FLocker ransomware now targeting smart tvs

(U) Trend Micro researchers have found the first major example of ransomware that can attack a Smart TV with hackers using an updated version of FLocker that targets devices running the Android operating system. Trend Micro researcher Echo Duan wrote in a blog post that this FLocker version, one of more than 7,000 variants that have been tracked by the company since the malware was first spotted in May 2015, has the ability to infect and lock the screen of any device running the Android operating system, including a Smart TV. "This is the first major instance of ransomware to infect TVs that we've found," Christopher Budd, global threat communications manager, told SCMagazine.com in an email. This FLocker operates as a police Trojan and attempts to scare the victim into paying by claiming to be the "US Cyber Police." Once the malware is downloaded and the TV locked, the hacker accuses the victim of a false crime and demands $200 in iTunes gift cards to have the Smart TV or mobile device unlocked. "As far as how, it's being delivered through standard infection vectors: nothing new or special. The TVs in this case are accidental collateral damage of the ransomware, and not specifically targeted. They just happen to be running an attackable version of Android." Budd said. Duan said there is little difference between FLocker that attacks mobile devices and the version that goes after Smart TVs. "To avoid static analysis, FLocker hides its code in raw data files inside the "assets" folder. The file it creates is named "form.html" and looks like a normal file. By doing so, the code of "classes.dex" becomes quite simple and no malicious behavior could be found there. Thus the malware has the chance to escape from static code analysis. When the malware runs, it decrypts "form.html" and executes the malicious code," he wrote. FLocker then checks to see if the device being attacked is located in Kazakhstan, Azerbaijan, Bulgaria, Georgia, Hungary, Ukraine, Russia, Armenia or Belarus. If so it deactivates itself. For those people who do not live in Eastern Europe Duan suggested contacting the manufacturer or if the victim is a bit tech savvy they can possibly handle the task on their own. "Another way of removing the malware is possible if the user can enable ADB debugging. Users can connect their device with a PC and launch the ADB shell and execute the command "PM clear percentpkg percent". This kills the ransomware process and unlocks the screen. Users can then deactivate the device admin privilege granted to the application and uninstall the app," he said. (scmagazine.com, 13Jun16)

(U) Vawtrak malware updated to break tools used by researchers

(U) A new version of banking malware includes updates to the Vawtrak trojan that break tools typically used by security researchers to analyze the malware, according to a report. The malware continues to be actively developed, John Shier, senior security advisor at Sophos, told SCMagazine.com. A new version of the banking malware, referred to by researchers at SophosLabs as 'Vawtrak version 2' contains added "features" targeting new victims and geographies. "There is an active set of developers that has been acquiring new customers on a regular basis," Shier said. "There are new command and control servers being added regularly." The malware used to have one monolithic binary that contained entire the payload, although the newest version now contains other modules, he said. "This may point to the ability to build particular custom modules for customers," Shier noted. "It makes it easier to deliver the payload." The Vawtrak malware is likely not related to any of the malicious programs that enabled attacks against SWIFT member banks. The malware used in the SWIFT cyberattacks, he said would require "more specialization and knowledge of esoteric systems," such as the mechanisms of SWIFT and banking protocol functionality. An earlier report by Sophos, in 2014, found that Vawtrak was used to target financial institutions in the U.S., Canada, United Kingdom, Japan, and Israel, with the US being the largest target. The earlier report was published after DDoS attacks by Iranian hackers that knocked banking systems offline. Shier said there was no "smoking gun indicator" that the malware was related to the Iranian attacks. "The authorship of this still remains rather cloaked," he noted. (scmagazine.com, 13Jun16)

(U) Hackers find way to bypass Google's two-factor authentication

(U) There's a sneaky new trick going around that can fool some people into divulging their two-factor authentication code to crooks, while thinking they're actually protecting their accounts. Two-factor authentication, or 2FA, is a second layer of authentication that many online services support, from banks to Google, from Facebook to government agencies. 2FA works by requiring a user to enter a code that they received via SMS on their phone after they logged into a 2FA-protected account. If the user doesn't enter the code promptly, the login is classified as a hacking attempt, and the user blocked from accessing the account, even if they entered the correct password. This past week, Alex MacCaw, co-founder of Clearbit.com, tweeted out the image of an SMS he had just received. The SMS read as follows: " (Google Notification) We recently noticed a suspicious sign-in attempt to jschnei4@gmail.com from IP address 136.91.38.203 (Vacaville, CA). If you did not sign-in from this location and would like to lock your account temporarily, please reply to this alert with the 6-digit verification code you will receive momentarily. If you did authorize this sign-in attempt, please ignore this alert. " Basically, the attackers were mentally preparing the victim to receive the 2FA verification code, for their illegal login attempt they were about to carry out. The crooks were going to access MacCaw's account, and when his 2FA system would kick in, MacCaw would act to lock his account by sending the "verification code to Google." In fact, MacCaw would be sending the 2FA code to the crook, who would then enter it in the login page and access his account, with his cooperation. Fortunately, MacCaw recognized their tactics and didn't fall for this new type of social engineering trick. (Softpedia, 12Jun16)

(U) Combo of Zeus and Carberp trojans discovered with self-spreading capabilities

(U) Bolek is the name of a new banking trojan that has spawned from the leaked source code of the Carberp and the Zeus banking trojans. Malware coders have mixed their code to create an all-new threat that is currently going after the customers of Russian banks. CERT Poland researchers spotted the trojan first in mid-May, when they investigated a phishing campaign originating from their country, noticing a slight resemblance between Bolek and the KBot module of Carberp. Two days later, US security firm PhishMe expanded CERT-PL's findings with a comprehensive report on Bolek's mode of operation, also noticing the visible similarities between Bolek and Carberp. More reports also followed, first from Russian antivirus maker Dr.Web, and then from Arbor Networks, both at the start of June. While the Arbor report focused on Bolek's C&C server communications, the Dr.Web one included a breakdown of the trojan's mode of operation, along with similarities between Bolek, Carberp, and even the ancient Zeus banking trojan. Dr.Web's says the trojan is fully equipped for today's banking ecosystem. Bolek is able to steal login credentials from online banking applications by injecting itself into a Web browser's process, can take screenshots of the user's screen, can intercept Web traffic, can log keystrokes, or can create a local proxy server in order to transfer files out of the infected machine. Bolek can target Microsoft Internet Explorer, Google Chrome, Opera, and Mozilla Firefox browsers, and comes with an embedded version of the Mimikatz, a known password dumping application. The part that Bolek borrowed from Carberp includes a custom virtual file system, which the trojan uses to store various files needed for its operation, in order to hide them from security software. From Zeus, Bolek borrowed its powerful Web injection mechanism that allows it to tap into browser processes and take over the entire Web page when the user visits an online banking portal. Furthermore, the trojan can infect both 32-bit and 64-bit Windows machines, and when instructed, it can also open a reverse connection to the attacker via RDP (Remote Desktop Protocol). Despite all these deadly features, this was not the most interesting feature highlighted by Dr.Web researchers. After infecting a target, Bolek's masters can send a command to the trojan and activate a worm-like self-spreading mechanism. This feature allows the trojan to spread to other files on the same filesystem or USB drives. Bolek has the ability to taint Windows 32-bit or 64-bit executables, which, if moved to other computers, can help the trojan spread to other targets. (Softpedia, 12Jun16)

(U) Ransomware now comes with live chat support

(U) Victims of a new version of Jigsaw now have access to live chat operators to help them through the ransom payment process, Trend Micro says. The purveyors of the malware have introduced a new live chat feature that gives victims a way to directly contact their extortionists and negotiate a ransom payment. Instead of requiring customers to go to dark web sites, the operators have made people available to answer questions and provide direction to victims on how to pay the ransom. Security vendor Trend Micro, which reported on the chat feature this week, said the threats displayed by the new Jigsaw variants are similar to the threats displayed to victims of the original version of the ransomware. Jigsaw first surfaced earlier this year and was notable at the time for what Trend Micro described as its tendency to lock and delete files incrementally. "To an extent, it instills fear and pressures users into paying the ransom. It even comes with an image of Saw's very own Billy the puppet, and the red digital clock to boot," Trend Micro said about that version. The new versions of Jigsaw are not different in that respect. But in addition to the usual threats about the ransom amount doubling after a specific period of time and data being deleted if any attempt is made to tamper with the program, the screen also displays a link, which appears to go to a live chat session. To test the service the attackers offered, a Trend Micro researcher posed as a New York-based worker whose office computer had been infected with Jigsaw. The ensuing conversation, a transcript of which is pasted on Trend Micro's blog, suggests that the chat operator is willing to negotiate a little on the price and wants to reassure the "victim" about the data being decrypted upon receipt of the ransom. A script that calls the onWebChat client is embedded in the website. The connection between the website that the victim is directed to for payment and onWebchat's servers are encrypted making interception and packet capture difficult, according to the security vendor. Somewhat interestingly, the individual conducting the chat conversation did not appear to know the ransom amount that the victim was being asked to pay and appeared reliant on the honesty of the victim to provide that information. "That's because they haven't built a channel to upload data from the victim to the 'call center,'" says Christopher Budd, global threat communications manager at Trend Micro. The countdown clock associated with the ransomware also is only tied to a cookie set on the infected machine by the attackers. If the cookie is deleted, the timer is reset to 24 hours, Trend Micro said. By providing a human voice to go to and by making the process of paying the ransom easier, the purveyors of the new Jigsaw variant appear to be trying to convince users into paying up, the vendor noted. "This is a first for ransomware, but this type of support is consistent with a broader trend of professionalization" in the cybercrime industry, Budd says. (Dark Reading, 10Jun16)

(U) Hackers shift to Neutrino exploit kit to spread CryptXXX ransomware

(U) Change of tactics from cyber-criminals may be an attempt to bypass signature detection and improve infection performance. The criminal gang behind the enhanced CryptXXX ransomware have moved away from using the Angler exploit kit to the Neutrino EK. Researchers from SANS said that pseudo-Darkleech campaign began using Neutrino exploit kit (EK) to send CryptXXX ransomware this Monday. The researchers noted that up to this point the ransomware was only distributed using Angler. In a blog post, Brad Duncan, a handler and researcher at the SANS Internet Storm Center, said that while a malware campaign switching exploit kits was nothing new, this was the first time he has witnessed CryptXXX distributed by Neutrino. Why the hackers have changed tactics is anyone's guess. Angler samples containing CryptXXX haven't been detected in several days. He said that people can protect themselves from Neutrino EK by following best security practices (up-to-date applications, latest OS patches, software restriction policies, etc.). Gunter Ollmann, CSO at Vectra Networks, told SCMagazineUK.com that the change of exploit kit is likely driven by infection performance -- which would support the idea that additional AV products would be less capable of detecting the threat. "Anti-malware technologies that use static signatures will likely be slow to react to the change of threat vector and distribution -- which is why behavioral-based detection and machine learning approaches perform better at detection of this class of threat," he said. (scmagazine.com, 10Jun16)

(U) Crysis ransomware fills vacuum left by TeslaCrypt

(U) TeslaCrypt has reached the end of the road, and other ransomware is ready to fill the vacuum left behind it. A relative newcomer to the market, Crysis ransomware is already laying claim to parts of TeslaCrypt's territory. The Crysis ransomware family -- not to be confused with the Crisis backdoor/spyware Trojan that targeted both Windows and Mac users some four years ago -- is currently in its second iteration, and doesn't differ much from other similar malware. Its first version dates back to February 2016, and according to ESET researchers, victims hit with it have a decent chance of getting their files back without paying the attackers (the company offered their help). This latest version apparently uses strong encryption algorithms and a scheme that makes it difficult to crack in reasonable time. Crysis encrypts (RSA, AES encryption algorithm) every file it finds on fixed, removable and network drives, except Windows system files and its own files. It appends the .ID percentvariable percent. percentemail_address percent.xtbl extension to each of the encrypted files, and then drops the message for the victim, both in the form of a text file and desktop wallpaper: The victims are instructed to contact the crooks directly via one of the two offered email addresses, and they ask for 400 to 900 euros (in bitcoin) for the decryptor that will restore the encrypted files to their original form. "During our research we have seen different approaches to how the malware is spread. In most cases, Crysis ransomware files were distributed as attachments to spam emails, using double file extensions. Using this simple -- yet effective -- technique, executable files appear as non-executable," ESET researchers shared. "Another vector used by the attackers has been disguising malicious files as harmless looking installers for various legitimate applications, which they have been distributing via various online locations and shared networks". (helpnetsecurity.com, 10Jun16)

(U) Malicious macros in Office documents find new tricks to evade detection

(U) Malware coders are some of the most creative and talented programmers you'll find, and the speed at which malware keeps evolving stands as proof. One of the cases where this has been proven true once again is detailed by Zscaler, a San Jose-based security firm. While analyzing the most recent malware samples detected by their security software, the company's experts came across malicious Microsoft Office documents that employed macros with new social engineering tricks, but also new anti-analysis detection mechanisms. The cyber-criminals used highly obfuscated code for their malware, hoping to thwart the efforts put in by security experts who were taking a look at the macro's tangled source. This tactic had some of the desired effects, but Zscaler's team prevailed, and their efforts were rewarded. The security researchers managed to get a glimpse of the most recent tactics employed by malware coders to detect virtual machines and malware analysis products. While malware has been checking for VM environments for years, the way it does this has continually evolved, just like the malware's code. The malicious macros Zscaler stumbled upon used three older techniques to scan for VM and sandbox environments. The malware was checking for standard virtual environment strings, was employing the Windows Management Instrumentation (WMI) interface to identify virtual environment & automated analysis systems, and was using a static list of software pieces known to be used by security researchers. Besides these three, all known to most security researchers, Zscaler also discovered two new tricks. For the first one, the malware was looking at Office's list of Recently Opened Files. If the infected target had less than three files, the malware deemed it a test environment and stopped its execution. The second new check found in malicious macro scripts used Maxmind's GeoIP service. The malware was checking the user's IP address and was comparing the result to an internal list of known IPs belonging to security firms, data centers, or other malware analysis services. "This API asks for user credentials but we did not see any hardcoded credential information being sent by the malicious document," Zscaler's team notes. "We are still verifying if this is by design or if this is an authentication bypass issue for the API that is being exploited." If any of these checks fails, the macro script stops execution immediately, but if it succeeds, Zscaler says that crooks will download the Matsnu backdoor trojan on infected hosts, and sometimes later, the Nitol backdoor trojan, and the Nymaim ransomware. (Softpedia, 09Jun16)

OGA

Incidents of Interest:

OGA

(U) US company's China employee allegedly stole code to help local government

(U) The US has charged a Chinese national, Xu Jiaqiang, with economic espionage and theft of the source code of a clustered file system belonging to his former US employer, which he is alleged to have stolen for his own benefit and that of the National Health and Family Planning Commission in China. The charges against Xu highlight the intellectual property risks faced in other countries by development operations of US companies; particularly in those countries the US suspects could be involved in economic espionage. Xu, who was initially arrested by the Federal Bureau of Investigation in December and was charged with one count of theft of trade secrets, is scheduled to be arraigned on a superseding indictment of charges of economic espionage on Thursday in a federal court in New York, the Department of Justice said. The company whose source code he is alleged to have stolen has not been named in court filings or the DOJ statement, but a Reuters report said he was employed by IBM. LinkedIn lists a developer with the same name as employed with IBM in China during about the same period. Xu worked as a developer for the US company's branch in China from November 2010 to May 2014. He had full access to proprietary source code, including the ability to download it to a computer or storage device, according to the original complaint in December in the US District Court for the Southern District of New York. He resigned voluntarily in May 2014 and was allegedly caught trying to sell the code to US undercover agents, who claimed they were starting a large-data storage company. Xu told the agents in May 2015 that he would consider downloading the code to the new startup for testing its functionality if they would set up a small network of computers for the purpose. By August 2015, the files were remotely uploaded to the network set up the FBI agents and by the assessment of one of the "victim company's" employees appeared to contain a functioning copy of the proprietary software. On 7 December 2015, Xu met with one of the agents at an hotel in White Plains, New York, where he is alleged to have stated in "sum and substance," that he had used the proprietary source code to make software to sell to customers. Xu was arrested on 7 December by the FBI. The three counts of economic espionage each carry a maximum sentence of 15 years in prison while the three counts of theft, distribution and possession of trade secrets each have a maximum sentence of 10 years. The software is described as a key component of one of the world's largest scientific supercomputers and of commercial applications that require rapid access to large volumes of data, according to the original complaint. Xu is charged with the "intent to benefit" the Chinese agency but no specific charges relating to actual transfer of the code to the National Health and Family Planning Commission are mentioned in the superseding indictment. (IDG News Service, 14Jun16)

(U) Hacker puts 290,000 US driver's license records up for sale

(U) A hacker who uses the name of NSA has put up for sale on the Dark Web a dataset that contains the personal details and driver's license information of over 290,000 US citizens. The hacker discloses he stole the data after breaching the networks of several Louisiana organizations, and as such, most of the details are from Louisiana locals. NSA says he extracted the driver's license details from the stolen databases that contained information on driving violations. In some cases, he claims the databases also held information about more serious crimes, such as murders. The format of the leaked data, according to the hacker, is: driving offense, fine total, first name, middle name, last name, date of birth, driver's license number, state in which the driver's license was issued, address, city, state, ZIP code, phone number, and email address. The hacker said that the most common dates of birth are from 1983, but the data also includes information on teenagers and senior citizens. Additionally, information on non-Louisiana residents is also included, in smaller numbers, which the hacker attributes to travelers or tourists. The hacker's selling the data on the Dark Web marketplace named The Real Deal and is willing to negotiate with anyone who's interested in acquiring it. Because the hacker is selling the data via private ads, Softpedia has not been able to verify how many instances of the dataset have been sold. NSA has not responded to Softpedia's request for comment via his Jabber ID. (Softpedia, 12Jun16)

Items of Interest

(U) NATO adds cyber to operation areas

(U) NATO agreed Tuesday to make cyber operations part of its war domain, along with air, sea and land operations, and to beef up the defense of its computer networks. NATO Secretary-General Jens Stoltenberg said the decision to formally consider cyber operations a military domain is not aimed at any one country. He says the allies need to be able to better defend themselves and respond to attacks on their computer networks. The decision has been long in coming, particularly amid rising tensions with Russia, which has proven its willingness to launch computer-based attacks against other nations. About a year ago, US Defense Secretary Ash Carter told NATO that it must improve its ability to protect itself before it builds its cyberwar capabilities. And he pledged that the US would use its expertise to help allies assess their vulnerabilities and reduce the risk to their critical infrastructure. In 2014, after years of debate, NATO finally agreed that a cyberattack could rise to the level of a military assault and could trigger the Article 5 protections, which allow the alliance to go to the collective defense of another member that has been attacked. On Tuesday, Stoltenberg said that cyber must be a war domain, much like air, land and sea. He said the decision means that NATO will coordinate and organize efforts to protect against cyberattacks in a more efficient way. And he noted that any hybrid military attack would include cyber operations as a key dimension. (AP, 15Jun16)

(U) What the Joint Chiefs' email hack tells us about the DNC breach

(U) The Russian hacking groups that stole the Democratic National Committee's secret files on Donald Trump have plenty of experience in filching sensitive data from US officials. Last year, one of the two groups, known as APT29 or COZYBEAR, broke into the Joint Chief's non-classified email system. Here's what last summer's hack can teach us about what happened to the DNC. On Tuesday, officials with the information security company Crowdstrike disclosed that APT29 had injected malware onto the DNC network about a year ago, enabling the hackers to pick up opposition research on Donald Trump, among other information. The group is known for its spearphishing campaigns, which sends emails that appear to be from a trusted source. But when a recipient clicks on a link, the machine will download malicious code, in the case of the DNC hack, containing a Remote Access Tool (RAT). This code lets a hacker into the system -- and takes pains to keep itself hidden. The malware Crowdstrike discovered on the DNC network "allowed the adversary to launch malicious code automatically after a specified period of system uptime or on a specific schedule". Aside from the perpetrator, the DNC hack bares a number of things in common with the 2015 phishing attack on the Joint Chief's non-classified email system. Early last year, APT29 began using a backdoor malware dubbed HAMMERTOSS. Once an unsuspecting target opened an email from the group and downloaded the virus via a link, the malware installed itself and began using Microsoft Active Directory to move laterally among computers in the (Windows server) network. At specific times, the malware checked in with a web page to receive instructions on uploading data. In combination, these techniques make it particularly hard to identify HAMMERTOSS or spot malicious network traffic," wrote the computer security firm FireEye. But, while it took the DNC almost a year to realize it had been hacked, the Pentagon detected the breach of its non-classified network within days. Last August, Defense One interviewed the head of the company that the Pentagon trusted to detect and remedy the breach. He asked that his name and the name of the company not be disclosed as they have not received clearance to discuss their role in mitigating the hack. The incident was a key example of a new trend, he said. "When you typically see these large-scale attacks where you see these large amounts of lateral movement [jumping from one computer to another within the network] and especially when you have relatively tightly wound network controls, a lot of the time you don't have the command-and-control architecture to be able to go in and see the attack," he said. "So the advance threat characteristics change to be more automated, a kind of pervasive deployment using common vulnerabilities and exploiting them widely". That bears resemblance to what Crowdstrike just discovered APT29 doing to the DNC. (defenseone.com, 14Jun16)

(U) DOD to eliminate common access cards

(U) Department of Defense CIO Terry Halvorsen announced on 14 June that his agency will be eliminating common access cards for authenticating users on information systems. "We are embarking on a two-year plan to remove CAC cards from our information systems," he said at the Brocade Federal Forum in Washington DC. "Frankly, CAC cards are not agile enough to do what we want," he said. According to Halvorsen, the cards have too much overhead in terms of cost, time and location. It's difficult, for example, to get to one's CAC card to access a system when mortar shells are flying, he quipped. The plan is to use true multifactor authentication and some combination of behavioral or biometric information to allow users to access networks. Halvorsen was sure to clarify that DOD would not be eliminating Temporal Key Integrity Protocol, or TKI, an encryption protocol. Halvorsen also discussed data center consolidation, conceding that it's "no secret, we're behind in data center closures inside of DOD". He announced the establishment of a panel within DOD -- which will include some members of industry -- to look at the 50 most expensive data centers currently in operation and figure out which should be closed. Halvorsen called this an easy first step, noting that the harder step will be determining where the data housed in those closed centers will go. That, he said, will be an enterprise decision, not an individual element decision. (Government Computer News, 14Jun16)

(U) IARPA exploring deceptive cyber defenses

(U) Intelligence work is often as much about gathering information as it is about disseminating misinformation. To that end, the Intelligence Advanced Research Projects Activity (IARPA) is looking for innovative solutions around deceptive cyber defenses. In a request for information issued 6 June, IARPA contracting officers put out the call to "identify existing capabilities and emerging methods" for protecting data and systems by confusing and otherwise deceiving the adversary prior to and during a cyberattack. "Historically, denial and deception (D&D) has been used by militaries for defense, whether it is to instill uncertainty or to provide misinformation," contracting officials explain in the RFI. "D&D can also be looked at similarly for increasing cyber defense posture and resiliency." In the RFI, IARPA notes this concept is gaining traction in the private sector but has yet to really mature. "Many techniques lack rigorous experimental measures of effectiveness, information is insufficient to determine how defensive deception changes attacker behavior or how deception increases the likeliness of early detection of a cyberattack," according to the notice. Specifically, IARPA is looking for feedback on existing deception methods, test and evaluation methods, emerging techniques and information on the respondent company's organizational structure and service offerings. Responses to the RFI are due by 1 p.m. on 1 July. -- federaltimes.com. (IDC News Service, 13Jun16)

(U) Computer crash wipes out years of Air Force investigation records

(U) The US Air Force has lost records concerning 100,000 investigations into everything from workplace disputes to fraud. A database that hosts files from the Air Force's inspector general and legislative liaison divisions became corrupted last month, destroying data created between 2004 and now, service officials said. Neither the Air Force nor Lockheed Martin, the defense firm that runs the database, could say why it became corrupted or whether they'll be able to recover the information. Lockheed tried to recover the information for two weeks before notifying the Air Force, according to a service statement. The Air Force has begun asking for assistance from cybersecurity professionals at the Pentagon as well as from private contractors. For now, Air Force officials don't believe the crash was caused intentionally. Lockheed declined to answer specific questions about the incident. "We are aware of the data corruption issue in the Air Force's Automated Case Tracking System (ACTS) and are working with the Air Force to identify the cause, and restore the lost data," Maureen Schumann, a company spokeswoman, said in an email. The Air Force inspector general is an independent organization that reports directly to Air Force Secretary Deborah Lee James and Gen. Mark Welsh, the Air Force chief of staff. The office investigates claims of waste, fraud, and abuse within the service. Ann Stefanek, an Air Force spokeswoman at the Pentagon said the ACTS system contains all sorts of personal information, such as complaints, the findings of an investigation, and any actions taken. The database also contains records of congressional and constituent inquiries. The data lost dates back to 2004. Data about current investigations has also been lost, which is delaying them. "The Air Force is assessing the immediate impact of the data loss, but at this time we are experiencing significant delays in the processing of inspector general and congressional constituency inquiries," the service said in a statement. It's possible that some data is backed up at local bases where investigations originated. (defenseone.com, 13Jun16)

(U) Intel looks at stopping hackers and malware at the processor level

(U) Plans are being hatched to prevent return-oriented programming attacks on memory flaws Intel is looking at introducing security features at the chip level in order to prevent hackers from using return-oriented programming to take advantage of memory vulnerabilities. The chip firm has worked with Microsoft on Control-flow Enforcement Technology (CET) which should stymie attempts by criminals to use techniques such as return-oriented programming (ROP) and jump-oriented programming (JOP). ROP attacks can exploit memory flaws to install malware, despite mitigations such as data-execution prevention (DEP), and address-space layout randomization (ASLR). CET works by using what is known as a shadow stack. This is a second stack which stores control transfer operations. With CET, return addresses get copied to the normal stack and shadow stack. The shadow stack is isolated and tamper-proof. CET compares return addresses with those stored in the shadow stack. If the two don't match up, a red flag is raised. Patel said that the specification is the result of many years of research carried out by Intel and Microsoft in finding a way to stop ROP/JOP attacks. "We also wanted to make sure that the solution is applicable to not just applications, but also to operating system kernels, and is beneficial to software written using most programming languages. We also wanted to ensure that software enabled for CET works on legacy platforms without changes, albeit with no security benefits. Finally, and most importantly, we wanted to address all known ROP/JOP attacks," said Patel. CET is currently in the process of being reviewed and more work is needed to be done. (scmagazine.com, 13Jun16)

(U) IETF proposal details using cookies as anti-DDoS protection in DNS protocol

(U) A proposal submitted to the Internet Engineering Task Force (IETF) details Domain Name System (DNS) Cookies, an extra security layer to the DNS protocol. The security measures included in the RFC 7873 proposal describe a system named DNS Cookies, which are 64-bit keys generated on the client-side to authenticate the user on the server-side. Servers will be able to verify a client's origin based on the 64-bit key, which will be calculated based on each user's IP address, the DNS server IP address, and a client secret. According to Donald Eastlake of Huawei and Mark Andrews of ISC, deploying DNS Cookies will make it harder for attackers to spoof DNS requests because they'll have to supply a correctly-calculated 64-bit key. DNS has been a popular protocol for launching DDoS attacks, and more precisely, reflection DDoS attacks. In the first three months of the year, according to Akamai, DNS has been the second most popular protocol used for reflection DDoS attacks after NTP. DNS Cookies will allow a server to detect the authenticity of incoming DNS requests and drop all packets that don't have a proper 64-bit key. RFC 7873 will also help protect servers against simple DoS attacks as well. These are cases where an attacker sends a massive number of DNS requests to the server in order to make it use all of its resources. Attackers usually spoof their malicious DNS requests with multiple IP addresses in order to avoid getting the real source of their attack blacklisted (their own IP). DNS Cookies, once again, makes it easier to reject all spoofed traffic. Additionally, DNS cache poisoning can also be thwarted by DNS cookies, Eastlake and Andrews claim. The two also say that existing DNS security systems such as DNSSEC and DNS Message/Transaction Security "do not provide the services provided by the DNS Cookie mechanism: lightweight message authentication of DNS requests and responses with no requirement for pre-configuration or per-client server-side state." Both DNSSEC and DNS Message/Transaction Security (TSIG) are notoriously difficult to set up, especially TSIG, which needs pre-agreement and key distribution between client and server, keeping track of server-side key state, and required time synchronization between client and server. RFC (Request For Comment) 7873 proposal is currently under public debate and IETF awaits everyone's input before moving forward into making this an official spec. (Softpedia, 10Jun16)

(U) $1.8B approved for DHS cybersecurity efforts

(U) The Department of Homeland Security (DHS) received a $1.8B infusion aimed at protecting against cyberattacks and safeguarding critical infrastructure, according to The Hill. On Thursday, The House Appropriations Subcommittee on Homeland Security unanimously approved a spending bill providing the funds -- $120.5 million above its budget for 2016 -- earmarked for the National Protection and Programs Directorate (NPPD), the DHS sector in charge of protecting and enhancing the nation's physical and cyber infrastructure. "Hacking and cyberattacks have already cost the federal government billions of taxpayer dollars, and have exposed the personal information of thousands of Americans," the committee reportedly stated. Most of the funds are allocated for civilian government networks (.gov sites), mitigating foreign incursions and upgrading emergency communications. Additional funds will also be assisting in the cybercrime efforts of Immigration and Customs Enforcement and the Secret Service. (scmagazine.com, 10Jun16)

(U) US Homeland Security could get its own cyber defense agency

(U) A panel of House lawmakers wants to turn the existing National Protection and Programs Directorate into the Cybersecurity and Infrastructure Protection Agency. A key House panel on Wednesday voted to create a new Homeland Security Department agency that reflects the primacy of cyber protection among DHS' protective responsibilities. A bill introduced yesterday by the Homeland Security Committee -- approved by a voice vote -- would turn an existing DHS bureaucracy, the National Protection and Programs Directorate, or NPPD, into an "operational" agency, like the Transportation Security Administration. The directorate would be renamed the Cybersecurity and Infrastructure Protection Agency. It is expected the overhaul would take effect under the next White House administration in 2017. This measure "realigns and streamlines the department's cybersecurity and infrastructure protection missions to more effectively protect the American public against cyberattacks that could cripple the nation," committee Chairman Michael McCaul, R-Texas, said. The Cybersecurity Act of 2015 enacted a controversial program that encourages companies to share hack data -- including private citizens' information -- with the federal government. In February, DHS officials also had proposed a realignment of the directorate, but their plan would have merged cyber operations with other NPPD activities. The House plan keeps intact divisions between cybersecurity, the protection of critical infrastructure like the power grid, emergency communications and the existing Federal Protective Service. The agency's units would coordinate through working groups and integrated risk assessments, under the committee's legislation. In March, current NPPD Undersecretary Suzanne Spaulding characterized the administration's proposed merger as recognition that our digital lives and personal safety are now intertwined. Spaulding, at the time, said DHS is "uniquely restricted" in its ability to reorganize, as compared to most federal agencies; Congress must pass a law to authorize office name and structural changes. In addition to rechristening NPPD as CIPA, the House bill would shuffle management duties. The directorate's leader, now Spaulding, would be renamed the "director" of the agency. The head of the current cyber division, presently Deputy Undersecretary Phyllis Schneck, would become an assistant secretary-level position, like the role currently held by Andy Ozment. Essentially, there would be a single cyber lead, who would be called the "principal deputy director" for cybersecurity. A separate agency "assistant director" would oversee the information-sharing program, which is run out of the 24-7 DHS National Cybersecurity and Communications Integration Center. House committee leaders are collaborating with their counterparts on the Senate Homeland Security and Governmental Affairs Committee to craft an agreement, a House staffer said. (defenseone.com, 08Jun16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424