[redacted] Cyber-Threat Newsletter – 19 Aug 16 (b)(3) 10 USC 424

Patches & Updates of the Week:

(U) Microsoft stops Windows 7 and 8.1 users picking and choosing updates
(U) In May, Microsoft introduced a Convenience Rollup for Windows 7 SP1 that brought the operating system fully up to date. The company also announced that it would be issuing monthly update rollups for Windows 7 and 8.1, as well as Windows Server 2008 R2 SP1, Windows Server 2012 and Windows Server 2012 R2. Those rollups only contained non-security updates, so you could still choose which security patches to apply, which to avoid, and when to apply them. Not anymore. Based on user feedback -- Microsoft claims -- from October onwards, the software giant will be releasing a single Monthly Rollup that contains both security and reliability fixes in a single update. Microsoft says: 'By moving to a rollup model, we bring a more consistent and simplified servicing experience to Windows 7 SP1 and 8.1, so that all supported versions of Windows follow a similar update servicing model. The new rollup model gives you fewer updates to manage, greater predictability, and higher quality updates. The outcome increases Windows operating system reliability, by eliminating update fragmentation and providing more proactive patches for known issues. Getting and staying current will also be easier with only one rollup update required. Rollups enable you to bring your systems up to date with fewer updates, and will minimize administrative overhead to install a large number of updates.' Several update types aren't included in a rollup, such as those for Servicing Stack and Adobe Flash. The rollup will be cumulative, so if you skip or miss the October rollup, the November one that replaces it will have all the October updates, as well as the latest ones. If you don't want to install that rollup, there will be another option as Microsoft is planning to release a single monthly security-only update. This will contain all of the security patches for that particular month (none from previous months). Unlike the Monthly Rollup, this won't be available through Windows Update -- you'll need to get it from WSUS, SCCM, or the Microsoft Update Catalog. There will also be a .NET Framework Monthly Rollup. As to the reason for this latest change, it's simple really. Microsoft says: 'Historically, we have released individual patches for these platforms, which allowed you to be selective with the updates you deployed. This resulted in fragmentation where different PCs could have a different set of updates installed leading to multiple potential problems'. (BetaNews, 16Aug16)

Threats & Vulnerabilities of the Week:

(U) Industrial espionage hackers targeted companies in more than 130 countries
(U) Since March 2015, a well-organized cyber-crime syndicate has targeted more than 130 companies in over 30 countries for the purpose of industrial espionage. The vast majority of the victims are small to medium companies (30-300 employees) activating in the industrial sector. The majority of targeted companies activate in industrial sectors such as the petrochemical field, naval, military, aerospace, heavy machinery, solar energy, steel, pumps, and plastics. Other activity sectors were also targeted, such as engineering, shipping, pharmaceutical, manufacturing, trading, education, tourism, IT, and more. The group has shown a narrow focus on companies activating in the industrial sector, but not specific to one country. Attacks were scattered all over the globe, with the most recorded in Spain (25 incidents), Pakistan (22), the United Arab Emirates (19), India (17), Egypt (16), and more. Other targeted countries include the UK, Germany, South Africa, Portugal, Qatar, Switzerland, Gibraltar, USA, Sweden, China, France, Azerbaijan, Iraq, Turkey, Romania, Iran, Iraq, and Italy. Ghoul hackers used the HawkEye RAT (Remote Access Trojan), also known as KeyBase, to carry out their attacks. The crooks packed their RAT inside an EXE file, which they put inside a ZIP file and sent via spear-phishing emails to high-ranking persons in the targeted companies. The RAT is one of the top remote access toolkits on the market and can steal clipboard data, keystrokes, license information from installed applications, and passwords from several apps such as browsers, FTP, and email clients. For these attacks, HawkEye collected the data from targets and sent it via HTTP, unencrypted, to one of two servers. Kaspersky says these two servers belonged to two legitimate businesses that were compromised in the past. (Softpedia, 17Aug16)

(U) Backdoor trojan uses TeamViewer components to spy on PCs in Europe, Russia, and US
(U) A new trojan called BackDoor.TeamViewerENT.1 is using parts of the legitimate TeamViewer application to allow crooks to spy on infected systems. The concept is not new by any means, and crooks employed TeamViewer in the past, when they packaged the legitimate app alongside their malware and used it to transform the user's PC into a web proxy. That particular trojan, BackDoor.TeamViewer.49, did not allow the crooks to steal anything, only to spy on traffic, but this newer variant does, according to Dr.Web security researchers. In fact, the two variants seem to be related because they both use stripped-down versions of the TeamViewer application, where they replace the avicap32.dll file with a malicious version that loads trojan's malicious features. The infection process revolves around users installing applications, where the stripped-down TeamViewer version is also installed without their knowledge. Whenever this modified TeamViewer version starts, the avicap32.dll is loaded by default, being a must-run DLL. Crooks modified this DLL to include the BackDoor.TeamViewerENT trojan, which gets loaded into the computer's memory, without needing any files on disk to function. This fileless operation mode makes antivirus detection harder. The modified DLL also contains functions to suppress any TeamViewer error messages, a functionality included to avoid giving away the trojan's presence. Another odd feature is that, whenever the user starts the Windows Task Manager or Process Explorer apps, the trojan automatically shuts down (the parent TeamViewer process) to avoid getting seen by the victim in the process list. After this, BackDoor.TeamViewerENT.1 begins to behave like a regular backdoor. It starts communicating with its C&C server, from where it receives various types of commands. The trojan includes the ability to restart or turn off the computer, remove or relaunch its parent TeamViewer process, listen to conversations via the microphone, access the webcam, download and execute files, run command-line instructions, or connect to specified remote servers. During their investigation, security researchers found the trojan was very active, especially targeting Russian users, but also users in the UK, Spain, and the US. Attackers switched focus to US targets in August, says the security vendor. (Softpedia, 16Aug16)

(U) UAC vulnerability in Windows 7 and Windows 10 allows for traceless code execution

(U) Windows' User Account Control (UAC) feature was designed to help keep computers safe from malicious software installations, but there are already at least a couple of ways to bypass it. A new technique for circumventing UAC not only makes it possible to execute commands on a computer, but to do so without leaving a single trace. Security researchers Matt Nelson and Matt Graeber discovered the vulnerability and developed a proof-of-concept exploit. The pair tested the exploit on Windows 7 and Windows 10, but say that the technique can be used to bypass security on any version of Windows that uses UAC. While the vulnerability does require an attacker to already have access to a computer in order to exploit it, it is a concern nonetheless. Speaking to Threatpost, Nelson said: "This attack simply allows an admin user to execute code in a high-integrity context without requiring the user to 'approve' the administrative action via the pop-up. It essentially removes the restrictions an attacker has when running under the context of a local administrator". The attack -- which is detailed on Nelson's website -- makes use of the Event Viewer (eventvwr.exe) to hijack a registry process to launch Powershell. This can then be used to execute arbitrary code. The researcher says that he has informed Microsoft about the vulnerability but was told that UAC bypasses are not considered important enough to warrant a Patch Tuesday fix. In a statement Microsoft said: This particular technique can be remediated or fixed by setting the UAC level to "Always Notify" or by removing the current user from the Local Administrators group. Further, if you would like to monitor for this attack, you could utilize methods/signatures to look for and alert on new registry entries in HKCU\Software\Classes\. (BetaNews, 16Aug16)

(U) Chrome and Firefox affected by simple URL spoofing bug

(U) Security researcher Rafay Baloch has discovered a simple way to defeat several browser security features and spoof URLs in the browser address bar using a very, very simple trick. At the time of writing, Google and Mozilla have fixed the issue, but Baloch says that other vendors are still working on getting this corrected. The researcher also reveals he received a $5,000 reward from Google for his bug report. In a very simplistic explanation of the issue, the problem relies on how the browsers align URLs written with mixed RTL (Arabic) and LTR (Roman) characters. According to Balock, several browsers get confused and end up switching parts of the URL, tricking the user into thinking they're accessing a different site than the one they're really on. A hacker running a phishing site can take the server's IP, add one of few Arabic characters that trigger this behavior in the middle of the URL construction, and append the domain of a legitimate website at the end. They can then embed this URL in spam email, SMS, or IM messages, and when the user clicks on it, they'll end up on a page that shows a URL starting with a valid domain, but in reality, they'd be on the crook's server. Users should update their browsers to the latest versions to avoid being exposed to this security bug. (Softpedia, 16Aug16)

(U) Ransomware-as-a-service tool generates $195,000 profit in July

(U) There are a number of high profile ransomware programs doing the rounds at the moment and we know that it can generate lucrative returns for the people behind it. But just as in the legitimate commercial world, the as-a-service model is starting to gain traction with attackers. Security vendor Check Point is releasing details of Cerber, which it believes is the world's biggest ransomware-as-a-service scheme. Cerber operates as a franchise, with its developer recruiting affiliates who then spread the malware further for a cut of the profits. In July 2016 alone, Cerber had over 160 active campaigns, targeting 150,000 users in 201 countries and generating profits of $195,000 during the month. Cerber is believed to originate from Russia and, in the spirit of not fouling its own nest, actively does not infect targets in 12 former Soviet Union countries. Cerber is built to enable non-technical criminals to take part in the highly profitable ransomware business and run independent campaigns, using a set of command and control servers and an easy-to-use control interface that's available in 12 different languages. The malware creates a unique BitCoin wallet for each of its victims. When the ransom (usually one BitCoin, currently worth $590) is paid, the victim receives the decryption key. The BitCoin is then transferred to the malware developer and affiliates by flowing through thousands of BitCoin wallets, making individual payments practically untraceable. "This research provides a rare look at the nature and global targets of the growing ransomware-as-a-service industry," says Maya Horowitz, group manager, research and development at Check Point. More detail on Cerber is available on the Check Point website and the company has also released a free decryption tool to allow users to recover files that have been encrypted by Cerber. (BetaNews, 16Aug16)

(U) FalseCONNECT vulnerability affects software from Apple, Microsoft, Oracle, and more

(U) Researcher Jerry Decime has revealed details about a security vulnerability that allows an attacker to gain a Man-in-the-Middle position and intercept HTTPS traffic thanks to flaws in the implementation of proxy authentication procedures in various products. According to Decime, there is a flaw in how applications from several vendors respond to HTTP CONNECT requests via HTTP/1.0 407 Proxy Authentication Required responses. This flaw manifests itself only in network environments where users utilize proxy connections to get online. This type of setup is often used in enterprise networks where companies deploy powerful firewalls. Decime explains that an attacker that has a foothold in a compromised network and has the ability to listen to proxy traffic can sniff for HTTP CONNECT requests sent to the local proxy. When the attacker detects one of these requests, they reply instead of the real proxy server and issue a 407 Proxy Authentication Required response, asking the user for a password to access a specific service. Because the HTTP CONNECT requests are unencrypted, the attacker knows when the victim wants to access sensitive accounts such as email or Intranet servers, even if those services are delivered via HTTPS. The attacker can force the user to authenticate, sending the responses to them instead, hence the vulnerability's name of FalseCONNECT. "WebKit-based clients are vulnerable to additional vectors due to the fact that HTML markup and JavaScript are rendered by the client Document Object Model (DOM) in the context of the originally requested HTTPS domain," a US-CERT alert reads. WebKit is used for software such as Chrome, iTunes, Google Drive, Safari, and many mobile applications. Multiple software vendors deploy applications that can handle proxy connections. Until now, Apple, Microsoft, Oracle, and Opera have acknowledged their products are affected. Lenovo has said this bug does not impact its software. Other software vendors that are still evaluating the FalseCONNECT bug and may be affected include multiple Linux distros, Cisco, Google, HP, IBM, Juniper, Mozilla, Nokia, OpenBSD, SAP, Sony, and others. (Softpedia, 16Aug16)

(U) Hacking group claims to offer cyber-weapons in online auction

(U) Hackers going by the name Shadow Brokers said on Monday they will auction stolen surveillance tools they say were used by a cyber group linked to the US National Security Agency. To arouse interest in the auction, the hackers released samples of programs they said could break into popular firewall software made by companies including Cisco Systems Inc, Juniper Networks Inc and Fortinet Inc. The companies did not respond to request for comment, nor did the NSA. Writing in imperfect English, the Shadow Brokers promised in postings on a Tumblr blog that the auctioned material would contain "cyber weapons" developed by the Equation Group, a hacking group that cyber security experts widely believe to be an arm of the NSA. The Shadow Brokers said the programs they will auction will be "better than Stuxnet," a malicious computer worm widely attributed to the United States and Israel that sabotaged Iran's nuclear program. Reuters could not contact the Shadow Brokers or verify their assertions. Some experts who looked at the samples posted on Tumblr said they included programs that had previously been described and therefore were unlikely to cause major damage. "The data [released so far] appears to be relatively old; some of the programs have already been known for years," said researcher Claudio Guarnieri, and are unlikely "to cause any significant operational damage". Still, they appeared to be genuine tools that might work if flaws have not been addressed. Other security experts warned the posting could prove to be a hoax. The group said interested parties had to send funds in advance of winning the auction via Bitcoin currency and would not get their money back if they lost. The auction will end at an unspecified time, Shadow Brokers said, encouraging bidders to "keep bidding until we announce winner". (Reuters, 15Aug16)

(U) New Windows trojan steals enterprise data and Microsoft Office files

(U) Threat actors are circulating a new type of infostealer trojan that will search for eleven file types and upload them to a C&C server. The files it targets are specific to enterprise environments, being mostly extensions associated with Microsoft Office applications. Based on a sample of the trojan, crooks are distributing this threat as a file named Aug_1st_java.exe, which currently has a very low detection rate on VirusTotal, 34/55. The distribution method is currently unknown, and it could be either via spam or via watering hole attacks. As is the case with almost all malware programs today, when users install this trojan, it will modify the Windows Registry to gain the ability to start automatically after the user reboots their computer. Current versions of this yet unnamed infostealer trojan disguise themselves as the process of the Google Chrome browser. Right after it is installed, the trojan will collect data about the current computer and direct it to its C&C server, to which it sends communications via the MSMQ (Windows Message Queuing) protocol. The data gathered includes the computer's name, the username, the version of Windows, the service pack version, and a list of currently installed applications. The C&C server is located at web4solution.net. When contacting the company in charge of the domain, it came to light that their site had been compromised and loading a hidden iframe that relayed traffic to the real C&C server. The company cleaned their site, but the C&C server remained active and will continue to work, presumably with another redirect through another hacked website. After the trojan reports to the C&C server, its malicious operations don't stop here, and it will start scanning the infected computer for eleven file types: INP, SQL, PDF, RTF, TXT, XLSX, XLS, PPTX, PPT, DOCX, and DOC. The trojan will upload all the files with these extensions to its C&C server and then write a log at C: Users [username] uninst.dll. (Softpedia, 13Aug16)

(U) DiskFiltration attack steals data via HDD sounds

(U) DiskFiltration is the name of a new attack devised by researchers from the Ben-Gurion University in Israel that records and interprets the sounds made by a computer's hard drive. The new attack is meant to be used to steal data from air-gapped systems that can't be reached via the Internet. The presence of a malicious insider is still required in order to install malware on the target PC and to place a smartphone or microphone that records the sounds emanated by the computer's hard disk drive (HDD). The technique doesn't work with the regular HDD sounds that come from read-write operations, but only from moving the HDD laser head (actuator) to specific positions, in an operation called "seeking". The malware's role is to gather data from the infected target, such as cryptographic keys, passwords, or other information, and then move the HDD actuator in order to produce mechanical sounds. The wavelengths of the produced sounds are meant to represent 1s and 0s in binary language. The nearby recording device, which can be a smartwatch, laptop, mobile phone, or any other device with audio-recording features, will save the data or send it to the attacker. Because of its mode of operation, the attack only works on classic HDD, and not on newer storage drives based on SSD and SSHD technologies, which don't rely on disk plates and disk reading heads. The other downside is that because data is sent out as 1s and 0s, it takes a considerable amount of time to relay even basic details such as a password. According to the researchers, the DiskFiltration attack can send 180 bits/minute and to a distance of up to two meters (six feet). As such, DiskFiltration is nothing more than a theoretical attack, with little applicability in the real world. (Softpedia, 12Aug16)

(U) New hacking technique imperceptibly changes memory virtual servers

(U) For the first time ever a team of Dutch hacking experts, led by cyber security professor Herbert Bos at Vrije Universiteit Amsterdam, managed to alter the memory of virtual machines in the cloud without a software bug, using a new attack technique. It's a new deduplication-based attack in which data can not only be viewed and leaked, but also modified using a hardware glitch. By doing so the attacker can order the server to install malicious and unwanted software or allow logins by unauthorized persons. With the new attack technique Flip Feng Shui (FSS), an attacker rents a virtual machine on the same host as the victim. This can be done by renting many virtual machines until one of them lands next to the victim. A virtual machine in the cloud is often used to run applications, test new software, or run a website. There are public (for everyone), community (for a select group) and private (for one organization accessible) clouds. The attacker writes a memory page that he knows exists in the victim on the vulnerable memory location and lets it deduplicate. As a result, the identical pages will be merged into one in order to save space (the information is, after all, the same). That page is stored in the same part of the memory of the physical computer. The attacker can now modify the information in the general memory of the computer. This can be done by triggering a hardware bug dubbed Rowhammer, which causes flip bits from 0 to 1 or vice versa, to seek out the vulnerable memory cells and change them. The researchers of the Vrije Universiteit Amsterdam, who worked together with a researcher from the Catholic University of Leuven, describe in their research two attacks on the operating systems Debian and Ubuntu. The first FFS attack gained access to the virtual machines through weakening OpenSSH public keys. Debian, Ubuntu, OpenSSH and other companies included in the research were notified before the publication and all have responded. The National Cyber Security Center (NSCS) of the Dutch government has issued a fact sheet containing information and advice on FFS. The researchers presented their findings this week during the UNESIX Security Symposium 2016 in the United States. (Vrije Universiteit Amsterdam, 11Aug16)

(U) Shade ransomware adds RAT features to spy on high-value victims

(U) The crooks behind the most recent versions of Shade have added an interesting new tidbit to their malware, installing a modified version of TeamViewer on infected systems so they could spy on their targets and adjust the ransom note accordingly. This new Shade version only targets Russian companies that are running accounting software on their computers. Kaspersky researchers say that this new Shade version, prior to infecting the target, during its installation routine, actively scans the computer name for strings such as "BUH," "BUGAL," "???," "?????". These strings are likely to be found on computers used by the accounting departments at Russian-speaking companies. If Shade finds any of these strings, it stops the ransomware installation process and delivers another trojan called Teamspy, also known TVSPY, TVRAT, or SpY-Agent. The trojan contains a modified version of TeamViewer 6 that the malware authors have altered to hide its GUI. The trojan also includes the legitimate 7Zip archiving tool and the NirCmd command-line utility. Furthermore, the crooks are also installing the TeamViewer VPN driver and the RDP Wrapper Library, used to open VPN connections and interact with the RDP protocol. Kaspersky suggests that the crooks are using Teamspy's RAT (Remote Access Trojan) features to gather intelligence on the infected computer, to determine the appropriate ransom sum. Teamspy is quite a powerful RAT and allows a crook to record audio from infected systems, record the victim's desktop, run terminal commands, and download and install other executables. This last feature is most likely used to deliver the Shade ransomware at a later point in time, after crooks deemed the target important and decided on the ransom amount. Shade is one of today's most popular ransomware families, but Kaspersky researchers cracked its encryption and have provided a free decrypter via the No More Ransom initiative. Another name for the Shade ransomware is Troldesh. (Softpedia, 11Aug16)

(U) Chrome, Firefox, and IE browser hijacker distributed via legitimate software

(U) Intel McAfee security experts have discovered that the latest versions of the infamous Bing.vc browser-hijacking malware are distributed via applications distributed by Lavians Inc. Security companies have known about the existence of the Bing.vc malware for more than a year and many of them have added support for removing this threat from the computers of infected users. According to a report from McAfee, recent versions of the Bing.vc malware have been found bundled with legitimate-looking products. The security vendor is pointing the finger at a software company called Lavians Inc. "We have come across several files from Lavians Inc. that look like legitimate applications but may pose a serious risk," writes Intel's Santosh Revankar. "We have observed that Lavians Inc. is repackaging clean applications with a browser hijacker to avoid suspicion and to increase its outreach". Intel says that most of the infected files hide as driver utilities, using names such as HP DESKJET F4580 Driver Utility Setup, DELL Inspiron 5100 Drivers Utility Setup, or Acer Aspire ONE ZG5 Drivers Utility Setup. When users install these files, they'll get the legitimate application, but also Bing.vc, hidden inside a file called IconOverlayEx.dll. Bing.vc will install itself into Chrome, Firefox, and Internet Explorer, and will take over the site's homepage and insert ads into visited websites. The page to which this browser hijacker will redirect all users is Bing.vc, hence the malware's name. This website has nothing to do with Microsoft's Bing service and is quite strange that Microsoft hasn't registered the domain beforehand, or moved to take it down by now. Ironically, the Intel McAfee team has noticed that a link on this hijacked homepage leads users to a site that tries to sell them a very expensive utility to fix their browser hijacking problem. Users that notice something strange and move to uninstall the original driver utility they installed will find that all files will be removed, except IconOverlayEx.dll, which will remain on the infected system. During the uninstall routine, Bing.vc will alter the user's PC registry keys and add two new entries that will load the DLL on every boot-up. By doing so, even after uninstalling the original infected files, Bing.vc remains on the system. Users that want to get rid of this infection have to remove the registry keys by hand or use an automated PC clean-up utility that usually comes with antivirus software. (Softpedia, 10Aug16)

Incidents of Interest:

OGA

[redacted]

(U) Malware hits 20 major hotels

(U) As many as 20 hotels in the US have been hit by malware, and fears are spreading that customer data, including credit card information, was stolen. According to a Reuters report, hotels under attack include Starwood, Marriott, Hyatt and Intercontinental -- all part of the HEI Hotels & Restaurants. The malware was developed specifically to target it and collect credit card data from its systems. The malware was found two months ago, on payment systems used all over these hotels -- in restaurants, bars, lobbies, and spas. The number of people affected is hard to estimate, as many people used their credit cards more than once. However, there were some 8,000 transactions at the Hyatt Centric Santa Barbara hotel in California, as well as 12,800 at the IHG Intercontinental in Tampa, Florida, during this period. A total of 12 Starwood hotels were affected, six Marriott International's, one Hyatt Hotel and one InterContinental Hotels Group, with the malware being in operation from 1 March 2015, to 21 June 2016. Fourteen hotels were infected during December last year. Federal authorities have been notified, and a new payment system installed. (BetaNews, 16Aug16)

(U) WikiLeaks published a bunch of malware together with the Turkey AKP emails

(U) The WikiLeaks dump of emails stolen from the server of AKP, Turkey's ruling party, contains hundreds of links to downloadable malware, Bulgarian security researcher Vesselin Bontchev has discovered. The researcher, who works at the National Laboratory of Computer Virology at the Bulgarian Academy of Sciences in Sofia, Bulgaria, has created a script that parsed the WikiLeaks AKP email data dump for links and sent them for scanning via VirusTotal's API. Bontchev initially discovered around 80 links pointing to malware downloads, which he presented in a report he later amended and now lists 323 samples. The links Bontchev's script scanned are contained in the emails AKP party members have received and were later stolen by a hacker called Phineas Fisher. Most of these are spear-phishing emails, often pointing to RATs (Remote Access Trojans), but most of the time to ordinary malware such as malware droppers, password stealers, and ransomware. Bontchev's report includes the WikiLeaks ID, the link of the malicious attachment, and a link to a VirusTotal report. The researcher also says that he initially didn't scan the files found in the spam folders. A subsequent scan revealed over 962 malicious attachments and 2,093 if including duplicate emails. More surprising is that the researchers scanned only for emails containing file attachments in the form of DOCM files. The total number of malware links included in the WikiLeaks AKP dump is most likely much, much larger. The danger is that reporters and investigators looking into the AKP emails might download malware that infects their computers. Since mid-July, after it dumped the AKP emails and the DNC hack files, WikiLeaks has been under heavy criticism because of the unprofessional way it handled these files. First, the hacker who broke into the AKP email servers to steal the data accused WikiLeaks of rushing to dump the files, even if he was not yet ready to do so and was still inside the AKP servers. After the AKP dump was published, WikiLeaks came under heavy fire from women's rights groups who accused the organization of not taking the time to screen the files for personal data. Many high-profile figures, such as Zeynep Tufecki, a US citizen of Turkish origins, revealed that WikiLeaks had published the personal information on all Turkish women voters from 79 out of the 81 Turkish provinces. Tufecki argued that these women may now be in danger from extreme Islamist groups who think women should not be allowed to drive, let alone vote. But the WikiLeaks criticism didn't stop here. A week later, after the organization leaked the data stolen by Guccifer 2.0 in the DNC hack, US privacy organizations pointed out that WikiLeaks, once again, had not sanitized the data, which contained a plethora of personal information from US and foreign citizens who had donated funds to the Democratic Party. Criticism is mounting against WikiLeaks from all sides, as the organization seems to have turned into a run-of-the-mill data dump site, instead of an organization with a higher purpose. (Softpedia, 16Aug16)

(U) RT besieged by DDoS attacks after US think tank called for cyber terrorism

(U) Hackers bombarded RT with a well-planned series of Distributed Denial of Service (DDoS) attacks one week after the Atlantic Council wrote an article suggesting preemptive cyber terrorism against RT and the Moscow Metro. Last week the influential Atlantic Council led by President Obama's former Ambassador to Singapore and failed 2012 Republican candidate Jon Huntsman released a paper contemplating preemptive cyber attacks against the Russian infrastructure and RT's offices. This week, RT was the target of the exact type of cyber terrorism that was postulated in the article creating cause for concern. RT's systems have been bombarded throughout the week by a "particularly well-planned series of Distributed Denial of Service (DDoS) attacks that continued into early Friday" the outlet said in an article. The attacks targeted the station's data centers and internet provider in the US, Europe and Russia. The attack, which if conducted by a government would amount to an instance of censorship, caused repeated disruptions for RT.com visitors forcing the station to undertake necessary actions to prevent further attacks. According to RT's IT specialists, "the attackers were trying to overwhelm to provider's capacity." The attacks, according to IT experts, all originate from the same source as is established by the tactics and code signature used by the attackers. The hackers were deemed to be sophisticated selecting precise targets in order to create maximum disruption. "It looks like the attackers are continuously studying the company's outer network infrastructure and its security mechanisms. The cyberattacks that we are seeing are not the most powerful, but they are different from hundreds of others in their cunning methods and analysis -- they are looking at how we will react or how we switch the traffic," explained RT's Head of Interactive Projects Elvira Chudnovskaya. The attacks on the RT system are the most substantial in years with comparable attacks striking RT.com in February 2012 and in August 2012. The hacker group AntiLeaks, which opposed Julian Assange's WikiLeaks, took responsibility for those two prior attacks. (Sputnik, 15Aug16)

Items of Interest

(U) US offers states help to fight election hacking

(U) The government is offering to help states protect the 8 November US election from hacking or other tampering, in the face of allegations by Republican Party presidential candidate Donald Trump that the system is open to fraud. Homeland Security Secretary Jeh Johnson told state officials in a phone call on Monday that federal cyber security experts could scan for vulnerabilities in voting systems and provide other resources to help protect against infiltration, his office said in a statement. Trump has questioned the integrity of US election systems in recent weeks, but his allegations have been vague and unsubstantiated. In his phone call, Johnson encouraged the state officials to comply with federal cyber recommendations, such as making sure electronic voting machines are not connected to the internet while voting is taking place, the department said. Concerns in both parties about manipulation of electronic electoral systems are not new. Hackers can wreak havoc in myriad ways, from hijacking a candidate's website to hacking voting machines or deleting or changing election records. An Electronic Privacy Information Center report this week said 32 of the 50 states would allow voting by insecure email, fax and internet portals in this election cycle. (Reuters, 17Aug16)

(U) DHS funds small biz cyber R&D

(U) The Department of Homeland Security has awarded funding to 13 small businesses around the country for new cybersecurity technologies that address the research and development needs of DHS components and the homeland security enterprise. Awards were made in four areas: [1] Applicability of blockchain technology to identity management and privacy protection. [2] Remote identity proofing alternative to knowledge-based authentication and verification. [3] Malware prediction for situational understanding and pre-emptive cyber defense. [4] Real-time assessment of resilience and preparedness. Under the Science and Technology Directorate's Small Business Innovation Research program, each company will receive approximately $100,000 for development of their projects. (Government Computer News, 16Aug16)

(U) US intelligence to share supply chain threat reports with industry

(U) The US National Counterintelligence and Security Center will soon provide classified supply chain threat reports to critical US telecommunications, energy and financial businesses. The effort is designed to reduce threats against a vast private supply chain of equipment and services that could result in the theft of vital data or disrupt operations in critical systems. Supply chain threats are not well understood by security professionals, yet the supply chain is relatively easy to manipulate by foreign governments like Russia and China, as well as criminal gangs, hackers and even disgruntled workers, according to NCSC officials. The Office of the Director of National Intelligence described the threats to private sector supply chains in a press release on Thursday and released a video on supply chain risk management. The video urges companies to include a member of the company's acquisition division in planning sessions to defend against cyberattacks. It also urges companies to know their suppliers and whether they are associated with adversaries of the US and from which vendors those companies purchase parts. The NCSC, in the statement, said it will provide "threat briefings to government partners and eventually to industry." NCSC officials could not be reached for more details, but the statement referred to a Bloomberg interview that said the threat reports would begin in about two months through secure channels and would include the context behind hacking attacks, such as whether another country is responsible. Gartner analyst Avivah Litan called the government's plan to share supply-chain threat reports "a really important initiative." "This is one area that the federal government pays attention to while private industry generally does not," she added. "Many of the threats to the US supply chain are perpetrated by nation-states like China and Russia who use weaknesses and vulnerabilities in the supply chain to infiltrate US infrastructure and systems." She said private companies typically focus on preventing and detecting known attacks that started long ago, but not on pre-empting them. "It's a very good thing for US intelligence agencies to bring information that can pre-empt attacks. This is probably one of the most useful activities our government can engage in to help protect US infrastructure." Litan said only a handful of security companies focus on pre-empting attacks by finding criminal perpetrators and then uncovering how they act well before they strike. (Computerworld, 15Aug16)

(U) SANS to host Baltimore information security training event

(U) SANS Institute, the global leader in information security training, today announced its return to Baltimore, MD 10 October -15. The SANS Baltimore 2016 training event will feature 10 hands-on immersion style training courses taught by real-world practitioners. Included among the courses is the new FOR578: Cyber Threat Intelligence course which trains individuals and teams to detect, scope, and select resilient courses of action in response to intrusions and data breaches. According to Rebekah Brown, threat intelligence lead for Rapid7 and co-instructor of the FOR578 course alongside SANS instructor Robert M. Lee, "There is a high demand for cyber threat intelligence analysts in the community -- we've reached a point where we need trained and capable analysts to support security operations and to inform leadership on the threats facing organizations. Threat intelligence provides both of these things, and FOR578 is one of the best places to get this crucial training." For those wanting to learning more about threat intelligence, Brown will present a bonus evening discussion entitled Analyze, Act, Share: Avoiding Intelligence Failures. This talk will analyze the three areas that contribute to intelligence failures and how they apply specifically to cyber threat intelligence. It will step through ways to identify and address these problems when they appear, and how to properly position your program to avoid them in the first place. For a complete list of courses and bonus evening discussion, or to register for SANS Baltimore 2016, please visit: www.sans.org/u/k9t. (PRNewswire, 15Aug16)

[redacted]

(b)(3) 10 USC ⊥ 424

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

[redacted]

(b)(3) 10 USC ⊥ 424