[redacted] Cyber-Threat Newsletter – 27 Jun 16

(b)(3) 10 USC ⊥ 424

Patches & Updates of the Week:

(U) WordPress 4.5.3 release mends eight security flaws, 17 bugs

(U) WordPress has released version 4.5.3 of its content management system, fixing eight security vulnerabilities that surfaced in previous versions, as well as 17 other bugs. In its latest online maintenance and security release, WordPress described the eight security holes as follows: a redirect bypass in the customizer, two cross-site scripting problems via attachment names, a revision history information disclosure issue, an oEmbed denial of service flaw, the unauthorized category removal from a post, password changes via stolen cookies and insufficiently secure "sanitize_file_name" edge cases. WordPress has recommended that its users update their websites immediately with the new version. Sites that support automatic background updates have already begun updating to 4.5.3. (scmagazine.com, 22Jun16)

(U) Siemens update advised following US CERT advisory

(U) The US Computer Emergency Response Team (CERT) has issued advisory ICSA-16-161-02, which is warning of "weakly protected" credentials in Siemens SIMATIC WinCC flexible industrial control system. Due to this weak protection, any data it sends over the network could be listened to and decrypted. According to CERT, Gleb Gritsai and Roman Ilin from Positive Technologies reported this issue directly to Siemens, and fortunately Siemens has already produced an update to mitigate this vulnerability. The advisory reads, "Attackers capturing network traffic of the remote management module could possibly reconstruct user credentials. The remote management module of SIMATIC WinCC flexible panels and SIMATIC WinCC flexible runtime transmits weakly protected credentials over the network. Attackers capturing network traffic of the remote management module could possibly reconstruct the credentials". CERT has said that Impact to individual organizations depends on many factors that are unique to each organization. However it advised that companies should protect network access to devices running SIMATIC WinCC flexible with appropriate mechanisms, and configure the environment according to Siemens operational guidelines in order to run the devices in a protected IT environment. Other defensive measures advised by CERT to minimize the risk of exploitation of these vulnerabilities include: [1] Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. [2] Locate control system networks and remote devices behind firewalls, and isolate them from the business network. [3] When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices. Additional mitigation guidance and recommended practices are publicly available in the ICS/CERT Technical Information Paper, ICS-TIP-12-146-01B -- Targeted Cyber Intrusion Detection and Mitigation Strategies, available for download from the ICS-CERT web site (http://ics-cert.us-cert.gov/). CERT says organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents. (scmagazine.com, 16Jun16)

Threats & Vulnerabilities of the Week:

(U) There's no virus in the iTunes database -- it's a phish

(U) A new phishing campaign aimed at Apple users has been spotted by security researcher Bryan Campbell. It takes the form of a fake email supposedly sent by Apple Service, claiming that a 'virus' has been detected in the company's iTunes database, and that users need to 're-validate' their details to keep their iTunes account secure. "This is the second time out admin is sending you this message and failure to re-validate your iTunes account upon receiving this message, will lead to permanent closing of your account within the next 72 hours," the message effectively threatens. "Please follow the secure link below to clean and re-validate your iTunes Account." The link leads to a spoofed Apple ID login page, and once the login credentials are entered, the victim is redirected to a fake 'Update Billing' page: Users whose suspicions weren't triggered by any of the obvious signs of trickery -- the email starting with "Dear Apple Customer" instead with their names, poor spelling, the fake login page's random domain name that has nothing to do with Apple, etc. -- will enter and submit their name, date of birth, address, as well as payment card details and login credentials. This information is effectively everything the phishers need to know to complete fraudulent transactions in the victims' name and with their money. The fake pages have already been taken down, but setting them up again on new locations and changing the link in the phishing email is quick and easy work for the scammers, so Apple users are advised to be on the lookout for similar emails. "Remember to always be careful about the links you click on, and verify that a site that is asking for your password is the real deal", Graham Cluley advises. (helpnetsecurity.com, 21Jun16)

(U) Check Point tracks two waves of Cerber ransomware hitting US, UK

(U) A team of Check Point researchers have tracked two large waves of attacks using Cerber ransomware in the last few months with more spikes in the number of incidents expected. While Cerber has been steadily used since earlier this year, two spikes took place in between 4 April to 18 April and then again between 17 May to 30 May, Check Point reported. In each case the majority of attacks hit targets in the United States, 41 percent; Turkey, 15 percent; and the U.K., nine percent. Seven other nations also experienced an uptick in the number of attacks during these two periods, but at a much lower rate. "We have no doubt that we will continue to see spikes in Cerber's activity," the report stated. Check Point estimates the number of attacks that have taken place at about 600. The research firm also detailed its reasoning behind why the attack took place in waves. "It allows the attackers to control their operation closely for a short period of time, without the need for constant management, which can require large resources. Second, striking in waves enables the attackers to make necessary code changes, improving their malware and evasion techniques between bursts. Lastly, this pattern can also be caused by changes in the distribution infrastructure," said Gadi Naveh, a threat prevention researcher with Check Point to SCMagazine.com via email. One change that does coincide with these events Cerber has recently been spotted being advertised as a ransomware as a service on several Russian dark web forums. (scmagazine.com, 21Jun16)

(U) Foreign government hackers are the gravest and most common threat, agencies say
(U) The gravest attacks -- and most common -- perpetrated against agency networks involved nation states, according to an audit that happened to be released amid accusations the Russian government allegedly hacked the Democratic National Committee. The Government Accountability Office assessment comes one year after the Office of Personnel Management disclosed the biggest known breach of government-held personal information, also allegedly a foreign job. OPM is one of four representative agencies scrutinized that still does not always use effective access controls, the February 2015-May 2016 audit found. The other departments studied were the Veterans Affairs, NASA and the Nuclear Regulatory Commission. All 18 agencies that operate high-impact systems vital to society cited nation-state attacks as the most serious threat. All but three departments said they happened most often. Most frequently, agencies are alerted to incidents involving spearphishing emails with malicious links or attachments, GAO says. And those attacks -- emails tailored to deceive specific employees -- were rated the most serious at 17 of the 18 agencies. OPM and Auditors Dispute Findings of Security Testing. In response to a draft of the report, however, OPM argued the auditors did not supply the agency with enough details to cross-check the weaknesses categorized as "boundary protection" and "authorization" vulnerabilities. The agency also contended GAO did not fully describe the nature of the security weaknesses until a week before a response to the draft was due 2 May. OPM officials also disputed the final audit report. "While OPM and GAO are in agreement on most of their recommendations, we continue to disagree with GAO's security control assessments recommendation as written because it does not address the issues identified within the technical assessment, and suggests another cause for which no analysis was conducted and/or provided to OPM for review," OPM spokesman Sam Schumach told Nextgov in an email. Government wide, there were 500 incidents in fiscal 2014 that involved the installation of malicious code at agencies holding information that could cause catastrophic harm to individuals or the nation if lost, GAO said. At the four agencies GAO selected for testing, the departments hadn't always installed effective system login restrictions or patched software flaws that could allow hackers inside. Nor did they always have contingency plans in place to make sure the high-impact systems remained accessible, as well as maintained confidentiality and data integrity, the audit found. Each of the chosen agencies has been hacked by suspected nation-states in recent years. (NextGov, 21Jun16)

(U) Ransomware and SCADA access as a service are emerging threats for ICS operators
(U) Ransomware and services that sell access to Supervisory Control and Data Acquisition (SCADA) systems are quickly emerging as new challenges for operators of industrial control systems (ICS), management consulting firm Booz Allen Hamilton warned in a report released this week. Booz Allen's report is based on a review of publicly available information on threats targeting ICS operators and also a detailed analysis of 295 ICS incidents that the US Department of Homeland Security responded to in 2015. The analysis showed, somewhat unsurprisingly, that attacks against ICS operators are increasing. Nation state actors and criminal groups combined to make FY 2015 the most eventful year from a security standpoint, for ICS operators ever. The 295 incidents that DHS responded in 2015 represented a 15 percent increase over the previous year. Exacerbating the trend was the increasingly lower barrier to entry for threat actors seeking to target industrial control systems. The energy sector, as usual, was heavily targeted and accounted for 16 percent or 46 of the 295 incidents. But for the first time, organizations in the critical manufacturing sector, such as transportation equipment manufacturers, electrical equipment and component makers and primary metals manufacturers, experienced even more incidents. Booz Allen counted a total of 97 incidents against such organization last year, or 33 percent of the total number of incidents. The report attributed the increase to a single malicious campaign involving the use of targeted spearphishing to distribute malware. Spearphishing campaigns, as an initial attack vector against ICS operators jumped dramatically from 42 reported incidents in 2014 to 109 in 2015, a 160 percent increase in 12 months. Only 12 percent of the security incidents that the DHS responded to last year involved a compromise of the actual operational technology (OT) network. All of the others involved attacks against the network perimeter or the enterprise network. (Dark Reading, 17Jun16)

(U) Get ready for a surge in online travel fraud
(U) Unsurprisingly, transactions for booking flights, hotels and rental cars increase significantly over the summer months. In addition, fraudulent activity against online travel companies goes up during the same period. Iovation based these findings on its analysis of the hundreds of millions of online travel transactions and billions of total transactions that it screens for fraudulent indicators every year. Summer transaction trends Total transactions -- The amount of online travel transactions during an average summer month in 2015 was eight percent higher than a typical month the rest of the year, 39 percent higher in 2014 and three percent higher in 2013. Mobile usage -- During the summer, travel transactions from mobile devices increased at a higher rate than transactions from non-mobile devices. Travel transactions conducted from a mobile device during an average summer month in 2015 were 14 percent higher than a typical month the rest of the year, 40 percent higher in 2014 and 36 percent higher in 2013. Travel fraud -- The amount of fraudulent online travel transactions during an average summer month in 2015 was nine percent higher than a typical month the rest of the year, nine percent higher in 2014 and 23 percent higher in 2013. Mobile fraud -- More fraudulent travel transactions originating from a mobile device occurred during the summer months. Much like legitimate mobile purchases, online travel fraud originating from a mobile device increased during the summer months. It increased 18 percent during an average summer month in 2015, 11 percent in 2014 and 23 percent in 2013. Device type -- Android devices saw the largest increase in online travel transactions conducted from them during an average summer month in 2015 (16 percent) compared to a typical month the rest of the year followed by iPhones (13 percent). In 2014, Windows desktops and laptops (39 percent) saw the biggest increase followed by Macs (36 percent). In 2013, iPhones saw the biggest increase (59 percent) followed by Android phones (57 percent). "Our research shows that when people are out and about in the summer, they like to use their mobile device to book their travel and fraudsters like to do the same," said iovation's CTO, Scott Waddell. (helpnetsecurity.com, 17Jun16)

Incidents of Interest:

(U) Malware found on Maryland parking garage payment servers

(U) Annapolis, Md., officials spotted malware on parking garage servers that may have compromised customer payment information. On 11 June, SP+ Municipal Services, the company that owns the servers, launched an investigation after suspicious activity was detected on servers that handle payments for the Noah Hillman, Gott's Court and Knighton Garages, according to the Capital Gazette. The malware was capable of accessing card numbers, names, expiration dates and CVV numbers, officials said they don't know how many have been affected by the breach but believe it may have impacted anyone using the facilities between 23 December and 11 June, the report said. Officials said the breach might not have affected monthly parking or residential permit holders. The Maryland Attorney General has been notified of the incident and SP+ was brought in an outside security expert to conduct comprehensive investigation as well. (scmagazine.com, 22Jun16)

(U) DNC hacker Guccifer 2.0 releases files on Hillary Clinton

(U) Guccifer 2.0, the hacker who claims to be behind the cyber-attack on the DNC (Democratic National Committee) servers, has released eleven files on Hillary Clinton, the presumptive nominee of the Democratic Party for President of the United States in the 2016 election. Despite two reputable cyber-security firms coming forward and saying that hackers tied to the Russian government were behind the attack, Guccifer 2.0 continues to claim he's working as a lone wolf. The hacker previously released two batches of files, eleven in the first and twenty in the second. While both file dumps contained random documents, this time around, the hacker leaked only data relating to Hillary Clinton. More files are to be expected. Guccifer 2.0 says he donated the entire data trove to WikiLeaks, who'll be publishing in full in the coming weeks. (Softpedia, 21Jun16)

(U) Russian hackers were indeed behind DNC breach, claims another security firm

(U) One lone hacker has tried to take credit for the recent breach of the Democratic National Committee, calling it "easy". But some security researchers aren't convinced. On Monday, security company Fidelis Cybersecurity came forward, and agreed that expert hacking groups from Russia were indeed behind the attack. The malware involved was advanced, and at times identical to malware the Russian hacking groups have used in the past, Fidelis said in a blog post on Monday. It backs the conclusion that security firm CrowdStrike made last week, when the company said two Russia-based hacking groups were behind the breach. CrowdStrike was hired to mitigate the attack and blamed the breach on two expert hacking teams, codenamed "Cozy Bear" and "Fancy Bear", which are believed to have ties with the Russian government. CrowdStrike called them among the best hacking groups in the world. However, a day later, a lone hacker named "Guccifer 2.0" emerged online and took credit for the attack. Guccifer 2.0 mocked CrowdStrike and then posted some of the files purportedly stolen from the DNC. This included a 231-page dossier on Trump. On Monday, Fidelis said the company was brought onboard to analyze the malware used in the DNC breach. It performed its own independent review and found that the malware was similar to those Cozy Bear and Fancy Bear are known to use in the past. CrowdStrike also maintains that Cozy Bear and Fancy Bear are the true culprits, despite the claims from Guccifer 2.0. (IDG News Service, 20Jun16)

(U) Acer breach caused by improperly stored data

(U) The breach that compromised the information of nearly 34,500 Acer online shoppers was caused by the company "inadvertently" storing consumer data "in an unsecured format, the company reportedly told PCWorld. As a result, a hacker obtained unauthorized access to the data between 12 May 2015 and 28 April 2016, and was able to access to names, addresses, card numbers, expiration dates and three-digit security codes, Acer said in a breach notification filed with the California Attorney General. "Upon identifying this issue, we took immediate steps to fix the problem and are continuing to work with outside cyber security experts to enhance our security," an Acer spokesperson told SCMagazine.com via email. Acer subsequently notified law enforcement and those were affected. Mark Bower, HPE global director of product management, told SCMagazine.com via emailed comments that there is no reason Acer needed to store payment card data in any form on their systems. "Today, there are specific and simple to deploy technologies that mitigate the risk of cyber attacks to e-commerce sites," he said. "Thousands of leading merchants and well-known, name-brand online stores throughout the world have already adopted these approaches with great success, either on premises, or through payment processors services - with them, the risk of an attack being successful is absolutely minimized - attackers get nothing of value, just meaningless random data." Bower added that tokenization is the de-facto approach to avoid cardholder data from needing to be stored while still letting analytics and applications function without live data risks Acer sent a Notice of Breach letter to the affected customers. (scmagazine.com, 20Jun16)

(U) GoToMyPC hit with hack attack

(U) If you use Citrix's GoToMyPC remote desktop access service, you need to change your password. According to a post published to GoToMyPC's system status page, the service experienced a hack attack this weekend, and it's now requiring all users to reset their passwords before logging in to the service. "Unfortunately, the GoToMYPC service has been targeted by a very sophisticated password attack," the update reads. "To protect you, the security team recommended that we reset all customer passwords immediately". According to GoToMyPC, it wasn't immediately clear that it was experiencing an attack: On Saturday, users reported being unable to log into their accounts, and were being forced to reset their password. Several hours later, GoToMyPC warned users of the attack. Before you next use GoToMyPC, you'll have to reset your password. GoToMyPC recommends that you use a complex password that isn't just a word straight out of the dictionary. It also suggests using two-step verification to help prevent attackers from accessing your account. (PC World, 19Jun16)

OGA

[redacted]

[redacted] OGA

(U) Hackers steal 45 million forum account credentials

(U) The Canadian media company VerticalScope, which operates a number of support forums on a range of topics, was targeted by hackers who were able to obtain user information from around 45 million accounts. Although news of the massive security breach has just surfaced thanks to LeakedSource, which collects information on data breaches, the actual hack took place in February when over 1,000 support forums and websites on tech, sports and other topics were infiltrated by unknown attackers. Some of the most popular forums affected by the hack were Motorcycle.com, Pbnation.com, MobileCampsites.com and Techsupportforum.com. Luckily for the users of those and of the other countless other forums run by VerticalScope, as of now their user data has not been listed on the dark web or exposed publicly through a leak. In response to the hack LeakedSource said: "Given the massive scale of this breach, it is also likely that VerticalScope stored all of their data on interconnected or even the same servers as there is no other way to explain a theft on such a large scale. Passwords were stored in various encryption methods but less than 10 percent of the domains which account for a very small amount of leaked records used difficult to break encryption (less than a couple of million). Most of the records (over 40 million) were just MD5 with salting and this is insufficient". VerticalScope has acknowledge the hack, but refused to outright confirm it. The company has yet to make any public announcements regarding the security breach and it is currently investigating who and or what led to such a devastating attack on its systems. (BetaNews, 17Jun16)

Items of Interest

(U) Cyber Guard 2016 aims to manage complexity in invisible domain

(U) Between one million and ten million US homes and businesses are without power. An oil spill from a near-shore refinery is gushing into the waters off Texas and Louisiana. The port of Los Angeles is shut down due to a network outage. Visitors to exercise Cyber Guard 2016 here viewed mock newscasts detailing these scenarios as examples of the likely effects of a massive cyberattack. Navy Adm. Michael S. Rogers commands US Cyber Command and also directs the National Security Agency and serves as chief of the Central Security Service. He spoke on 16 June to exercise visitors, explaining that training to meet cyber threats has advanced since the first Cyber Guard exercise in 2012. This year's Cyber Guard brought together about 800 participants from 100 organizations. Representatives are here from the Department of Homeland Security, the Defense Department, the FBI, the Federal Aviation Administration, and other government agencies, as well as power companies, port facilities, allied foreign partners including Australia, Canada, and the United Kingdom, and ten National Guard teams representing thirteen states. The exercise scenario reaches into banking, corporate profits, and other business concerns most vulnerable to internet denial. Cyber Guard is part of a suite of annual exercises aimed at preparing critical defense and economic sectors to deal with cyber threats. Each set of exercises builds on the previous year's, with the training population constantly expanding, he noted. "This is our seed corn for the future," Rogers said. He noted that the service members assigned to Cybercom view themselves as "the warriors of the twenty-first century." Value and takeaways. Maj. Hannah Frost of the British army said her team has been to three Cyber Guard exercises and had "slightly different objectives" for the 2016 event. The Royal Air Force, Royal Navy, and a joint cyber unit joined together this year, she said, "to actually allow more developmental learning." While her team's focus was "definitely technical operator-level skills," she said, "what we actually found is that we've gotten a lot more than that out of it." Her team incorporated and emphasized intelligence analysis into its exercise play, and the greater focus on intelligence is something "we might want to take back into the United Kingdom," Frost said. A three-star UK officer visited the exercise, she said, "and he's interested in us reporting back to him about what we've learned." Exercises such as Cyber Guard are "absolutely critical" for UK forces, she said, and "we keep coming back, because we keep learning things. (homelandsecuritynewswire.com, 22Jun16)

(U) Cyber Command getting on the job training fighting ISIS

(U) The ongoing battles in Syria and Iraq between US and allied forces against ISIS is giving American Cyber Command forces its first combat experience, which is helping the force gain much needed experience at a very rapid pace. This according to Lt. General James McLaughlin, deputy commander of US Cyber Command, who testified and answered questions before the House Armed Services Committee on 22 June. "The war on ISIL is the first at scale opportunity to do that in support of US Central Command. In many cases this is the first actual live opportunity for these forces to conduct that type of mission. We've learned more in the last several months since it was announced publicly that we are supporting this and it's given us the opportunity to mature and plow back in lessons learned in a real circumstance that might have taken us several years to have learned, this is the nature of military operations," McLaughlin told the committee. The committee meeting was held for the Cyber Command leaders and for Thomas Atkin, acting assistant secretary of defense for homeland defense and global security office of the secretary of defense, to bring the elected officials up to speed on how Cyber Command is growing and maturing, along with how it is learning its trade of defending the nation and armed forces from a cyberattack. McLaughlin and Atkins also gave an overview of that growth along with a broad idea of what the organization is doing to prepare itself to handle future threats. McLaughlin noted that of the 133 planned cyber mission teams 46 are in place, up to strength and fully mission capable, while 59 are still in the process of being assembled and trained. The force itself now consists of 4,684 active duty, National Guard and reserve component members, but the goal is to have 6,187 troops eventually on staff. "The department's recent budget submission clearly reflects the high priority of this effort. Of the $6.8 billion of DoD's cyberspace budget request, $3.9 billion are designated for cyber security or cyber defense activities. This contributes to a broader $19 billion investment across the Administration on cybersecurity and in support of the Cybersecurity National Action Plan," Atkins said in his opening remarks. He added that any Combat Command commander can now call on Cyber Command for support. (scmagazine.com, 22Jun16)

OGA

[redacted]

(U) US, Israel team in cyber threat-sharing program

(U) The US and Israel announced today a bilateral threat sharing program that is expected to begin in the next few months. US Department of Homeland Security Deputy Secretary Alejandro Mayorkas and Israel National Cyber Head Dr. Eviatar Matania spoke of the agreement Monday in their respective speeches at the 6th Annual International Cybersecurity Conference, also known as Cyber Week Tel Aviv, according to The Times of Israel. "One of the lessons we learned is to go it alone is precarious; working together makes us stronger," Mayorkas said Monday at the conference according to the publication. "The cybersecurity threat is borderless. Information must be shared." Matania told reporters at the conference, the two countries will automatically compile and screen information, including of mitigation strategies, attacks and vulnerabilities, in "near real time" from various agencies and sources and will share what is deemed useful. (scmagazine.com, 21Jun16)

(U) Poorly crafted LogMeIn password reset email looks phishy, but isn't

(U) LogMeIn has been sending out password reset emails to some of its customers, to prevent account hijacking fueled by the recent spate of massive login credential leaks. Unfortunately, their own legitimate email looks too much like a phishing message that many customers began reporting them as such to the company: As SANS ISC handler Rob VandenBrink pointed out two of the links included in the message look "phishy", indeed. "The blog entry in the email (blog.logmeininc.com) is different than the blog on logmein's home page, which is at blog.logmein.com. And accounts.logme.in is a domain that truly looks like it was set up to steal credentials," he noted. "This is absolutely awful… sets off almost all of the phishing alarms I'm preaching my users," one commenter pointed out. "They have about 12 different blogs, so even going to logmein.com manually and looking at the blog linked there does not get you any info related to the stated issue (that's on a sub-blog of LogMeIn Pro / logmeininc.com)." Nevertheless, the emails are legitimate. "Accounts.logme.in is one of our publicly available domains, and the email you are looking at is ours," the company replied to a user who also believed that the password reset link looked like it might lead to a phishing page. LogMeIn, whose many products and services are widely used by businesses, did a good job forcing a password reset for accounts that might be endangered by the recent leaks, and by offering good advice on choosing a new password, as well as on spotting phishing attempts. Too bad they didn't follow it themselves, especially because their customers have been targeted with phishing emails just two weeks ago. (helpnetsecurity.com, 21Jun16)

(U) Pentagon prepares to launch mega database for screening national security workers

(U) The Pentagon next month is slated to launch one mega database for investigating the trustworthiness of personnel who could have access to federal facilities and computer systems. The Defense Information System for Security, or DISS, will consolidate two existing tools used for vetting employees and job applicants. The reboot represents a reform spawned by leaks of classified data and shootings on military bases, Defense Department officials say. DISS will provide "a common, comprehensive medium to request, record, document and identify personnel security actions," Aaron Siegel, alternate defense Federal Register liaison officer, said in a notification about the addition of the new system of records. An older background check-management tool, the Joint Personnel Adjudication System, will move into DISS and take on a different acronym JVS, or the Joint Verification System. The current Case Adjudication Tracking system, or CATS, which shares completed investigations with other agencies, also will sit inside the application bundle. The musical chairs is "part of the effort to reform the security clearance process within the federal government," according to the Defense Personnel and Security Research Center website. DISS will track decisions about an individual's eligibility to handle classified materials and fitness for employment, as well as suitability to enter government buildings and computer networks, Siegel says. The system also will aid with the "support of continuous evaluation and insider threat detection, prevention and mitigation activities," he says. Continuous evaluation relies on automated data checks, rather than the traditional method of re-investigating employees every five years. If all goes according to plan, DISS should interface with a new, massive information-sharing hub designed to flag potential traitors and other "insider threats." Both systems are key to continuous evaluation. DISS is expected to ping the hub for threat monitoring, a practice that exploits, among other profiling techniques, cybervetting. The research center considers that term to mean checking blogs, social media sites, and other Internet-based sources. An agency or contractor that has hired a security-clearance holder can keep an eye on the employee's activities using DISS, Siegel explains in the notification. The White House also can take a peek to assess potential administration appointees. In addition, US Citizenship and Immigration Services can look inside for "use in alien admission and naturalization inquiries," Siegel says. And records in the database can be searched during authorized counterintelligence activities to enforce laws that protect US national security. DISS is expected to go online 16 July, pending a comment period that ends 15 July. Last summer, the Pentagon temporarily unplugged JPAS as a precaution, after a historic breach of 21.5 million background check records. A vulnerability in an Office of Personnel Management tool that links to the system was discovered during a probe of the hack. (NextGov, 20Jun16)

(U) Navy creates a 'safe space' for cyber innovation

(U) With security threats to virtually every aspect of government operations, cyber warriors and technology developers need safe spaces to practice and develop tools without compromising existing networks. That's where the Naval Undersea Warfare Center Rapid Innovation Center comes in. RIC was designed to be a sandbox where devices, programs and innovative ideas can be tested at a safe remove from the rest of the warfare center, RIC innovation lead Steve O'Grady told GCN. By emptying an old storage facility that housed spare parts for submarines in Newport, R.I., the Naval Undersea Warfare Center freed up 3,200 square feet of space for the RIC. Navy officials visited Google and other companies using sandboxes to get a feel for how to shape the new innovation center. RIC takes advantage of what O'Grady called slack-hacks, time apart from their daily jobs when warfare center employees can work on real-world scenario that keep four-star admirals up at night. This creative time was made popular by Google, which gave employees about 20 percent of their time to work on a passion project with 80 percent of the day devoted to daily business tasks. The RIC is available to individuals and teams from elsewhere in the military to brainstorm and think outside the box, O'Grady said. (Government Computer News, 17Jun16)

(U) Hackers find security gaps in Pentagon websites

(U) High-tech hackers brought in by the Pentagon to breach Defense Department websites were able to burrow in and find 138 different security gaps, Defense Secretary Ash Carter said Friday. The so-called white-hat hackers were turned loose on five public Pentagon internet pages and were offered various bounties if they could find unique vulnerabilities. The Pentagon says 1,410 hackers participated in the challenge and the first gap was identified just 13 minutes after the hunt began. Overall, they found 1,189 vulnerabilities, but a review by the Pentagon determined that only 138 were valid and unique. The experiment cost $150,000. Of that, about half was paid out to the hackers as bounties, including one who received the maximum prize of $15,000 for submitting a number of security gaps. Others received varying amounts, to as low as $100. The Pentagon said this was the first time the federal government has undertaken a program with outsiders attempting to breach the networks. Large companies have done similar things. One of the hackers was David Dworken, who just graduated from high school. He said he worked on the program during his free time, logging in between homework assignments. He ended up submitting six vulnerabilities, but they all were reported by other hackers also. He said he started getting interested in hacking when he was in the 10th grade. "I took a computer science course at my school and then other students and I were actually just messing around and we found a couple vulnerabilities on my school's website. That's the first thing I did with that," the future Northwestern University student told reporters. Even though he didn't qualify for a payout, Dworken said it was worthwhile. "It also works well in terms of, like networking and getting a reputation kind of thing," he said. "You know, I'm just in high school. I've had recruiters contact me about internships over the summer". (AP, 17Jun16)

(U) Simple encryption algorithm allows decryption of Crypt38 ransomware

(U) A new ransomware family called Crypt38 uses a simple encryption routine that allowed Fortinet researchers to reverse engineer the process and find a method of unlocking files. Named Crypt38 because it appends the .crypt38 extension to all encrypted files, this ransomware's infection method is currently unknown. What we know is that the ransomware seems to be targeting only Russian users at the moment, and based on the simplistic encryption routine and low ransom demand, it may be in the testing phase, and users might get to see a much more powerful version in the upcoming future. Right now, the ransomware only asks for 1,000 Rubles (~$15) and doesn't require users to access a decryption website. To unlock files, infected users only have to send an email to the ransomware's author, which will reply with payment details and decryption details. Fortinet says that during the infection process, the ransomware generates a 12-digit random number to identify each user. It then takes this ID, runs it through a mathematical operation, appends "6551" at the end of the result and uses the final number as the encryption key. The problem is that the ransomware's author didn't use an asymmetric encryption, opting for a symmetric algorithm. This means the encryption key is also the decryption key. Since Fortinet researchers managed to crack the encryption routine, they say that by taking a look at each victim's ID number, they could compute the encryption/decryption key. Michael Gillespie created a free decryption key generator for Crypt38, which is available for download via Bleeping Computer. Users can enter their ID, and the keygen will spit out a decryption key. Before using the decryption key, users should back-up their data first, in case the decryption process fails. (Softpedia, 17Jun16)

(U) Facebook plans to track which stores you shop at, report data to advertisers

(U) Privacy advocates and Facebook have been at odds almost since the service made its public debut, and the company's latest plans to expand its advertising service aren't likely to play well with anyone who values controlling their own digital foot print. Facebook has added new measurement and information tools that are designed to make it easier for FB users to find businesses relevant to their interests, according to Adweek, while simultaneously handing those businesses an unprecedented amount of information about the customers that walk through their door. Here's how the system works: If you have location services enabled on your phone, Facebook will track which local ads it serves you, as well as your response to those advertisements. If you visit a partner store after seeing an ad for the company's products, Facebook will know it. This itself isn't necessarily new; Google debuted a similar service back in 2014 to track whether or not ads drove foot traffic to specific businesses. What does appear to be new, however, is Facebook's ability to track whether ads result in actual sales. Adweek reports: Along with measuring foot traffic, Facebook is also adding a way to connect which ads lead to actual sales -- at least at the cumulative level -- in stores or even over the phone. An Offline Conversions API will allow businesses to match transaction data from a customer database or point-of-sale system with Ads Reporting. The tool will also let businesses gather insights about demographics of the people who make a purchase... Facebook is also adding a store locator option for local ads, which will allow people to navigate their way to the nearest store from within the ad itself. The feature shows information such as address, hours, phone numbers and estimated travel time. As for Facebook's visit tracking and data collection, the company doesn't plan to share individual visitor information with any of its partners. The problem is, such information may be relatively easy to extract, depending on which demographic data the company chooses to share. For example, if a company knows that an unidentified male between the ages of 25-34 entered the store at 3:45 PM and left at 4:20 PM, Facebook could compare the latter timestamp against cash register logs to see if a male checked out by credit card around 4:17 PM. If someone did, that person's name can be run through other commercially available databases to determine if they're a probable match. This type of data mining itself isn't unusual -- it's the way corporations create detailed behind-the-scenes profiles on their customers. (extremetech.com, 17Jun16)

(U) Oversight lawmakers demand overdue data security plan from census
(U) For the first time in 2020, the federal government will allow millions of American households to fill out census forms using the internet. It's part of the US Census Bureau's grand plan to leverage technology in a bid to shave billions off the price tag for the decennial count. But even as the Government Accountability Office has listed cybersecurity as a "critical" challenge for the effort, bureau officials are nearly six months late in delivering a congressionally mandated report on data security procedures at the bureau. The report appeared to have fallen almost entirely off the bureau's radar until officials were prodded about it by members of the House Oversight and Government Reform Committee last week. » Get the best federal technology news and ideas delivered right to your inbox. Sign up here. In a 14 June letter to Commerce Secretary Penny Pritzker, the two top members of the oversight committee call the missed deadline "problematic," pressed the bureau to deliver the report by the end of the month and asked agency officials to hand over all documents and communications relating to the drafting of the report. "Many federal agencies store Americans' personally identifiable information (PII), but few if any agencies store more such data than the Census Bureau," wrote Reps. Jason Chaffetz, R-Utah, and Elijah Cummings, D-Md. In the letter, Chaffetz and Cummings called Census a "prime target" for hackers, pointing to last year's massive hack at the Office of Personnel Management, in which cyberintruders made off with background check data on more than 22 million federal employees and contractors. Last fall, Congress mandated the report into Census' data security practices be completed by 20 January. At an oversight hearing last week that examined the bureau's plans for managing the rollout of the 2020 census, Chaffetz questioned agency officials about the status of the report. In the letter, Chaffetz and Cummings sought Commerce Department communications between Pritzker and top agency officials about the data security report. The letter also seeks communications between Census officials and members of the bureau's IT shop. The committee wants responses by 28 June. As part of its tech plans for the 2020 count, Census is planning for up to 55 percent of American households to complete questionnaires via the internet. In a recent report, GAO warned of a possible rash of phishing attacks targeting both census respondents and employees. A phishing attack on a Census worker "could act as an entry point for attackers to spread throughout an organization's entire enterprise, steal sensitive personal information, or disrupt business operations," auditors concluded. At the hearing last week, Chaffetz said he had "deep concerns" about the bureau's internet-friendly plans. Census has already fallen victim to two data breaches over the past year, one last July and another in February. Harry Lee, Census' acting chief information officer, told lawmakers last week, the breaches were confined to external-facing websites. Some data that was already publicly available was exfiltrated, Lee said, but it was considered of "low sensitivity". (NextGov, 16Jun16)

(U) Cyberattack on NATO could trigger a military response
(U) NATO Secretary General Jens Stoltenberg said a cyberattack on a member state could trigger the defense organization's mutual defense agreement possibly resulting in a joint, conventional response to the attack. Stoltenberg made this comment, Reuters said, during an interview with the German Bild newspaper. He told Bild the type of response would depend on the severity of the cyberattack. NATO officially recognizes cyber as an official warfighting domain and its member states have agreed to a joint defense against such attacks. US officials are also debating the proper response to a cyberattack. In May Sen. Mike Rounds (R-S.D.), a member of the Senate Armed Services Committee (SASC), introduced The Cyber Act of War Act of 2016 that asks the administration to define whether a specific cyberattack would and would or not be considered an act of war thus enabling the United States to respond appropriately. Part of the problem facing NATO and the US would be determining the culprit in any attack. "The asymmetric nature of it (cyberwarfare) makes it hard to determine the culprit," Stratfor Security analyst Tristan Reed told SCMagazine.com, adding that for "most cyberattacks any conventional military response would be considered over the top". Stoltenberg said to Bild any response, be it cyber or kinetic, would only come after a consensus among NATO members is reached. (scmagazine.com, 16Jun16)

[redacted]

(b)(3) 10 USC ⊥ 424

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

[redacted]

(b)(3) 10 USC ⊥ 424