[redacted] Cyber-Threat Newsletter – 31 May 16

Patches & Updates of the Week:

(U) Recently patched Flash Player exploit is being used in widespread attacks
(U) It took hackers less than two weeks to integrate a recently patched Flash Player exploit into widely used Web-based attack tools that are being used to infect computers with malware. The vulnerability, known as CVE-2016-4117, was discovered earlier this month by security researchers FireEye. It was exploited in targeted attacks through malicious Flash content embedded in Microsoft Office documents. When the targeted exploit was discovered, the vulnerability was unpatched, which prompted a security alert from Adobe Systems and a patch two days later. As usually happens with zero-day exploits, it was only a matter of time until more cybercriminals got their hands on the CVE-2016-4117 exploit code and started using it in widespread attacks. On Saturday, a malware researcher known as Kafeine spotted the exploit in Magnitude, one of the most popular exploit kits used by cybercriminals. In order to stay protected users should make sure that they're running the latest version of Flash Player available for their browser and should also make sure that the other browser plug-ins are also up to date. (IDG News Service, 23May16)

(U) Cisco patches high severity flaws in its Web Security Appliance
(U) Cisco Systems has fixed four denial-of-service vulnerabilities that attackers could exploit to cause Web Security Appliance devices to stop processing traffic correctly. The Cisco Web Security Appliance (WSA) is a line of security devices that inspect Web traffic going in and out of an organization in order to detect malware, prevent data leaks, and enforce Internet access policies for users and applications. The devices run an operating system called Cisco AsyncOS. One of the four DoS vulnerabilities fixed Wednesday by Cisco stems from how the OS handles a specific HTTP response code. An attacker could send a specifically crafted HTTP request in order to consume the entire memory of an affected device. If this happens, the device will no longer accept new incoming connection requests, Cisco said in an advisory. All Cisco AsyncOS versions older than 9.0.1-162 are affected. Users are advised to upgrade to this version. Version 9.1 is also unaffected. Another DoS vulnerability is caused by a lack of proper input validation of the packets that make up HTTP POST requests. Only AsyncOS version 8.0 is affected by this vulnerability. Users can upgrade to 8.0.6-119 or 9.0.1-162, which contains patches for all four flaws, Cisco said in an advisory. The third vulnerability stems from a failure to free memory when a file range for cached content is requested through the WSA. By opening multiple connections and requesting file ranges, an attacker can cause the WSA to run out of memory and stop passing traffic. Versions 8.5 to 8.8 of AsyncOS are affected and Cisco recommends upgrading to 9.0.1-162. The fourth vulnerability occurs because AsyncOS does not properly allocate space for the HTTP header and an expected HTTP payload. Exploiting this flaw can cause the proxy process to reload and the traffic to be stopped. The flaw affects AsyncOS versions 8.8 and lower. Cisco has fixed the flaw in versions 8.5.3-069 for the 8.5 branch and 9.0.1-162. In addition to the WSA flaws, Cisco also patched a moderate severity cross-site scripting vulnerability in the Web interface of the Cisco Unified Computing System (UCS) Central Software. (IDG News Service, 19May16)

Threats & Vulnerabilities of the Week:

(U) FBI warns of wireless keystroke loggers disguised as USB chargers
(U) At the end of April, the FBI issued a public alert regarding KeySweeper, a piece of custom hardware created by security researcher Samy Kamkar as a proof-of-concept project, capable of stealing keystrokes from wireless Microsoft keyboards by intercepting nearby radio signals and decrypting the keyboard's protocol. The device works on top of an Arduino board, which is small enough to fit inside the case of a USB charger. Since USB chargers have become commonplace with the proliferation of mobile devices such as smartphones and tablets, seeing one such device plugged into a wall socket and abandoned in an office is not out of the ordinary these days. The FBI warns companies to limit the number of outlets available for device charging, to instruct employees to recognize whose chargers are currently plugged in, and not to leave any charger plugged into the wall if not used. Additionally, companies were also instructed to limit the usage of wireless keyboards, either by switching to wired keyboards or to ones that use Bluetooth for communications. However, if companies use Bluetooth keyboards, the FBI also recommends using encryption, along with a strong PIN. KeySweeper cannot harvest keystrokes from Bluetooth keyboards, with Kamkar only designing it for RF-based wireless keyboards created and sold by Microsoft. Of course, with the documentation out there in the open, anyone can very easily adapt it to other platforms and manufacturers. While it was doing damage control after Kamkar's announcement last year, Microsoft also said that keyboards that operate on the 2.4 GHz frequency and manufactured after 2011 are also safe because thoy use Advanced Encryption Standard (AES) encryption for securing keystrokes between the keyboard and the computer. Kamkar released the device in January 2015, but the FBI has only recently issued this alert, which means that it investigated at least one case where someone used a KeySweeper device to log keystrokes. (Softpedia, 24May16)

(U) Changing of the TidePool: Operation Ke3chang malware evolves as APT threat reappears
(U) Operation Ke3chang, the advanced persistent threat (APT) that in 2013 was discovered targeting Europe-based Ministries of Foreign Affairs, not only apparently remains active but also seems to be leveraging a new family of malware called TidePool. Palo Alto Networks reported yesterday that researchers within its Unit 42 research team recently uncovered a malware-based cyberespionage campaign launched against Indian embassies, worldwide. Victims are infected via spoofed phishing emails containing attachments of TidePool, a malicious program featuring a code base and certain behaviors that largely overlap with Ke3chang's previous malware of choice, a program called BS2005. According to Unit 42, TidePool is a remote access trojan (RAT) that allows attackers to read, write and delete files, as well as silently run commands. The malware opens by default in Microsoft Word and exploits a Microsoft Office vulnerability that allows remote attackers to execute code via crafted EPS (Encapsulated PostScript) images. Like BS2005, malware appears to be Chinese in origin. (scmagazine.com, 23May16)

(U) New DMA Locker ransomware is ramping up for widespread attacks

(U) The TeslaCrypt creators called it quits recently, but unfortunately for users, there's a new ransomware program that's ready to take its place. Called DMA Locker, this threat first appeared in January, but its encryption implementation was so flawed that it was hard to take it seriously. Researchers had no problem developing a file recovery tool for the first two versions. However, its authors have recently fixed all issues and malware researchers believe that with the newly released version 4, DMA Locker has reached maturity and might be the next thing to hit users in widespread attacks. Previous versions reached infected computers through weak or stolen remote desktop credentials. The new version, however, is distributed via Web-based drive-by download attacks that rely on exploit kits, meaning that a much bigger number of computers can potentially be affected. Another big change is that the encryption routine now relies on a command-and-control server to generate unique public and private RSA keys for each infection. The malware first generates a unique AES (Advanced Encryption Standard) key for every file that it encrypts. That key is then encrypted with a public RSA key and gets appended to the beginning of the file. In order to decrypt the affected files, users need the corresponding private RSA key that is in the attacker's possession in order to recover the AES keys for each of their files and then use those keys to decrypt their content. Once it infects a computer, DMA Locker will now wait for a connection with the server to be established so it can send a unique computer ID and have a unique RSA public key generated for it. The good news is that, for now, the server is not hosted on the Tor anonymity network, so it should be fairly easy to block by security products, preventing the malware from ever initiating its encryption routine. DMA Locker also stands out by how it chooses the files to encrypt. Almost all file-encryption ransomware programs have a list of file extensions that they will target. Instead, DMA Locker has a list of extensions that it will not touch, encrypting everything else and potentially causing more damage. It will also encrypt files on network shares where the computer has write access, even if those shares have not been mapped locally to a drive letter. (IDG News Service, 24May16)

(U) Cerber ransomware on sale in Russian darknet with new scripting features

(U) An email campaign facilitating the distribution of the Cerber crypto-ransomware has been tracked by security researchers at Forcepoint. Use of Windows Script files (WSFs) differentiates this campaign from earlier instances. WSFs are executable with the Windows wscript.exe utility and can contain scripts from any Windows Script compatible scripting engine in a single file. After successful execution of the file, the Cerber crypto-ransomware will be downloaded on the victim's system. Cerber ransomware is identified as a new Ransom-as-a-service (RaaS) offered on a Russian underground forum, according to a blog post by SenseCy. Previously, it has been distributed via exploit kits or email using a macro-enabled Word document files, but this is the first time WSFs have been used for this purpose, Nicholas Griffin, Forcepoint security researcher, said in a blog post. The attackers lure victims into downloading the malware through two different methods. A double-zipped file with a WSF inside attached to the malicious email as well as an unsubscribe link at the bottom of the email which is linked to the same ZIP file. In addition, heuristics-reliant security solutions might be bypassed due to the uncommon use of a double-zipped file with a WSF inside, invoice -related subject line, genuine-looking content, and an unsubscribe link. Cerber has the encryption capability without communicating with associated command and control C&C servers, but, Griffin wrote that Forcepoint has found weaknesses in the encryption implementation which could be used to partially decrypt the files. "Although the number of observed victims is low, the majority currently appear to be within the UK. However, this is likely to change over time," Griffin said. (scmagazine.com, 23May16)

(U) Your car can be held for ransom

(U) Today's connected cars are loaded with software and are internet-connected. They're also proving vulnerable to malware, including so-called "ransomware," where a car is disabled by malicious code until a ransom is paid. Recently, Kirsten Thompson, a partner in the National Technology Group at the law firm, McCarthy Tétrault came across cases of ransomware being installed via the USB port on connected cars. One way this happens is through an innocuous visit to the mechanic. "The mechanic plugs something into the USB port and runs a diagnostic," or the mechanic may simply be trying to install software updates, Thompson explains. "If I'm a bad guy, I can drop or send a USB that looks like it's come from the manufacturer. So the mechanic...sticks it into the USB port and malware is installed." "The malware will actually..."brick" a car, it will shut it down," Thompson adds, "and then a message appears saying 'if you pay us the money, we'll release the car'." She has even come across a case of an entire fleet of vehicles disabled by ransomware. The USB port is not the only source of the problem. "Cars are now becoming WiFi enabled, which means lots of interesting things can get pushed to you," she adds. Thompson points out that exposure to malware is likely to be a significant risk in the future, especially as cars themselves become convenient payment mechanisms. "I press a button and my car makes the payment. I've already loaded my debit or credit card on there," Thompson says. "Vehicles are now becoming point of sale devices, and a lot of the big malicious malware hacks in the past couple of years have been at point of sale devices...and that's one of the basic ways of installing malware". (cbcradio, 22May16)

(U) Petya and Mischa ransomware bundled in one malicious payload

(U) Cybercriminals have bundled Petya and Mischa ransomware together into one payload for the purpose of using brute force to infect users on multiple fronts. As intriguing as the satellites in the James Bond film GoldenEye that they're named for, Petya and Mischa deploy attacks on different levels of the victim's systems and are primarily distributed in targeted campaigns via malicious emails, according to a Malwarebytes blog post. The duo even plays off of each other's strengths and weakness. "Since PETYA can't do his evil work without administrative privileges, MISCHA launches when those can't be obtained," the threat actors behind the cyberattacks said in a bitmessage to new recruits, according the Malwarebytes post. Researchers suspect that the group behind the attack is also the same group that released the Chimera and the Rokku ransomwares. To avoid infection, they recommended that users pay more attention to their email attachments. (scmagazine.com, 20May16)

(U) Furtim malware can run AND it can hide

(U) The creators of the newly discovered "Furtim" appear to have gone the extra mile to ensure that their malware flies under the radar. Infiltration prevention firm enSilo recently analyzed the malware, discovered by a researcher with the twitter handle @hFireFOX, and dubbed it Furtim (Latin for "by stealth"). At the time of its finding, the malware scored a zero-percent detection rate from Google's anti-virus aggregation service VirusTotal. Yotan Gottesman, senior security researcher at enSilo, said in an email interview with SCMagazine.com, "None of the malware that we've ever witnessed was as thorough as Furtim is in their attempt to avoid detection by security products." The list of tools and techniques Furtim uses to conceal and protect itself is exhaustive. The Furtim malware doesn't arrive in a packed or compressed state that might trigger red flags with some AV programs. Instead, Furtim installs a downloader that opens up a backdoor on the victim's computer, through which malicious payloads can be delivered later. In its pre-installation phase, Furtim searches its intended host for security products and virtualized or sandboxed environments, and will cancel installation if any are discovered. "Furtim not only tests against a monstrous list of 400 security-related applications, but the authors also took great care to cover a range of security applications, as we also found esoteric products," said Gottesman. If the malware detects the presence of a DNS filtering service, it replaces any known filtering name servers to public name servers with no filtering mechanisms. To further frustrate victims, Furtim blocks access to almost 250 cybersecurity, anti-virus update and technical help web sites by replacing Windows' hosts file. Because an infected device must be rebooted before Furtim can fully embed itself, the malware also overrides any user- or admin-authorized reboot policies, to ensure that all downloaded malicious payloads run upon rebooting. Furtim disables Windows notifications and pop-ups, and changes certain configurations on its host machine to block access to the command line and task manager tools, which could otherwise help users detect or kill the malicious processes. Finally, Furtime collects unique identifiers from infected machines and sends it to the command and control (C&C) server to ensure that it only sends the malicious payloads one time to any given victim. This is a defensive measure against security researchers who might be trying to collect and study multiple samples. So far, the malware's agenda is mostly hidden. It has three payloads: The first is a power-saving configuration tool that disables sleep mode and hibernation, so the victimized system remains continuously connected to the C&C server unless shut down manually. The second is an aggressive, commercial credential stealer known as Pony Stealer. The third payload is more mysterious: it communicates the presence of virtualization environments and anti-virus products to the C&C server, but that is likely not its main purpose because the malware is already designed not to install in the first place under such circumstances. Citing a timestamp of 22 October 2015, enSilo believes Furtim has been in existence for around seven months. The C&C server is hosted at a Russian domain that resolves to several Ukrainian IP addresses. With that in mind, and considering that the malware's communications are configured to accept Russian, enSilo wrote that it would be "easy to point a finger at Russia. However, we cannot jump to those conclusions as threat actors typically hide their identity by masquerading as coming from a certain location". (scmagazine.com, 19May16)

Incidents of Interest:

OGA

OGA

(U) TeslaCrypt ransomware project appears to shut down, offers free decryption key
(U) An ESET researcher discovered yesterday that the vaunted TeslaCrypt ransomware operation shut down and is now offering a free decryption key that anyone can use to unlock their files. The researcher said he contacted the TeslaCrypt operators using their ransom website hosted on the Dark Web, via their support channel. Crooks admitted they were shutting down TeslaCrypt operations, and surprisingly, agreed to offer a master decryption key for all users. The crooks posted the decryption key on the regular Dark Web website where users came to pay the ransom. The decryption master key works for both TeslaCrupt v3 and v4 infections, which regularly appended a secondary file extension to each encrypted file in the form of .xxx, .ttt, .micro, or .mp3. (Softpedia, 19May16)

(U) LinkedIn invalidates millions of potentially compromised passwords
(U) A 2012 LinkedIn data theft may have affected far more users than originally thought, the professional networking site said on Wednesday. LinkedIn said in a statement that it was working to invalidate the passwords of some 100 million accounts after it "became aware of an additional set of data that had just been released that claims to be email and hashed password combinations of more than 100 million LinkedIn members from that same theft in 2012." It said it was "taking immediate steps to invalidate the passwords of the accounts impacted, and we will contact those members to reset their passwords. We have no indication that this is as a result of a new security breach." More than 6 million member passwords were stolen when LinkedIn was hacked in 2012. (Reuters, 18May16)

Items of Interest

(U) Tor to use never-before-seen distributed RNG to generate truly random numbers
(U) Tor developers have been working on the next iteration of the Tor network and its underbelly, the Onion routing protocol, in order to create a stronger, harder-to-crack anonymous communications system. To advance the project, the developer team schedules brainstorming and planning meetings at regular intervals. The most recent of these meetings took place last week, in Montreal, Canada. In this session, the team tested the next generation of the Tor network working on top of a revamped Onion protocol. The team says it implemented a new mechanism for generating random numbers, never before seen on the Internet. The Tor Project says it created something it calls "a distributed RNG" (random number generator) that uses two or more computers to create a random number and then blends these outputs. The end result is something that's impossible to crack without knowing which computers from a network contributed to the final random number, and which entropy each one used. The Tor team says their new distributed RNG system is so strong not even the people who designed the new protocol can predict its output. Tor devs finished the new distributed RNG system a few months back, and at the Montreal meeting, the Tor team tested it on a network with eleven Tor routers. Currently, the distributed RNG is in the code review and auditing stage. "It's a complex system with multiple protocol phases that involves many computers working together in perfect synergy," the Tor team explains. "As far as we know, a distributed random generation system like this has never been deployed before on the Internet". (Softpedia, 25May16)

(U) Opera Software shareholders back Chinese takeover bid
(U) More than 90 percent of Norwegian online browser and advertising company Opera Software's shareholders have backed a Chinese consortium's $1.24 billion takeover bid, clearing a big hurdle for the deal to go ahead, the buyers said on Wednesday. The bid was accepted by shareholders owning 90.6 percent of Opera's outstanding capital and 90.9 percent of the votes, preliminary numbers showed. The bidders had needed more than 90 percent by a 24 May deadline, and a source close to the deal told Reuters before the announcement that threshold had been cleared. The offer, unanimously endorsed by Opera's board, still needs approval from the US and Chinese authorities. The consortium is made up of Qihoo 360 Technology Co Ltd, Beijing Kunlun Tech Co, Golden Brick Silk Road (Shenzhen) Equity Investment Fund, and its Yonglian Investment affiliate. Opera has said the deal will allow it to reach more emerging market consumers. (Reuters, 25May16)

(U) Navy official sounds alarm on cyber workforce shortage
(U) The Navy is fighting a losing battle trying to keep cyber specialists in its workforce, according to Deputy CIO Janice Haith. There is a revolving door in which the Navy trains IT professionals who then go on to lucrative jobs in the private sector, Haith said 24 May at a conference hosted by Gigamon. The workers the Navy does retain face a tall order in securing both shipboard and land-based IT systems, she added. "We have a workforce which is not adequately prepared to do this, and we are definitely relying on industry to help us with that," Haith said, adding that the problem is not unique to the Navy but common across government. "You may see us outsource a lot more because we don't have the skill set for that." Officials from across the military services held a meeting on 23 May in which they discussed the shortage of civilian IT personnel based overseas, she added. Haith estimated that the Navy has spent about $700 million on cybersecurity tools since a 2013 breach, attributed to Iranian hackers, of the unclassified portion of the Navy Marine Corps Intranet. (fcw.com, 24May16)

(U) USNA graduates first cyber operations midshipmen

(U) The first 27 of the US Naval Academy's cyber operations majors graduate 27 May as part of the Class of 2016. The academy first announced its intention to offer a cyber operations major in spring 2013, and midshipmen of the Class of 2016 were the first to be able to select it. "It's really a humbling experience to be one of those plankowners," said Midshipman 1st Class Zac Dannelly. "It's so unique because it's not only the first time USNA has offered it, but really it's the first program of this kind in the nation. It's not just for our education and those coming behind us at USNA, but we're kind of paving the way for how this can be taught uniquely around the nation." The major provides a basic foundation in computer architecture, programming, data structures, networks, the Internet, database systems, information assurance, cryptography, and forensics. The technical aspects of the program are balanced with courses and electives in areas such as policy, law, ethics, and social engineering. The cyber operations majors will leave USNA with a deeper understanding of the technical and broader cyber applications in the military and national services. These midshipmen are headed to a variety of Navy warfare communities and the Marine Corps. "Cyber is all about people, technology and processes," said Capt. David Bondura, deputy director of USNA's Center for Cyber Security Studies. "Whether these students are going into the cryptologic warfare, air warfare, submarine warfare, surface warfare or special warfare communities, USNA is building a cadre of junior officers who are leaving here with an understanding of cyber operations -- with capability, competence and confidence. This is the one warfighting domain that genuinely affects everyone across the entire warfighting spectrum." USNA's location affords the capability to map the education directly towards what our nation and Navy needs, said Bondura. With resources such as the Pentagon, the National Security Agency, US Cyber Command and the Office of the Chief of Naval Operations in close proximity, it gives midshipmen the unique opportunity to provide operational relevance towards their education and research. "I was fortunate enough to be able to do an in-semester internship program with the National Security Agency," said Dannelly. "I'm able to learn the 'how-to' here at USNA and then see the 'why' -- the real-world applications and practices. Our location makes a drive to the NSA, State Department or the Pentagon very convenient, and the opposite is true for many of our guests who take their time to come speak with us." After completing USNA's cyber operations program, future officers can enter advanced study or potentially choose assignments with various military cyber-related forces in support of national security. (defencetalk.com, 24May16)

(U) DARPA extreme DDOS project transforming network attack mitigation

(U) Researchers with the Defense Advanced Research Projects Agency (DARPA) have quickly moved to alter the way the military, public and private enterprises protect their networks from high-and low-speed distributed denial-of-service attacks with a program called Extreme DDoS Defense (XD3). The agency has since September awarded seven XD3 multi-million dollar contracts to Georgia Tech, George Mason University, Invincea Labs, Raytheon BBN, Vencore Labs (two contracts) and this week to the University of Pennsylvania to radically alter DDOS defenses. One more contract is expected under the program. The UPenn project is developing defenses against distributed denial of service attacks that target specific protocols and their logic. These attacks are often difficult to diagnose and stop because the total volume of malicious traffic may be very low. The UPenn project attempts to pinpoint the specific protocol component that is under attack and then massively replicate that component to blunt the effects of the attack, DARPA stated. The current art in DDoS defense generally relies on combinations of network-based filtering, traffic diversion and "scrubbing" or replication of stored data (or the logical points of connectivity used to access the data) to dilute volumetric attacks and/or to provide diverse access for legitimate users. In general, these existing approaches fall well short of desired capabilities in terms of response times, the ability to identify and to thwart low-volume DDoS, the ability to stop DDoS within encrypted traffic and the need to defend real-time transactional services such as those associated with cloud computing and military command and control, according to DARPA. Responses to DDoS attacks are too slow and manually driven, with diagnosis and formulation of filtering rules often taking hours to formulate and instantiate. A clear need exists for fundamentally new DDoS defenses that afford far greater resilience to these attacks, across a broader range of contexts, than existing approaches or evolutionary extensions, DARPA stated. DARPA says the XD3 program looks to develop technologies that: Thwart DDoS attacks by dispersing cyber assets (physically and/or logically) to complicate adversarial targeting; Disguise the characteristics and behaviors of those assets to confuse or deceive the adversary; And blunt the effects of attacks that succeed in penetrating other defensive measures by using adaptive mitigation techniques on endpoints such as mission-critical servers. (Network World, 23May16)

(U) Marine cyber warriors will mess with their enemies' heads

(U) Unlike the other services, the Marine Corps is looking to build out offensive information warfare capabilities for Marine air-ground task forces, Brig. Gen. Loretta Reynolds, commander of Marine Forces Cyber Command, said at a recent panel discussion at the Sea-Air-Space expo outside Washington. Information warfare is more than just protecting networks or knowing the cyber terrain, she said. "It's also trying to get inside the enemy's cognitive space in a way to have him make choices that you want him to make, when you want him to make it," Reynolds said. "What we're talking about is bringing it all together in a way that provides the commander options to dominate the information environment and to get after the enemy's thought processes." Reynolds, appointed in July to her new dual billet of assistant deputy commandant for information warfare, is leading the charge to ready Marines for this global digital battlefield. The Marine Corps provides 13 teams to US Cyber Command and is already engaged in daily, toe-to-toe clashes with adversaries seeking to assault networks and disrupt operations. But getting Marines to make the necessary cultural changes has been a challenge, Reynolds said. That's changed, due primarily to having a commandant who "absolutely gets it," Reynolds said. When Gen. Robert Neller became 37th Commandant in September, he immediately made clear that information warfare would be a top priority. As he realized the need to bring in professional talent to build the cyber force, though, he was concerned about having to change recruiting standards, Reynolds said. "Do I have to start letting guys with purple hair and earrings in?" she recalled Neller asking. The answer: No. "You can let them in with purple hair but we're going to shave it off anyways and plug up whatever holes they have if they're smart enough," Reynolds added. Although recruitment and retention of cyber Marines has been a challenge, the results have been impressive, she said. "These young Marines are so brilliant: they're smart, have great ideas, and sometimes we just have to unleash them and let them solve problems for us," Reynolds said. (defensenews.com, 20May16)

(U) Navy retools cyber policy

(U) Navy Secretary Ray Mabus has made significant additions to the service's cybersecurity policy by requiring the implementation of a layered approach to cyber defense and the establishment of a departmentwide program to tackle insider threats. Navy organizations, including the Marine Corps, "shall implement a defense-in-depth/defense-in-breadth [cybersecurity] strategy to mitigate information security risks throughout the entire life cycle of a system or network," the memo states. It is dated 2 May but was released publicly this week. Defense Department officials have long espoused a defense-in-depth approach to cybersecurity that mirrors the multiple barriers an assailant often faces in attacking a government building, for example. Mabus is trying to drive home the point by reminding commanders that they will be accountable for implementing defense-in-depth. The memo also updates acquisition strategy by calling on officials to make sure cybersecurity is considered at every phase of a system's development and implementation. The memo also rebrands the DON Information Assurance Program as the DON Cybersecurity Program. (fcw.com ,20May16)

(U) NSA's GenCyber Camps to triple number of summer camps offered

(U) The National Security Agency (NSA) will triple the number of GenCyber Camps offered to 133 summer camps across the nation in 2016. The program's goal is to help grow the cybersecurity workforce of the future by offering students no-cost, and what the agency deems invaluable, hands-on education, according to a press release. The NSA also said it is expanding the list of hosts for the program from participating universities to non-profit organizations and K-12 school systems. "We are committed to helping the nation enhance cybersecurity education -- providing opportunities for both teachers and students to learn more about an issue that affects all of us and will continue to do so in the future," NSA's GenCyber Program Manager Tina Ladabouche said in the release. Officials are looking to grow the program to 200 camps by 2020. (scmagazine.com, 19May16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424