[redacted] Cyber-Threat Newsletter – 12 Apr 16

Patches & Updates of the Week:

(U) Adobe to patch critical Flash Player vulnerability

(U) Adobe is expected to release a security update as early as 7 April to fix a critical vulnerability (CVE-2016-1019) in Adobe Flash Player 21.0.0.197 and earlier that "could cause a crash and potentially allow an attacker to take control of an affected system." In a Tuesday security advisory, the company said it "is aware" of the vulnerability, which affects Windows, Macintosh, Linux, and Chrome OS versions, "being actively exploited on systems running Windows 7 and Windows XP with Flash Player version 20.0.0.306 and earlier." Adobe urged users to update to a current version of Flash Player that includes a mitigation introduced in 10 March Flash Player 21.0.0.182 update that will prevent attackers from exploiting the vulnerability. Adobe credited researcher Kafeine (EmergingThreats/Proofpoint) as well as Genwei Jiang of FireEye, Inc. and Google's Clement Lecigne for reporting the vulnerability. (scmagazine.com, 05Apr16)

(U) Three-year-old IBM patch for critical Java flaw is broken

(U) Security researchers have found that a patch released by IBM three years ago for a critical vulnerability in its own Java implementation is ineffective and can be easily bypassed to exploit the flaw again. The broken patch was discovered by researchers from Polish firm Security Explorations who found the vulnerability and reported it to IBM in May 2013. IBM issued a fix in a July 2013 update for its Java development kit. IBM maintains its own implementation of the Java virtual machine and runtime. This version of Java is included in some of the company's enterprise software products, as well as in the IBM Software Developer Kit, which is available for platforms like AIX, Linux, z/OS, and IBM i. "The actual root cause of the issue hasn't been addressed at all," Adam Gowdiak, CEO of Security Explorations, said in a message sent Monday to the Full Disclosure mailing list. "There were no security checks introduced anywhere in the code. The patch relied solely on the idea that hiding the vulnerable method deep in the code and behind a Proxy class would be sufficient to address the issue." This is the sixth time the company has discovered an ineffective patch from IBM for some of the Java issues that Security Explorations discovered, Gowdiak said. For one vulnerability, IBM released two broken patches in a row, he said. IBM, in a statement, said it is aware of the vulnerability and is working to address it. (IDG News Service, 05Apr16)

Threats & Vulnerabilities of the Week:

(U) Bill Gates/bot malware family used to launch DDoS attacks

(U) The Bill Gates/bot family of malware continues to be used to facilitate distributed denial of service (DDoS) attacks, allowing bad actors to seize full control of infected systems, according to a threat advisory from Akamai's Security Intelligence Research Team (SIRT), which ranked the risk factor as "high." The researchers noted that the attack vectors in the toolkit of the malware, which was revealed on a Russian website in 2014, include ICMP flood, TCP flood, UDP flood, SYN flood, HTTP Flood (Layer7), and DNS query-of-reflection flood. "This malware is an update and reuse of the Elknot's malware source code," the advisory said. "Over the years, the botnets composed of it have grown, and today's botnets are launching significantly large attacks." Akamai's SIRT believes the malware, like the XOR botnet, originated in Asia, with attackers "using the same methods for infection, which are primarily SSH brute force attempts for root login credentials." Previous reports, the researchers said, had the infection methods including an ElasticSearch Java VM vulnerability. In Q4 2015, Akamai SIRT noted that the XOR C2 had become inactive, presumably as part of a takedown operation. With XOR C2 out of commission, the attackers began to take aim at the same target list, using BillGates Botnet to launch DDoS attacks. Once the initial phases have been completed, resulting in the malware being rooted in the system, the malware runs a "multi-threaded" MainProcess function "responsible for opening communication with the C2 server (s), parsing commands, and launching DDoS attacks," the advisory said. The most popular payloads observed by the team SYN and DNS Floods. Attack campaigns, which vary from many to hundreds of Gbps, are aimed at Asia-based organizations, mostly in the gaming and entertainment sector. While the malware can spoof source addresses from infected machines, Akamai SIRT said more commonly the source in the attacks it observed were infected machines. "This is likely due to an inability to route spoofed traffic from the infected host's network," the advisory said. (scmagazine.com, 06Apr16)

(U) Millions of Firefox users vulnerable to browser extension flaw

(U) Security researchers have warned that hundreds of popular extensions for the Firefox browser have exposed millions of users to hack attacks. Researchers from the Northeastern University in Boston discovered a flaw that allows hackers to stealthily execute malicious code hiding behind a seemingly benign extension, such as NoScript and Firebug, and steal data. The flaw is attributed to a weakness in Firefox's extension structure, which fails to isolate various browser add-ons. This allows them to connect to the capabilities of other popular third-party extensions. "These vulnerabilities allow a seemingly innocuous extension to reuse security-critical functionality provided by other legitimate, benign extensions to stealthily launch confused deputy-style attacks," the researchers wrote in a paper presented at Singapore's Black Hat security conference. Hackers could exploit an extension reuse flaw by developing their own add-ons that hide malicious code and tap into the legitimate functions of popular extensions. Connecting to other legitimate extensions allows hacker-developed add-ons to bypass Firefox's security checks and extension vetting processes and gain access to a user's machine. The flaw affects extensions with large user bases, such as DownloadHelper, which has over six million users, and NoScript, which has two million, indicating that the scope of the vulnerability is significant. It is not clear whether the flaw has actually affected any users, as the researchers demonstrated it only as a proof-of-concept. They have supplied the attack framework to Mozilla so that the firm can improve the way it handles security in reviewing extension approvals. The flaw is likely to be bypassed when Mozilla moves Firefox to its new WebExtensions model that isolates extensions. The company has given developers 18 months to migrate add-ons to the new model before the old extensions are purged. (v3.co.uk, 06Apr16)

(U) DHS: Cyberattack on the Ukraine power grid could happen here

(U) A type of cyberattack that recently turned off the lights in Ukraine could bring any vital US sector to its knees, cautioned a top Homeland Security Department official. After leveraging a cribbed password, a group of unidentified hackers on 23 December 2015, knocked out power to 225,000 of the foreign country's customers for up to 6 hours. "Don't be deceived that this was only an electrical sector issue," said Ret. Brig. Gen. Gregory Touhill, DHS deputy assistant secretary for cybersecurity and communications. "This type of attack can happen in any critical infrastructure company across all sectors." The perpetrators used stolen credentials to remotely access power company networks, Touhill said Tuesday afternoon at the Billington Cybersecurity International Summit. The bad guys not only caused a blackout in Ukraine; they blunted efforts to restore power at the three affected electricity firms. The victims caught on to their tactics, but only after reverting to manual operations. "This was an actual dogfight between the electrical company operators and the hackers," Touhill said. One employee pulled out his Android smartphone and filmed a computer screen with a cursor moving seemingly of its own accord across the display, Touhill said. The adversary had gained control of the system. But score one for the good guys -- that hacked computer was a decoy. The unknowing attacker was trying in vain to flick switches on an offline system. After the attack ended, DHS analysts in January traveled to the scenes of the crime, where they saw evidence that some power supplies "were toasted" and hackers had crippled an emergency contact center to foil first responders, Touhill said. The telephone center could not receive calls from "the guys in the bucket trucks" that would normally descend on substations to manually regain control of power operations, he explained. The call center shutdown demonstrated the level of consciousness and forethought of the attackers, Touhill said. (NextGov, 06Apr16)

(U) Server software poses soft target for ransomware

(U) An alternate method for infecting computers with ransomware signals a shift in tactics by cybercriminals that could put businesses at greater risk, according to Symantec. A type of ransomware called Samsam has been infecting organizations but is not installed in the usual way. "Samsam is another variant in a growing number of variants of ransomware, but what sets it apart from other ransomware is how it reaches its intended targets by way of unpatched server-side software," Symantec wrote. The perpetrators behind Samsam use a legitimate penetration tool called Jexboss to exploit servers running Red Hat's JBoss enterprise application server. It means that ransomware attackers are more directly targeting businesses and organizations to install their malware. "Ransomware has proven to be a viable business model, so it should come as no surprise that the techniques used have shifted beyond malicious spam and drive-by downloads to those more closely resembling targeted attacks," Symantec wrote. Victims are usually asked to pay a ransom in bitcoin. The amount can range from a few hundred dollars up to thousands for businesses. One of the latest victims of Samsam was MedStar Health, a not-for-profit organization that runs 10 hospitals in the Washington, D.C., area, reported the Baltimore Sun. Most of its systems have been restored, but the organization has not indicated if it paid the ransom, which the newspaper reported was $18,500 in bitcoins. (IDG News Service, 05Apr16)

(U) U.S., Canada issue ransomware alert

(U) With new ransomware incidents popping up almost on a daily basis, the US Department of Homeland Security (DHS), in collaboration with Canadian Cyber Incident Response Centre (CCIRC), have issued an official ransomware alert. While the alert intended to educate the general population to the threat and how to combat becoming a victim it also recommends to not pay the ransom. "Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed," the statement said. The statement gives a primer on ransomware running through the types currently being favored -- such as Locky and Samas -- that it is spread primarily through phishing scams and what can happen to a computer's files if infected. (scmagazine.com, 05Apr16)

(U) FBI observes major uptick in business email compromise scams

(U) Between October 2013 and February 2016, 17,642 global businesses collectively lost $2.3 billion to business email compromise scams, whereby cybercriminals pose as company executives, attorneys or reputable vendors to trick employees into transferring corporate funds into fraudulent accounts, according to the FBI. In an alert issued yesterday by the FBI's Phoenix division, the agency said it has recently observed a "dramatic increase" in these scams, which are often pulled off by spoofing legitimate email accounts or via social engineering. More specifically, in 2015 the FBI saw a 270 percent increase in complaints from victims of this breed of crime. The FBI advised readers that these scams often attempt to spear phish specific employees who typically handle and manage corporate funds, and also tend to target businesses that work with foreign suppliers or regularly perform wire transfer payments. (scmagazine.com, 05Apr16)

(U) Black Hat Asia: Researchers find reusable vulnerabilities in popular Firefox extensions

(U) Flaws affecting popular Firefox extensions were disclosed by researchers at Black Hat Asia in Singapore. The reusable vulnerabilities were discovered by Northeastern Univeristy PhD candidate Ahmet Buyukkayhan and assistant professor William Robertson. The attacks use functionality from non-malicious extensions to bypass Mozilla's security checks and use elevated privileges of extensions to access browsing history, passwords, and user information. The team researched 2,000 Firefox extensions and found several Firefox extensions, including NoScript, Video DownloadHelper, and GreaseMonkey are affected. One of the extensions, NoScript, is a favorite extension commonly used to prevent malware infection by limiting code execution. These extensions have each been downloaded by millions of users. Robertson is a co-director of Systems Security Lab at Northeastern University and a consultant at Lastline Labs. There is no readily available patch for the extension vulnerabilities. It is suggested that users uninstall extensions. Mozilla did not reply to requests for comment by press time. (scmagazine.com, 04Apr16)

(U) Flaw in popular door controllers allow hackers to easily unlock secure doors

(U) Doors that provide access into secure areas in airports, hospitals, government facilities and other organizations can easily be opened by hackers due to a vulnerability into a popular brand of networked door controllers. The flaw exists in the widely used VertX and Edge lines of door controllers from HID Global, one of the world's largest manufacturers of smartcards, card readers and access control systems. HID's VertX and Edge controllers can be remotely managed over the network and have a service called discoveryd (discovery daemon) that listens to UDP probe packets on port 4070, according to Ricky Lawshae, a researcher with Trend Micro's newly acquired DVLabs division. When such a packet is received, the door controller responds with its physical MAC address, device type, firmware version and other identifying information, like the human readable name that was assigned to it. However, Lawshae found that discoveryd also responds to a command called command_blink_on that can be used to change the blinking pattern of the controller's status LED. When this command is received, the service calls the system () function to run the blink program with a number as argument. However, the input is not properly sanitized, which means that in addition to the regular input an attacker could inject Linux shell commands that would be executed as root, the highest privileged account on the system. "Since the device in this case is a door controller, having complete control includes all of the alarm and locking functionality," Lawshae said in a blog post. "This means that with a few simple UDP packets and no authentication whatsoever, you can permanently unlock any door connected to the controller." Trend Micro reported the vulnerability to HID and the company released a patch through its partner portal. However, as with most embedded systems, it will probably take a long time until all customers obtain and deploy the patch and some of them probably never will. (IDG News Service, 01Apr16)

(U) Security vulnerabilities found in US visa database

(U) Cyber security experts have found vulnerabilities in a US State Department system that could have allowed hackers to alter visa applications or steal data from the more than half-billion records on file, ABC News reported, citing sources familiar with the matter. The department learned after an internal review several months ago that its Consular Consolidated Database (CCD) was at risk of being compromised, though no breach had been detected, the report said. The CCD holds current and archived visa records and data, including names, photos, addresses, biometric data and identification numbers from the Bureau of Consular Affairs and is key to processing passport applications for visa applicants and travelers. There was no evidence that a cyber security incident had occurred pertaining to the CCD, a State Department spokesperson said in an emailed statement. The vulnerabilities stemmed from aging "legacy" computer systems that comprise the CCD, the ABC News report said. An official associated with the department's efforts to address the security concerns said a mitigation plan had already fixed the visa-related vulnerabilities, and further steps were being taken, ABC News said. (Reuters, 31Mar16)

(U) FBI issues warning over MSIL/Samas ransomware

(U) The FBI has begun seeking the assistance of companies in the US to streamline its investigation on an increasing ransomware threat in the country. The FBI is looking into a strain of ransomware called MSIL/Samas, which has been encrypting data across entire networks rather than single computers, Reuters reports. The ransomware infects machines before encrypting data and asking for money in return of the access. The investigating agency found that the group behind MSIL/Samas used Jexboss, a publicly available security program, to scan for vulnerable versions of the JBoss software, which will be followed by a malware attack on the vulnerable network, according to information Reuters has gathered. To the dismay of companies, the malware, called Peyta, also finds and deletes the back-up files firms could use to restore data by overwriting a key Windows system file called the Master Boot Record, and includes ransomware variants that use different methods to lock up systems and force victims to pay. IT firm Cisco said it saw Samas targeting firms involved in healthcare, wherein early versions of the malware charged a ransom of one bitcoin (£300, $432) for every machine hit. This amount was later increased later to 1.5 bitcoins. Cisco security analyst Nick Biasini said: "It is likely the malware author is trying to see how much people will pay for their files. They even added an option for bulk decryption of 22 bitcoin (£6,600, $9,500) to decrypt all infected systems". (BetaNews, 31Mar16)

Incidents of Interest:

OGA

(U) Biggest ever data leak reveals firms linked to world's most powerful people

(U) A data leak by a Panama firm selling offshore companies has exposed alleged illegal financial activities of some of the world's most powerful people in tax havens, Germany's Sueddeutsche Zeitung said Sunday. SZ, which says it has obtained the documents from the database of Panama-based law firm Mossack Fonseca, turned to the International Consortium of Investigative Journalists (ICIJ) to help them sift through this tremendous bulk of data. The trove of over 11.5 million secret files totaling 2.6 terabytes -- emails, pdf files, and files -- covers a period spanning from the 1970s to the spring of 2016. This is by far greater than the combined total of the Wikileaks Cablegate, Offshore Leaks, Lux Leaks, and Swiss Leaks, SZ estimated. The documents reportedly provide information on current and former leaders, as well as celebrities and others who allegedly laundered billions of dollars, evaded taxes and dodged sanctions with the help of shell firms abroad. Some of the companies were purportedly linked to prime ministers of Iceland, Pakistan, the Saudi King, presidents of Ukraine, United Arab Emirates, Argentina, the father of the British prime minister, the family of Azerbaijan's president, cousins of the Syrian president and a close friend of the Russian president. Mossack Fonseca responded by refusing to validate the information contained in the leaks and accused reporters of gaining unauthorized access to its proprietary documents. It warned that using unlawfully-obtained data was a crime that it would not hesitate to punish by criminal and civil means. Representatives of the above mentioned officials weren't available for immediate comment. (Sputnik, 04Apr16)

OGA

(U) Another Canadian hospital hit with ransomware attack, spreads TeslaCrypt

(U) Malwarebytes researchers spotted ransomware attack against another Canadian hospital. The website of the Norfolk General Hospital was spreading TeslaCrypt via an Angler exploit kit just days after an attack against another Ontario-based facility, Ottawa Hospital, according to a 21 March blog post. Researchers said the Norfolk General Hospital's web portal was powered by an outdated version of the Joomla content management system (CMS), the site was running version 2.5.6, while the latest version is 3.4.8. Malwarebytes said it contacted the hospital and officials told them they are working on updating their CMS. The attacks came during a string of ransomware attacks against hospitals in the US and Canada. Earlier this week, MedStar Health in Los Angeles was allegedly hit with a ransomware attack and in February Hollywood Presbyterian Medical Center was also struck. (scmagazine.com, 01Apr16)

(U) DHS reports over 300 incidents of ransomware on federal networks since June

(U) There have been 321 incident reports of "ransomware-related activity" affecting 29 different federal networks since June 2015, according to the Department of Homeland Security. The numbers indicate a form of malware that has done high-profile damage in the private sector is a threat to government computers as well. DHS relayed the information in a letter to Sens. Ron Johnson (R-Wis.) and Tom Carper (D-Del.) after the senators inquired about the spread of ransomware. Not all of the 321 incident reports involved a computer being infected with ransomware, according to DHS -- some were phishing emails or ransomware that was thwarted by an agency's security operations center. "In the cases where agency systems were confirmed to be infected with ransomware, the majority of infections affected end-user workstations," the letter said. "In all cases, the system was removed from the network and replaced with a new, clean system with minimal impact to the user and agency." DHS officials said they were unaware of cases in which federal agencies paid off hackers to remove ransomware. Since 2005, the FBI's Internet Crime Complaint Center has received 7,694 ransomware complaints totaling $57.6 million, DOJ said in its response. It is, however, difficult to pinpoint the cost of ransomware attacks because victims sometimes put a price on encrypted data based on its perceived value, wrote Peter Kadzik, assistant attorney general for legislative affairs. The two department's work closely together on ransomware: the FBI shares information about compromised US-based websites with DHS' US Computer Emergency Readiness Team to notify ransomware victims. Cooperation gets trickier outside the country. "One of the biggest obstacles with foreign law enforcement cooperation is that cyber crime laws vary by country," Kadzik wrote. "In some places, if there is a lack of victims in the actors' home country it is difficult to take any legal action against the suspect." The agencies' letters leave unanswered the question of how many "ransomware-related viruses" DHS and DOJ are tracking. DHS said its tracking scheme "does not currently allow for the calculation of the number of ransomware variants." The DOJ's response to the question is redacted because, spokesman Peter Carr told FCW, it contains "law-enforcement sensitive information". (fcw.com, 30Mar16)

Items of Interest

(U) Pentagon chief may upgrade CYBERCOM to full combatant command

(U) Defense Secretary Ash Carter is considering turning US Cyber Command into a full combatant command, an acknowledgment that cyberwarriors are today not just defending military networks but joining in combined-arms attacks on the enemy. Pentagon leaders long have said that cyber has joined land, sea, air and space as a new warfare domain. Especially in cyberspace, Carter said at the Center for Strategic and International Studies in Washington, "our reliance on technology has given us great strengths and great opportunities, but also led to vulnerabilities that adversaries are eager to exploit," It is time, Carter said, to "consider changes to cyber's role in DOD's Unified Command Plan." The military is currently organized into nine COCOMs: six geographic commands (Pacific, Europe, Africa, Middle East, etc.) and three that field specialized capabilities: special operations, nuclear (strategic) forces, and transportation. US Cyber Command, or CYBERCOM, is currently a sub-unified command under US Strategic Command. "I have given Cyber Command in the ISIL fight its first wartime assignment," Carter said Tuesday, referring to the historic role that network experts are playing in the Mosul offensive, described primarily as disrupting the group's communications, command, and control capabilities. "Increasingly, I've brought Strategic Command and Cyber Command into these operations as well to leverage their unique capabilities in space and cyber to contribute to the defeat of ISIL. Beyond terrorism," Carter said. "A couple of years ago, that would never have occurred to a secretary of defense." The calculation has changed largely as a result of ISIS' own behavior and what the Defense Department perceives as the need to fight ISIS on the group's own turf, inside online communications networks. He described the thinking as: "Hey, these guys are using this tool. We need to take it away." Adm. Michael Rogers, commander of Cyber Command, told the Senate on Tuesday morning his unit was ready for the upgrade. Appearing before the Senate Armed Services Committee, he discussed the future of the fledgling Cyber Mission Force and defending networks and as part of the so-called Third Offset, the Defense Department's bid to develop technologies to secure technological advantage. "US CYBERCOM stands ready to help develop and deploy the new cyber capabilities entailed in the Third Offset, particularly hardened command and control networks and autonomous countermeasures to cyberattack," he said. Becoming a Combatant Command "would allow us to be faster, which would generate better mission outcomes," he said. (NextGov, 06Apr16)

(U) DOD lacks clear chain of command for domestic cyber attacks

(U) Despite increased public interest and attention to cybersecurity, the Defense Department has not defined how it will support civilian authorities in the event of cyber attacks, according to a Government Accountability Office report. Several federal agencies lend a hand during disasters, with the Department of Homeland Security designated as the lead agency. DOD's responsibilities include supporting civilian law enforcement agencies, restoring public health and providing support for national special security events. Additionally, DOD can, when authorized, provide military forces such as National Guard, as well as civilian and contracting personnel. Because it plays a crucial role in confronting cyber threats to critical infrastructure, the Defense Department must also be prepared to support civil authorities in cyberspace, GAO said. However, GAO found DOD has not identified the roles or responsibilities that could be called upon in such a cyber incident. It is also unclear which combatant command would be designated to support civil authorities -- the Northern Command, which is responsible for the geographic region of the United States, or the US Cyber Command, which is in charge of global cyber operations. Additionally, DOD has not identified the role of the dual-status commander -- the commander who has authority over both federal military and National Guard forces -- when it comes to supporting civil authorities in cyber incidents, GAO said. When asked about the GAO report by senators in an appearance before the Senate Armed Services committee 4 April, Cyber Command Commander Adm. Michael Rogers said that while he had not yet read the report, he is familiar with the issues it raised. "US Cyber Command and DOD writ large provide our cyber capabilities in the defense of critical infrastructure in the private sector in partnership and in support of DHS," Rogers said. However, "DOD is not resourced or tasked to defend every single computer in the US," he added. "DHS has overall responsibility in the federal government for the provision of government support to the private sector when it comes to cyber." GAO recommended that the Defense Department clarify how it will support government agencies in the event of a domestic cyber incident. A comprehensive plan for Cyber Command to support civil authorities in response to cyber attacks is due to Congress in May 2016, GAO noted. (Government Computer News, 05Apr16)

(U) UL takes on cybersecurity testing and certification

(U) Underwriters Laboratories (UL) today announced a new Cybersecurity Assurance Program (CAP) that uses a new set of standards to test network-connected products for software vulnerabilities. The new UL certification will be for both vendors of Internet of Things (IoT) products and for buyers of products who want to mitigate risks. The testing standards were developed as part of a voluntary program involving industry officials as well as academics and the US government. UL also noted that CAP will be used to test and certify IoT devices within critical infrastructures such as energy and utilities, as well as healthcare. UL CAP will evaluate both the security of network-connectable product and sytems as well as the processes used by vendors for developing and maintaining the security of products and systems. UL's CAP will rely on a publicly-available government vulnerability database kept by the National Institutes of Standards and Technology that tracks and enumerates product vulnerability worldwide and is updated daily. It has a multitude of product lists, including desktop and mobile platforms. It also lists flaws and patches and identifies which version of software has a patch to address a specific security flaw. Pricing for the UL testing is still being developed. UL, an independent company, has been providing safety-focused advice, including testing and certifications, in the sciences for more than 120 years; it has 67,000 clients. (Computerworld, 05Apr16)

(U) State Department official says capacity building 'critical' for cybersecurity

(U) A top official for the State Department's cyber bureau said the need for capacity building, which he described as everything from fighting cybercrime to countering violent extremism online, is essential to sustaining the progress made on the administration's International Strategy for Cyberspace. "Capacity building efforts are really critically important," the Coordinator for Cyber Issues Christopher Painter said at the National Press Club audience on 5 April. The former prosecutor, who has been leading the charge at State to implement the administration cyber strategy introduced in 2011, said success depends on getting countries around the world to make sure "they have the right policies in place, the right structures in place and .. are taking it seriously." Using the examples of the Cyber National Action Plan and the NIST cybersecurity framework as successes, Painter said "the issue over the next five years is getting more and more countries to sign up with this framework." The framework specifically notes that, as "cybersecurity is a global issue that must be addressed with national efforts on the part of all countries, we will expand and regularize initiatives focused on cybersecurity capacity building -- with enhanced focus on awareness-raising, legal and technical training, and support for policy development." Technical threats are constantly evolving, according to Painter, but he stress that the "policy threat" also must be constantly evaluated. An example would be when more repressive countries attempt to "draw up sovereign boundaries around their cyberspace" and take a different view of how technology needs to work. The United States must anticipate such challenges, Painter said at the Press Club event, and put the right policies in place to prepare for them. "This is really not he said. (fcw.com, 05Apr16)

(U) DHS issues solicitation for Security Operations Center

(U) The Department of Homeland Security is soliciting for a new contract, worth up to $395 million, to run the DHS Security Operations Center (SOC). DHS is looking for contracting support to accomplish one of the agency's core missions: detecting, analyzing and responding to cyberthreats. DHS provides a range of cybersecurity services to other agencies, but the agency also needs help with its own networks, which are overseen by the SOC. Running the SOC isn't a simple task: the agency operates "as a federated model," so analyzing internal cyberthreats requires direct monitoring from the main SOC and coordinating with other SOCs within the agency, according to a statement of work. The contractor would be in charge of just about every cybersecurity service imaginable, including network monitoring, vulnerability assessments and intrusion analysis. The SOC's charge includes protecting the agency's wide area networks, Internet gateways, security devices, servers and workstations. The new contractor will have to keep the SOC fully up and running during the transition from the previous contractor. In 2008, Verizon won a 10-year, $678.5 million contract that included implementing the SOC. The solicitation includes an attachment that asks interested firms to respond to a hypothetical threat scenario: an analyst observes large-scale data exfiltration carried out by an IP address belonging to an advanced persistent threat actor. The solicitation process began over a year ago with an industry day hosted by DHS' acquisition institute. The contract has a one year base plus six additional one-year options. Responses are due 13 May. (fcw.com, 04Apr16)

(U) DOD wants tools to support cyberstrategy

(U) It's been a year since the Defense Department unveiled a cyber strategy to signal both friend and foe that the US military was serious about the digital domain. Now DOD officials are calling on tech firms to provide a host of tools to complement the strategy, starting with a pitch session this summer. In June or July, DOD's Rapid Reaction Technology Office, whose mandate is to "provide a hedge against technical uncertainty," will host a demonstration session for firms to show off their technical capabilities, according to a DOD notice. Defense officials are looking for capabilities listed under categories such as situational awareness; insider threat detection; wireless, embedded and industrial control systems; malware detection; forensics and analysis; enterprise and cloud security services; and big data. The capabilities sought by RRTO take trends in cybersecurity technologies and adapt them to Pentagon needs. Interest in "IP-enabled command and control paths" and "autonomous planning and reasoning" are two examples of that tailoring. The pitch session matches up directly with the Pentagon's goal of building and maintaining adept forces and capabilities. The RRTO notice expresses interest in the security of the industrial control systems that underpin US infrastructure. Officials are seeking "network discovery and mapping for wireless and ICS networks," and ICS "centralized security management," the document states. Firms that impress Pentagon officials at this summer's pitch session could be chosen for a pilot project or another form of experimentation, according to the notice. RRTO anticipates some 150 to 200 registrants for the event, according to Pentagon spokesman Maj. Adrian Rankine-Galloway. The department won't be naming the firms registered, he added. Companies have until 19 April to apply for the pitch session. (fcw.com, 04Apr16)

(U) Army looks to the 'micro cloud' for cyber defense

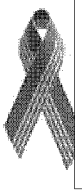
(U) The Army has challenged technology firms to make strides in the micro-cloud computing architecture that the service considers foundational for cyber defense, with a goal of awarding a prototype contract in 90 days. On 31 March at the Defense Department's Silicon Valley outpost, known as the Defense Innovation Unit Experimental (DIUX), Army officials hosted an information session with technologists to frame the challenge and drum up interest. The goal is to use an "agile contracting vehicle that helps us..better move at the speed of the commercial sector," said Lt. Col. Ernie Bio, US Cyber Command's lead for DIUX, in a call with reporters. The 90-day turnaround for awarding a contract would be rapid for a defense acquisition system that has struggled to keep up with private-sector innovation cycles. But Army officials point out that a similar cyber challenge initiated last year led to the award of more than $4 million in micro-cloud contracts. Those capabilities have been delivered to the cyber protection teams that make up the Army's defensive force, said Jack Dillon, who leads the Advanced Concepts and Technology Directorate at Army Cyber Command. The latest challenge seeks new ways to manage micro-cloud infrastructure, which DIUX said is characterized by "commonly abstracted and controlled hardware suites" that comprise a vast and varied resource pool. Ian MacLeod, a technology adviser at Army Cyber Command, said Army missions run on a diverse array of networks, and he sees great promise in computing systems that can be quickly installed anywhere in the world. (fcw.com, 01Apr16)

(U) US Marine Corps expands with new hacking unit

(U) The US Marine Corps announced last week plans to expand US Marine Corps Forces Cyberspace (MARFORCYBER) with a new unit called Marine Corps Cyberspace Warfare Group (MCCYWG). MARFORCYBER was set up in 2009, after leadership realized the need to deal with cyberspace threats while on offensive and defensive operations. MARFORCYBER launched at the same time the US Cyber Command (USCYBERCOM) was created, and similar divisions were also set up, such as the Navy's US Fleet Cyber Command (FLTCYBER), Army Cyber Command (ARCYBER), and Air Force Cyber Command (AFCYBER). This new unit, MCCYWG, will have to man, train and equip Marine Cyberspace mission teams under the command of MARFORCYBER and USCYBERCOM. Their role is unclear at the moment, but in simplified terms, they'll have to build small hacking units to assist ongoing operations of the US Marine Corps. (Softpedia, 01Apr16)

(b)(3) 10 USC ⊥ 424

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



(b)(3) 10 USC ⊥ 424