Cyber-Threat Newsletter – 14 Jun 16

(b)(3) 10 USC § 424

Patches & Updates of the Week:

(U) Google updates Chrome with 15 patches
(U) Google reported it has updated Chrome to version 51.0.2704.79 for Windows, Mac, and Linux with a total of 15 security fixes, including two high and five medium threats, being patched. The online giant paid out $26,000 in bug bounty fees to five individuals. The two high priority issues were CVE-2016-1696 and CVE-2016-1697, each of which earned its discovers $7,500 each. The former was a cross-origins bypass in Extension bindings and the latter was also a cross-origin bypass but in Blink. Google credited Mariusz Mlynski for finding the second issue. The other bug hunter was anonymous. Rob Wu found three issues for Google: CVE-2016-1698, $4,000, a Information leak in Extension bindings; CVE-2016-1700, $1,500, a Use-after-free in Extensions; and CVE-2016-1701, $1,000, Use-after-free in Autofill. (scmagazine.com, 06Jun16)

Threats & Vulnerabilities of the Week:

(U) New macro attacks use Anti-VM and Anti-Sandbox techniques
(U) A new wave of malicious documents containing highly obfuscated macros is using Anti-VM (virtual machine) and Anti-Sandbox techniques to avoid being downloaded and detected by the automated analysis systems. In late May, Zscaler researchers spotted the malicious documents leveraging the ability to detect virtual environments via Office RecentFiles property and the ability to check for external IP ownership to prevent sandbox solutions, Zscaler Director of Security Research Deepen Desai said in a 7 June blog post. The macros code checks if the number of RecentFiles collection is less than a predefined threshold and terminates if it is, the post said. The use of Microsoft Office RecentFiles property to detect a virtual environment is a new technique that may seem trivial, but has been effective against many automated analysis systems, Desai told SCMagazine.com via emailed comments. "The malware author makes an assumption here that most clean virtual environment snapshots will be taken after a fresh Microsoft Office install with probably one or two document files opened for testing the installation," Desai said. "Alternately, a standard user system with Office applications should have at least 3 or more recently accessed document files." The cyber crooks behind the malicious campaign aren't exploiting vulnerabilities to infect users, but instead are using social engineering tactics to lure the user into enabling the macros. To prevent these types of attacks, Desai said end users need to be more vigilant and should never trust documents that prompt them to enable macros for viewing content. (scmagazine.com, 08Jun16)

(U) Bitdefender finds eavesdropping vulnerability in public cloud
(U) Security firm Bitdefender has found a vulnerability in public cloud infrastructures which it said allows a third party to eavesdrop on communications encrypted with transport layer security (TLS) protocol. The vulnerability is leveraged by Bitdefender for its own research purposes, developing a technique called TeLeScope, which is only effective against virtualized environments that run on top of a hypervisor. According to Bitdefender, such infrastructures are provided by industry giants Amazon, Google, Microsoft, and DigitalOcean, with the security vendor flagging banks, companies dealing with either intellectual property or personal information, and government institutions as the sectors likely to be affected by the security flaw. Rather than exploiting a flaw in TLS, Bitdefender said the attack technique relies on extracting the TLS keys at the hypervisor level by clever memory probing and while the company said accessing a virtual machine's virtual resources was not new, real-time decryption of the TLS traffic without pausing the virtual machine at a particular moment had not been achieved before. Speaking last month at the HITB Conference in Amsterdam, Bitdefender security researcher Radu Caragea demonstrated in a proof of concept that encrypted communication can be decrypted in real-time using a technique that has virtually no footprint and is invisible to almost everyone. The security firm said Caragea's staged attack makes it possible for a malicious cloud provider, or one agreeing to give access to government agencies, to recover the TLS keys used to encrypt every communication session between a virtualized server and an organization's customers. Additionally, Bitdefender said its proof of concept uncovers a fundamental lapse that cannot be fixed or mitigated without rewriting the cryptographic libraries currently in use. The security firm said the only fix for the vulnerability is to prevent access to the hypervisor by a company running its own hardware inside its own infrastructure, adding that if an organization does not own its own hardware, it does not own the data, either. (zdnet.com, 08Jun16)

(U) Malware exploits BITS to retain foothold on Windows systems
(U) If you're sure that you have cleaned your system of malware, but you keep seeing malware-related network alerts, it's possible that at some point you've been hit with malware that uses Windows' BITS to schedule malicious downloads. BITS -- Background Intelligent Transfer Service -- is a native Windows tool that facilitates file transfers and it's used by the OS and some third-party software to retrieve updates. But it's also sometimes exploited by attackers and malware authors. SecureWorks researchers explained why: "Attractive features for threat actors include the abilities to retrieve or upload files using an application trusted by host firewalls, to reliably resume interrupted transfers, to create tasks that can endure for months, and to launch arbitrary programs when a task completes." They have recently encountered one instance when the malware misused the service to download and launch malicious files. The malware itself was not present on the computer anymore, having been removed months before, but they believe it to be the DNSChanger Trojan (aka Trojan.Zlob.Q), because the scheduled BITS tasks were meant to download malicious files from two domains that have been previously associated with it. "The poisoned BITS tasks, which created installation and clean-up scripts after their payloads were downloaded, were self-contained in the BITS job database, with no files or registry modifications to detect on the host," the researchers pointed out. Anomalous scheduled BITS tasks are also likely to remain undiscovered if the user or administrator doesn't know exactly what to look for. Users that keep encountering network or host alerts after malware remediation would do well to enumerate active BITS tasks on the system and look for those they don't recognize. They have also provided a list of domains associated with this particular malware, and advised admins to restrict access to them. (helpnetsecurity.com, 07Jun16)

(U) Low-profile Crysis ransomware suddenly stealing the show

(U) Security experts have been watching and waiting for Locky and other high-profile ransomware families to expand their spheres of influence following the sudden demise of TeslaCrypt. But surprisingly, researchers at ESET have discovered that an under-the-radar ransomware known as Crysis has been silently and quickly gaining momentum, and is currently even more prevalent than Locky. As ransomware goes, Crysis features some decidedly malicious traits. According to an ESET "We Live Security" blog post, Crysis encrypts virtually all file types -- including those with no extension -- on fixed, removable and network drives. "Most ransomware families are encrypting files with specific extensions, so this behavior is unusual," said Ondrej Kubovic, EMEA security specialist, in an email interview with SCMagazine.com. "Also, various executable files (.exe, .dll) get encrypted which is not common in comparison to high-profile ransomwares." As a result, the "affected computer may become unstable." On some Windows operating systems, Crysis can even run with administrator privileges, giving its encryption mechanism access to even more files. As is usual with ransomware, victims must comply with given payment instructions in order to restore their computers' normal functionality. In this case, the attackers are typically seeking bitcoins worth between 400 and 900 euros, ESET has reported. The instructions are delivered via a text file that gets dropped into the affected computer's desktop folder. First detected in February 2016, Crysis is reportedly spreading through a number of vectors. The most common one appears to be via widespread spam emails that use double file extensions that make executable files appear to be non-executable. Alternatively, the attackers are also "disguising malicious files as harmless-looking installers for various legitimate applications, which they have been distributing via various online locations and shared networks," the ESET blog post states. "We have seen the malware executable faking names of common applications such as: WinRar, MS_Excel, iExplore, setup2 [and] setap22," said Kubovic to SCMagazine.com. Beyond encryption, the trojan also collects the victim computer's name and some encrypted files and sends them to a remote command and control server. It also sets certain registry entries so that it automatically executes any time the system is restarted. "By setting the registry entries, Crysis gains a stronger foothold in the system, making itself more difficult to remove," said Kubovic. In its blog post, ESET is advising readers that files encrypted by older variants of Crysis might be salvageable without paying the ransom, with the assistance of ESET technical support. (scmagazine.com, 07Jun16)

(U) Massive DDoS attacks reach record levels as botnets make them cheaper to launch

(U) There were 19 distributed denial-of-service (DDoS) attacks that exceeded 100Gbps during the first three months of the year, almost four times more than in the previous quarter. Even more concerning is that these mega attacks, which few companies can withstand on their own, were launched using so-called booter or stresser botnets that are common and cheap to rent. This means that more criminals can now afford to launch such crippling attacks. "In the past, very few attacks generated with booter/stresser tools exceeded the 100 Gbps mark," researchers from Akamai said in the company's State of the Internet security report for the first quarter of 2016 that was released Tuesday. By comparison, only five DDoS attacks over 100Gbps were recorded during the fourth quarter of 2015 and eight in the third quarter. Nineteen such attacks in a single quarter is a new high, with the previous record, 17, set in the third quarter of 2014. But high bandwidth is not the only aspect of DDoS attacks that can cause problems for defenders. Even lower-bandwidth attacks can be dangerous if they have a high packet rate. A large number of packets per second pose a threat to routers because they dedicate RAM to process every single packet, regardless of its size. If a router serves multiple clients in addition to the target and exhausts its resources, that can cause collateral damage. According to Akamai, in the first quarter there were six DDoS attacks that exceeded 30 million packets per second (Mpps), and two attacks that peaked at over 50Mpps. DDoS reflection and amplification techniques continue to be used extensively. These involve abusing misconfigured servers on the Internet that respond to spoofed requests over various UDP-based protocols. Around one-in-four of all DDoS attacks seen during the first three months of 2016 contained UDP (User Datagram Protocol) fragments. This fragmentation can indicate the use of DDoS amplification techniques, which results in large payloads. The four next most common DDoS attack vectors were all protocols that are abused for DDoS reflection: DNS (18 percent), NTP (12 percent), CHARGEN (11 percent), and SSDP (7 percent). Another worrying trend is that an increasing number of attacks now use two or more vectors at the same time. Almost 60 percent of all DDoS attacks observed during the first quarter were multivector attacks: 42 percent used two vectors and 17 percent used three or more. China, the US and Turkey were the top three countries from where DDoS attack traffic originated, but this indicates where the largest number of compromised computers and misconfigured servers are located, not where the attackers are based. The most-hit industry was gaming, accounting for 55 percent of all attacks. It was followed by software and technology (25 percent), media and entertainment (5 percent), financial services (4 percent), and Internet and telecommunications (4 percent). (IDG News Service, 07Jun16)

(U) 'Black Shades' ransomware taunts researchers in its source code

(U) An independent security researcher who goes simply by the name Jack recently discovered a ransomware called "Black Shades," which not only encrypts files but also taunts security researchers. There are multiple obfuscated strings of source code within the ransomware which contain taunting messages for researchers who are analyzing the malware, according to Bleeping Computer. One of the codes said "YoxcnnotcrackthisAlgorithmynare>idiot<" which is meant to read "You cannot crack this algorithm … idiot" and another code written in Russian translated to "you cannot hack me, I am very hard." Researchers at the MalwareHunterTeam think the ransomware may be distributed through fake videos, fake cracks, or fake patches, Bleeping Computer said. Though he hasn't witnessed the attack in the wild, Jack told SCMagazine.com via emailed comments the ransomware is likely being distributed via rogue installs from file sharing websites and potentially as fake updates. "Some samples I have observed were dropped from a keygen "tool" that actually downloaded the SilentShade / BlackShades binary," he said. "That is an interesting distribution method because many people will bypass AV for downloaded keygen or cracked programs since they usually are detected as "hack tools" or something similar." Jack said the he thinks the use of the "Black Shades" branding is interesting and is due to either a lack of creativity or out of a social engineering tactic to coerce victims to pay. "If they were to google 'Black Shades,' for example, the first result is from the FBI, which may add 'legitimacy' to what the victim is seeing," Jack said. Once infected, the malware will only encrypt certain commonly used C drive folders such as the "Downloads," "Documents," and "Desktop" folders using AES-256 encryption and will also drop a file in each folder called YourID.txt, which contains the unique victim ID, according to the report. On other drives the malware will encrypt every folder it scans. When it is done encrypting the ransomware will display a ransom note which displays itself every time the user logs into the computer and instructs the user to how to pay the $30 ransom in Bitcoin or on Paypal. Researchers at Bleeping Computer noted the use of the Paypal option is strange because the payment platform is easily traceable. (scmagazine.com, 06Jun16)

(U) New Cerber ransomware variants morph every 15 seconds

(U) Malware coders behind the Cerber ransomware are now using a technique called "malware factory" to create a different version of their ransomware every 15 seconds in order to bypass client-side security software. Cerber is one of today's most active ransomware threats, backed by a group that has put in the time and resources to grow operations and evolve their malware payload. The ransomware has constantly changed since the beginning of the year, when it was first spotted, and nobody has been able to create a free decrypter until now. US security firm Invincea is reporting on the most recent change in Cerber's mode of operation. The company says that while it was analyzing a log file of Cerber's latest infection techniques and thus trying to reproduce the infection chain, their analysts got a Cerber ransomware payload with a different file hash. Retrying the infection chain after a few moments, the researchers got a third hash, and then a fourth hash, and so on. It didn't take them long to figure out that Cerber's C&C servers were churning out Cerber binaries with different file hashes every 15 seconds. This was a tell-tale sign of a "malware factory," an automated malware assembly line that puts together Cerber payloads but makes small modifications to the file's internal structure in order to generate files with unique hashes. Having files with unique hashes allows Cerber to infect computers that feature antivirus products. A deeper look at the Cerber payloads showed a connection to a suspicious file sample first collected in September 2015, after being dropped by the Neutrino exploit kit. This might be one of the earliest Cerber ransomware samples, long before researchers discovered it in late February, early March. "By constantly morphing the same old binary from 2015 [Cerber] is able to evade detection quite easily," Invincea's Patrick Belcher explained, who is coincidentally one of the authors of a research paper on malware factories and polymorphic malware. Invincea also claims to have previously discovered a Cerber sample that included the ability to launch DDoS attacks. (Softpedia, 06Jun16)

(U) Mysterious malware targets industrial control systems, borrows Stuxnet techniques

(U) Researchers have found a malware program that was designed to manipulate supervisory control and data acquisition (SCADA) systems in order to hide the real readings from industrial processes. The same technique was used by the Stuxnet sabotage malware allegedly created by the US and Israel to disrupt Iran's nuclear program and credited with destroying a large number of the country's uranium enrichment centrifuges. The new malware was discovered in the second half of last year by researchers from security firm FireEye, not in an active attack, but in the VirusTotal database. VirusTotal is a Google-owned website where users can submit suspicious files to be scanned by antivirus engines. The mysterious program, which FireEye has dubbed IRONGATE, was uploaded to VirusTotal by several sources in 2014, at which time none of the antivirus products used by the site detected it as malicious. It's also surprising that no company has identified the malware until late 2015, because the VirusTotal samples are automatically shared with all antivirus vendors who participate in the project. FireEye itself discovered it because the company was searching for potentially suspicious samples compiled with PyInstaller, a technique used by various attackers. Two IRONGATE payloads stood out because they had references to SCADA and associated functionality. The good news is that the samples seem to be a proof of concept or part of some research effort. They're designed to find and replace a specific DLL that communicates with Siemens SIMATIC S7-PLCSIM, a software product that allows users to run programs on simulated S7-300 and S7-400 programmable logic controllers (PLCs). PLCs are the specialized hardware devices that monitor and control industrial processes -- spinning motors, opening and closing valves, etc. They transmit their readings and other data to monitoring software, the human-machine interface (HMI) that runs on workstations used by engineers. Like Stuxnet did at Iran's Natanz nuclear plant, IRONGATE goal is to inject itself into the SCADA monitoring process and manipulate the data coming from PLCs, potentially hiding ongoing sabotage. The fact that IRONGATE interacts with a PLC simulator and replaces a DLL that is not part of the Siemens standard product set have led the FireEye researchers to believe this malware was likely just a test. The Siemens Product Computer Emergency Readiness Team (ProductCERT) "has confirmed that the code would not work against a standard Siemens control system environment," the FireEye researchers said in a blog post Thursday. However, if IRONGATE was just a proof of concept developed in 2014, intended to test a Stuxnet-like man-in-the-middle attack against PLCs, it could mean its creators have built another malware program since then that works against real industrial control system (ICS) deployments. Either way, IRONGATE's discovery should serve as a warning to organizations that operate SCADA systems. (IDG News Service, 02Jun16)

(U) FastPOS malware instantly delivers stolen credit card data

(U) Cybercriminals must be feeling the need for speed by brewing up a new point-of-sale (POS) malware family called FastPOS that is much faster at snatching and disseminating stolen credit card information. FastPOS was discovered by Trend Micro researchers, who have also given it the fancier moniker TSPY_FASTPOS.SMZTDA, differs from other POS malware by immediately transferring the stolen credit card data back to the command and control server. Traditionally, the payment card info is stored locally and then forwarded only periodically. This is done to help prevent detection. Trend Micro also believes FastPOS has been designed for use against smaller, simpler retail networks and not large retail chains. So far the malware has victimized people across the globe hitting the United States, Brazil, Japan, France and Taiwan. "This could be cases where the primary network gateway is a simple DSL modem with ports forwarded to the POS system. In such a situation, the target would rely almost exclusively on endpoint detection and less so on network-level detection," the researchers said. Injecting the malware onto the POS system appears to be done by brute force attacks to obtain login credentials, social engineering scams to trick the users into installing the malware or through a real-time file sharing service. The key logger and RAM scraper that is used with FastPOS also have a few new twists. Trend Micro said the key logger is similar to the one found in NewPOSThings malware, but instead of storing the information on the infected system it uses the device's memory and when the customer/victim presses the enter button the data is sent along to the criminal. The RAM scraper not only grabs all the card info, but includes a series of checks to make sure only valid credit card numbers are swiped. Another somewhat rare feature for this scraper is it verifies the card's service code. This lets the criminal know where the card can be used and it also helps weed out cards that require PINS. Trend researchers also found out that the actors behind the malware are also advertising and selling the stolen payment card credentials. "What is unusual is that we found that this site's IP address was used by FastPOS itself as a C&C server! In short, the persons behind FastPOS are selling stolen credentials via the same server they use to receive these credentials," the report said. (scmagazine.com, 03Jun16)

(U) KeePass update check MitM flaw can lead to malicious downloads

(U) Open source password manager KeePass sports a MitM vulnerability that could allow attackers to trick users into downloading malware disguised as a software update, security researcher Florian Bogner warns. All versions of KeePass, including the latest, are vulnerable. The team developing the software is aware of the flaw (CVE-2016-5119), but they currently have no intention of fixing it. "KeePass 2's automatic update check uses HTTP to request the current version information," Bogner has discovered. "An attacker can modify -- through for example ARP spoofing or by providing a malicious Wifi Hotspot -- the server response." The software would show a dialog box that indicates that there is a new version available for download. But even though the download link points to the official KeePass website (http://keepass.info/), the fact that the traffic to and from it is not encrypted means it could be intercepted and manipulated, and could result in the user downloading malware. "For any security centric tool -- like a password manager -- it is essential to not expose its users to any additional risks," Bogner points out. He believes that switching to HTTPS should not be difficult, but apparently the developers are not of the same mind. "The vulnerability will not be fixed. The indirect costs of switching to HTTPS (like lost advertisement revenue) make it an inviable solution," KeePass developer Dominik Reichl responded when Bogner alerted them to the danger. Users can protect themselves from this type of attack by downloading new versions of the software directly from KeePass' SourceForge page. Reichl also pointed out that verifying the KeePass download -- no matter from where it's downloaded -- is also important. "The binaries are digitally signed (Authenticode); you can check them using Windows Explorer by going 'Properties' -> tab 'Digital Signatures'," he noted. (helpnetsecurity.com, 02Jun16)

(U) Lenovo advises users to remove a vulnerable, pre-installed support tool

(U) PC maker Lenovo is recommending that users remove an application preloaded on their computers because it contains a high-severity flaw that could allow attackers to take over their systems. The vulnerable tool is called Lenovo Accelerator Application and is designed to speed up the launch of other Lenovo applications. It was preinstalled on more than 100 laptop and desktop models shipped with Windows 10, but not those from the ThinkPad and ThinkStation lines. The flaw was discovered by researchers from security firm Duo Security as part of an analysis of OEM software update tools from five PC manufacturers. The company found that a process called LiveAgent, apparently the update component of the Lenovo Accelerator Application, does not use encrypted connections when checking and downloading updates. LiveAgent also does not validate the digital signatures of the downloaded files before running them, the researchers said. This allows man-in-the-middle attackers who can intercept a user's traffic -- for example, on an insecure WiFi network or through a compromised router -- to trick LiveAgent into downloading and executing malware. LiveAgent was one of the worst software updaters Duo Security identified, but the company found flaws in update tools from all five vendors it looked at: Acer, ASUSTeK Computer, Lenovo, Dell and HP. The company plans to release a System Update removal utility soon, a Lenovo representative said in an emailed statement. (IDG News Service, 01Jun16)

(U) CryptXXX ransomware, again updated, can now encrypt network shared files

(U) An updated version of the CryptXXX ransomware -- that again renders decryption tools ineffective and has the ability for network share encryption -- has been spotted in the wild. Proofpoint researchers said in a blog post that CryptXXX v3.1000 was found in the wild last week. The nasty network share capability allows an infected machine to scan the /24 subnet on a local area network, find shared storage resources and then encrypt those files. It was also noted that the CryptXXX decryptor tool developed by Kaspersky Labs had been rendered ineffective by CryptXXX v 2.0 in May. It now remains basically unusable as "decrypting individual files is time-consuming and scales poorly, especially as CryptXXX begins encrypting many more files across network shares," the Proofpoint researchers wrote. The attackers also rolled out a new payment portal. (scmagazine.com, 02Jun16)

(U) FBI warns of bitcoin-based extortion attempts following recent mega breaches

(U) The FBI's Internet Crime Complaint Center (IC3) has issued a public alert today, warning against a spike in Bitcoin-based extortion attempts against regular US citizens who had their personal details leaked in one of the recent mega breaches. The FBI says crooks collected the data from these data breaches and are sending intimidating emails to people who had their personal details exposed. Crooks threaten to release the victim's personal data onto the public Internet while some other times they claimed they hacked the victim's social media accounts as well. In some weirder cases, the crooks also make preposterous claims that they have "dirt" on the recipient, which they're willing to share with the victim's friends on various social networks. In order to keep the crook quiet, victims have to pay between 2 and 5 Bitcoin ($500 and $2,500). All of this is happening because, in the past month, sites like LinkedIn, MySpace, Tumblr, Fling.com, or BeautifulPeople have suffered massive data breaches that exposed the personal details of hundreds of millions of users. This data often reaches the public Internet or is available for purchase on Dark Web marketplaces. Besides public services, voter databases belonging to the US, Mexico, Turkey, and the Philippines have ended up online in the past months as well, and they contained even more personal details than your regular social media profile. (Softpedia, 01Jun16)

Incidents of Interest:

OGA

(U) University pays $20,000 in ransomware attack

(U) The ransomware plague has hit the University of Calgary, and the academic institution did what many victims do: they paid the ransom to get the encrypted files back. The amount they paid was 20,000 Canadian dollars, in Bitcoin, and they received the decryption keys that -- according to Linda Dalgetty, the University's VP of finances and services -- work as they should. "The actual process of decryption is time-consuming and must be performed with care. It is important to note that decryption keys do not automatically restore all systems or guarantee the recovery of all data. A great deal of work is still required by IT to ensure all affected systems are operational again, and this process will take time," she pointed out. "The university is working with various experts in this field, and because this was a criminal act, the Calgary Police Service has been brought in as part of the investigation. As this is an active investigation, we are not able to provide further details on the nature of the attack, specific actions taken to address it, or how or if decryption keys will be used." According to the Calgary Herald, the attack happened in late May, and affected over 100 computer systems, as well as the University's email, Skype, wireless networks and other services. CBC News reports that the University decided to pay the ransom because they do world-class research and they did not want to be in a position that they had exhausted the option to get people's potential life work back. "We did that solely so we could protect the quality and the nature of the information we generate at the university," Dalgetty said. She also noted that there is no indication that any personal or other university data was released to the public by the attackers. (helpnetsecurity.com, 08Jun16)

(U) Hacker claims to be selling millions of Twitter accounts

(U) A hacker, who has links to the recent MySpace, LinkedIn, and Tumblr data breaches, is claiming another major tech scalp -- this time, it's said to be millions of Twitter accounts. A Russian seller, who goes by the name Tessa88, claimed in an encrypted chat on Tuesday to have obtained the database, which includes an email addresses (and sometimes a second email), usernames, and plain-text passwords. Tessa88 is selling the cache for 10 bitcoins, or about $5,820 at the time of writing. The seller said they obtained 379 million accounts as early as 2015. That would be far more than its 310 million monthly active users, but could account for cumulative accounts, such as inactive users. But an analysis of the database by LeakedSource, a breach notification site which received the database from the seller on Wednesday, showed there are in fact over 32 million purported accounts in the database, after duplicates were removed. LeakedSource said in a blog post that it was unlikely that Twitter was breached, and pointed to malware as the culprit. "The explanation for this is that tens of millions of people have become infected by malware, and the malware sent every saved username and password from browsers like Chrome and Firefox back to the hackers from all websites including Twitter," the blog post said. The group said it was able to verify the passwords associated with 15 users. LeakedSource said that the passwords were likely "stolen directly from consumers, therefore they are in plaintext with no encryption or hashing." The groups said it did not believe that Twitter stored data in plain-text at the time the data was taken, thought to be around 2014. A Twitter spokesperson said in a prepared statement, "A number of other online services have seen millions of passwords stolen in the past several weeks. We recommend people use a unique, strong password for Twitter. We detail other steps people can take to keep their accounts secure on our help center." In a recent tweet, the company also said that it periodically checks its data against recent password leaks to ensure that accounts stay secure. (zdnet.com, 08Jun16)

OGA

Items of Interest

(U) Destructive BadBlock ransomware can be foiled

(U) If you have been hit with ransomware, you want that malware to be BadBlock -- but only if you haven't restarted your computer. This particular malware is a lackluster attempt to create something on par with more popular ransomware, and that allowed Emsisoft security researcher Fabian Wosar to create a decrypter tool for it. The tool can be downloaded for free, and Bleeping Computer has offered instructions on how to use it. But, aside from encrypting document, image, database and other files not crucial for the functioning of the computer, it also encrypts Windows' system files, and this makes the targeted machine slow and unstable, Dell SonicWALL researchers have found. "In the instructions, the Badblock authors suggest not to shut down the infected machine. If the user decides to, they will not be able to log back in because during our analysis we found that the files responsible for rebooting the machine were also encrypted," they pointed out. "At this point, the victim is locked out of their machine and the machine is rendered useless. Users will also be unable to use system restore because the files, progman.exe and rstrui.exe, have also been encrypted". (helpnetsecurity.com, 06Jun16)

(U) Congress probes Fed's cyber breaches

(U) A US congressional committee has launched an investigation into the Federal Reserve's cyber security practices after a Reuters report revealed more than 50 cyber breaches at the US central bank between 2011 and 2015. The House Committee on Science, Space and Technology on Friday sent a letter to Federal Reserve Chair Janet Yellen to express "serious concerns" over the central bank's ability to protect sensitive financial information. The letter cited the Reuters report, which was based on heavily redacted internal Fed records obtained through a Freedom of Information Act request. The redacted records did not say who hacked the bank's systems or whether they accessed sensitive information or stole money. "These reports raise serious concerns about the Federal Reserve's cyber security posture, including its ability to prevent threats from compromising highly sensitive financial information housed on the agency's systems," said the letter, signed by House Science Committee Chairman Lamar Smith, a Texas Republican, and Barry Loudermilk, a Georgia Republican and chairman of the panel's oversight subcommittee. The panel asked the Fed's national cyber security team -- the National Incident Response Team -- to turn over all cyber incident reports in unredacted form from 1 January 2009, to the present. It also asked for incident reports from the Fed's local incident response teams. The committee said it has jurisdiction over the Fed's cyber security because the panel is tasked with oversight of the US National Institute of Standards and Technology, an agency responsible for developing federal cyber security standards and guidelines, under a 2014 federal information technology law. The panel also requested a "detailed description of all confirmed cyber security incidents" from 2009 to the present, all documents and communications referring or relating to "higher impact cases" handled by the Fed's NIRT team, all documents and communications with the Fed's Office of Inspector General related to confirmed cyber incidents, and an organizational chart detailing the Fed's top cyber security personnel. The committee requested a response to its inquiry by 17 June. (Reuters, 03Jun16)

(U) NATO weighs making cyber wartime domain

(U) July's NATO Warsaw Summit will come with a major focus on cyber-related capabilities, and could conclude with a new definition of cyberspace as a warfighting domain -- reinforcing the idea that a cyber-attack on a partner could trigger an Article 5 invocation. Such an announcement represents the increasing focus of cyber for the alliance at a time when Russia is increasingly focused on asymmetrical warfare to try and weaken the European members, as Western officials have said. The thinking behind the discussions is focused on the modern reality that major infrastructure damage could be caused by a cyber strike. The question of how to respond to cyberattacks is a thorny one. Attribution for the attacks can often be murky, making it very hard to prove accurately the original source. Even if the location of an attack is identified, a nation can claim that the attacks came from a rogue individual and not a government. In addition, defining the proportionality of a response can be tricky. How should a nation state respond to a small hack from a neighbor that steals information? How does that compare to an attack on critical infrastructure, such as shutting down a power grid, which could lead to injuries or accidents to civilians? Should cyberattacks always merit a response in the virtual domain, or could a kinetic or economic response be launched as a result? While NATO Secretary General Jens Stoltenberg has previously said a cyberattack could trigger Article 5, the reciprocity issue is a particularly hard one for NATO officials to figure out, as nations understandably do not want to risk being dragged into conflict by an ally over a low-level hacking attempt. The 2007 denial-of-service attacks on Estonia was noted by the source as an example where the government could have -- hypothetically, under the new operating concept -- invoked Article 5, the NATO rule that requires allies to come to the defense of whatever nation triggers it. However, that incident did not result in any serious property or economic damage, in comparison to the STUXNET virus that destroyed part of Iran's nuclear program. Regardless of what decision comes out of the Warsaw Summit, the NATO partners are increasingly focused on building cyber resiliency among the allied nations. (defensenews.com, 02Jun16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424