[redacted] Cyber-Threat Newsletter – 26 Apr 16

(b)(3) 10 USC 424

Patches & Updates of the Week:

(U) Oracle patches 138 bugs, 9 in Java, 31 in MySQL

(U) In its quarterly update train, Oracle addressed 136 security issues in 49 different product suites, among which were the Oracle database, Java, MySQL, Solaris, VirtualBox, SPARC, and Berkeley DB. This Critical Patch Update (CPU) is the first one Oracle released using the CVSS 3.0 system instead of the old one, CVSS 2.0. The Common Vulnerability Scoring Standard (CVSS) 3.0 was introduced in June 2015 and allows a more accurate classification of security problems, with grades from 0 to 10. Oracle released April's CPU with both CVSS 2.0 and 3.0 scores. As for the actual fixes, the MySQL database received the most patches, 31, followed by the Oracle Fusion Middleware with 22, and Oracle Sun System Products Suite with 15. Java also received nine patches, four of which were labeled critical, one high, three medium, and one low priority. The four Java critical issues were CVE-2016-3443, CVE-2016-0687, CVE-2016-0686, and CVE-2016-3427. The first three are easy to exploit via various network protocols but require human interaction in order to execute their malicious code. The fourth is a little bit more difficult to exploit, but if successful, attackers may also impact additional products. Users should update to the latest Java version, which is Java 8u92. (Softpedia 20Apr16)

(U) VMware plugs critical information-leaking hole

(U) VMware has plugged a critical security issue in the VMware Client Integration Plugin, which could allow for a Man in the Middle attack or web session hijacking in case the user of the vSphere Web Client visits a malicious website. The vulnerability (CVE-2016-2076) is due to incorrect session handling, and could lead to disclosure of sensitive information. The buggy plugin is found in vCenter Server 6.0 (any 6.0 version prior to 6.0 U2), vCenter Server 5.5 U3a, U3b, U3c, vCloud Director 5.5.5, and vRealize Automation Identity Appliance 6.2.4. "In order to remediate the issue, both the server side (i.e. vCenter Server, vCloud Director, and vRealize Automation Identity Appliance) and the client side (i.e. CIP of the vSphere Web Client) will need to be updated," VMware has explained in an advisory. No additional details about the vulnerability have been shared, but it's likely not being exploited in the wild, as the company would surely say so if it is. Nevertheless, updating affected installations as soon as possible is a good idea. (helpnetsecurity.com 15Apr16)

Threats & Vulnerabilities of the Week:

(U) 'Multigrain' variant of POS malware crops up; uses DNS tunneling to steal data

(U) Whoever says "Multigrain" is good for you obviously hasn't run into the point-of-sale malware that goes by this nomenclature. A variant of the NewPosThings POS malware family, dubbed Multigrain, has introduced a interesting wrinkle -- exfiltrating stolen payment card data from POS systems via the Domain Name System (DNS), as opposed to via HTTP or File Transfer Protocol (FTP), FireEye explained in its threat research blog on Tuesday. Because DNS is conventionally used to translate domain names into IP addresses, and not to transfer general data, the system is often overlooked by cybersecurity officials when assessing potential threats to their organizations. While HTTP or FTP traffic might be closely monitored or restricted to prevent unauthorized external queries, the DNS "is still necessary to resolve hostnames within the corporate environment and is unlikely to be blocked," explains the FireEye blog. Consequently, DNS remains vulnerable to cyber intruders, making this tactic especially appealing to sneaky cybercriminals. Another of Multigrain's quirks, according to FireEye, is that it is uniquely designed to target systems that run the specific POS process multi.exe, which is associated with a popular back-end card authorization and POS server software package. The malware will simply delete itself if the POS system in question does not run this particular process; but if the process is detected, then Multigrain installs itself. FireEye suggests that this means the attackers are likely familiar with how to exploit the multi.exe process in particular. Once executed, Multigrain scrapes the memory of the multi.exe process, looking for Track 2 magnetic stripe data, which normally includes a payment card's Primary Account Number, expiration date, service code and CVV/CVC number. The malware checks every five minutes to see if this data is ready for exfiltration via DNS query. SCMagazine.com contacted FireEye to provide additional details on the Multigrain variant, including its most common method of delivery and propagation, but researchers were not available on Tuesday to answer questions. (scmagazine.com 20Apr16)

(U) Python malware slithers its way into European organizations

(U) A strain of malicious code written entirely in Python, dubbed PWOBot, has been discovered infecting a number of organisations based in Europe, specifically in Poland. Palo Alto Networks found that PWOBot uses a modular design allowing it to carry out different attacks in a wealth of functionalities that include logging keystrokes, executing files, executing arbitrary Python code and communication with a remote server. The malware has been attacking since the end of 2013 in at least 12 different variants. Some distribution routes of the malware include a Polish file-sharing web service known as chomikuj.pl, a Polish national research institution, a Polish shipping company, a Polish retailer, a Polish info tech organization, a Danish building company and a French optical equipment provider. "It is unclear how this malware was originally delivered to the end-user. Inferences can be made based on the filenames witnessed, as this malware may have been delivered to end-users who believed they were downloading other software. Alternatively, it's possible that phishing attacks were used in order to entice victims into downloading these files," Palo Alto's blog noted. The malware family has not previously been disclosed to the public. The PWOBot uses the Tor network to communicate with remote servers, which could assist organizations in spotting it on their systems. "While (Tor) provides both encryption and anonymity, it also should raise alert's to an organization's network administrators if viewed, as such traffic likely violates said organization's policies," Palo Alto said. (scmagazine.com 19Apr16)

(U) New CryptXXX ransomware locks your files, steals Bitcoin and local passwords

(U) CryptXXX is a new ransomware variant discovered during the past weeks, which, besides encrypting the user's data, is also capable of stealing Bitcoin from infected targets, along with passwords and other personal details, security researchers from Proofpoint have found. The first signs of the CryptXXX ransomware appeared towards the end of March. Security experts say the ransomware is distributed via Web pages that host the Angler exploit kit. This crimeware kit uses vulnerabilities to push the Bedep click-fraud malware on the users' systems. After infecting users, the ransomware changes the users' wallpaper with its ransom note and drops text and HTML ransom notes all over your computer. You can spot CryptXXX infections by the ransom notes, which are named de_crypt_readme.txt and de_crypt_readme.html, or by the extension they add to all encrypted files, which is .crypt. The standard ransom note asks for 1.2 Bitcoin, which is roughly $515 (€455), a sum that is well above the average of recent ransomware infections. In past infections with the Bedep click-fraud malware, Proofpoint said it also saw Bedep deliver an infostealer component. After an in-depth analysis, it was revealed that this is also true with CryptXXX, which too includes such a feature. CryptXXX is capable of harvesting information and credentials about the user's local instant messenger clients, email clients, FTP clients, and Internet browsers. Proofpoint has also said CryptXXX can "steal Bitcoin" but has not elaborated on how this takes place. But the most interesting detail about CryptXXX comes at the end of the company's analysis. Having a closer look at the big picture, Proofpoint saw similarities between CryptXXX and the older Reveton ransomware. Similarities to Reventon include details such as the fact that both ransomware families were coded in Delphi, both use a delayed start, DLLs are called with a custom entry function, both include Bitcoin and credential stealing functions, and also use a custom C&C protocol on TCP 443. Even worse, all clues point to the fact that CryptXXX was created by the same criminal group that came up with the Angler exploit kit itself, the Bedep click-fraud malware, and Reveton in the past. Taking into account that the person behind Bedep, Angler, and Reveton is the same as the one behind even older tools such as the Cool exploit kit, "Given Reveton's long history of successful and large-scale malware distribution, we expect CryptXXX to become widespread," Proofpoint researcher Kafeine explains. Based on the large number of translations available for the payment page, it appears that the Reveton team shares those expectations". (Softpedia 19Apr16)

(U) Beware of emails with JavaScript attachments

(U) Malware peddlers are always looking for the next trick to get users to infect their computers. According to Microsoft and other sources, the current latest trick is malicious JavaScript attachments. The spam campaigns delivering these attachments range from blank emails pretending to deliver a business cards and fake "order status" emails, to bank-related and resume-themed spam. The malicious attachment usually comes in the form of a ZIP or RAR archive file, and once unpacked, the files sport a .js or .jse extension. Clicking on them (i.e. running them) starts a process that results in malware -- usually ransomware or a banking Trojan -- being downloaded on the victim's computer from a malware-hosting site. "The JavaScript attachments are heavily-obfuscated to avoid antivirus software detections. In some cases, the malicious JavaScript attachment is bundled with a dummy file to evade email rules," Alden Pornasdoro of the Microsoft Malware Protection Center noted, and pointed out that this approach requires at least one less click by the victim when compared to the "Office attachment with malicious macros" malware delivery method. "Be wary of emails with JavaScript attachments. It is uncommon and quite suspicious for people to send legitimate applications in pure JavaScript file format via email. Do not click or open it," he advised. (helpnetsecurity.com 19Apr16)

(U) Congress investigation to probe SS7 mobile network security flaws

(U) A 60 Minutes feature on the security flaws found in the Signalling System No. 7 (SS7) telephony signaling protocol has sparked a Congress investigation after US Representative Ted Lieu didn't like being spied on for CBS' experiment. CBS reporter Sharyn Alfonsi, together with Karsten Nohl, a German computer hacker and member of the Chaos Computer Club, has carried out an experiment that showed how easy it is to exploit design flaws in the SS7 telephony signaling protocol to track users anywhere on the planet, and even eavesdrop on their conversations. To prove their point and make an impact, Mrs. Alfonsi recruited US Representative Ted Lieu and convinced him to use a brand new iPhone when talking to his staff. Knowing only Mr. Lieu's phone numbers, Mr. Nohl and his team of experts from Security Research Lab were able to pinpoint his location at any time he carried the handset and also recorded all conversations he had with his employees. Following the airing of the 60 Minutes piece last Sunday, Mr. Lieu called on Monday for a full investigation into the widespread SS7 security flaws affecting US mobile networks and also international telephony systems. Because of its central role, if a vulnerability exists -- and it has since late 2014 -- attackers could gain access to any mobile network's backend and track everything and anything about a mobile operator's clients. While SS7 implementations differ slightly from country to country, their system is generally universal, and Mr. Nohl claims that these types of attack should work, at least in theory, anywhere in the world. (Softpedia 18Apr16)

(U) US-CERT tells Windows users to quit QuickTime

(U) The cyber readiness team that's part of the US Department of Homeland Security has advised Windows users to uninstall Apple's QuickTime media player from their PCs. "Computers running QuickTime for Windows will continue to work after support ends," US-CERT wrote in an advisory published Thursday. "However, using unsupported software may increase the risks from viruses and other security threats. Potential negative consequences include loss of confidentiality, integrity, or availability of data, as well as damage to system resources or business assets. The only mitigation available is to uninstall QuickTime for Windows." US-CERT (US Computer Emergency Readiness Team) based its alert on news Thursday from Trend Micro's TippingPoint group, which said it had been told by Apple that QuickTime on Windows had been deprecated, or dropped from support, meaning no future security updates will be issued and development has been halted. Apple hasn't significantly upgraded QuickTime for Windows since 2009, when it launched QuickTime X for OS X but didn't port the new player to Windows. The most recent security update for QuickTime on Windows was issued three months ago. Apple has not changed its support policies for QuickTime on OS X, which will continue to receive security updates. Few Windows users will miss QuickTime: Although the media player was once an integral part of its iTunes, Apple stopped bundling QuickTime with iTunes on Windows in 2011. (Computerworld 18Apr16)

(U) Researcher identifies XSS filter bypass in Microsoft Edge
(U) Gareth Heyes, one of the security researchers working for PortSwigger, the company behind the famous Burp Suite security testing toolkit, has found a bypass for Microsoft Edge's built-in XSS filter. What this means is that there's a way for attackers to run malicious JavaScript inside Edge while navigating various websites, despite some of the security measures that Microsoft has worked on to put in the browser. XSS filters are present in almost all browsers, and they were added in order to stop XSS (cross-site scripting) attacks at the browser level, before reaching the website and its users. "Basically you use the object literal as a fake array which calls the join function that constructs a string from the object literal and passes it to valueOf which in turn passes it to the location object," the researcher explained the flaw on PortSwigger's blog. IE issues strike again Apparently, this issue was actually a flaw that got ported from some Internet Explorer code that made it into Edge, even if Edge is a new product altogether. The issue was fixed in IE, but is not in Edge. Mr. Heyes says he found the flaw on 4 September 2015, when he also reported it to Microsoft. "They acknowledged the report but didn't give me a timescale," Mr. Heyes told Softpedia. "I guess the complexity of detecting computed properties made via regex was quite difficult and probably why the fix is delayed." The issue seems to be related to new properties introduced in ES6, the latest version of JavaScript released last year. This is not the first time that new ES6 features have aided attackers in carrying out XSS attacks. (Softpedia 18Apr16)

(U) Adware program takes screenshot of your desktop and uploads it
(U) Lawrence Abrams, a security researcher at Bleeping Computer, has stumbled upon a new type of adware that's not content with just blasting you with ads and collecting data on your system, as it also secretly takes a screenshot of your desktop and uploads it online. Called Faster Internet, the program comes bundled with other legitimate software, but it is only when it's installed that the real damage is done. The first thing it will do is to record details regarding each user's PC setup, a technique called fingerprinting, often used in advertising to distinguish between different users. Faster Internet collects data such as motherboard, CPU, hard drives, network adapters serials, and other more. Besides this highly personal information, the adware literally crosses the line and adopts a malware behavior when it takes a secret screenshot of your active desktop windows and then uploads it to an online server. "The problem is that when this program is installed, the user may have confidential documents, web sites, or programs open that will be now be included in the screenshot and uploaded to these scumbags," Mr. Abrams noted. Besides Faster Internet, Mr. Abrams recently also discovered another sneaky program, called VNLGP Miner, which transforms your computer into a Bitcoin mining bot for the gain of an unknown attacker. (Softpedia 18Apr16)

(U) New GozNym banking malware steals millions in just days
(U) A new banking trojan named GozNym is actively hitting US and Canadian banks and has already taken about $4 million from two dozen North American banks. IBM's X-Force Research team reported that 24 banks in the two countries, 22 in the U.S., have so far lost about $4 million to attacks using GozNym since the malware was discovered earlier this month. Who conducted the attacks is not known. Limor Kessem, executive security advisor for IBM, wrote in a blog that GozNym was created by combining some of the source code from the older Nymaim and Gozi IFSB banking malware to create an even more dangerous piece of software. "From the Nymaim malware, it leverages the dropper's stealth and persistence; the Gozi ISFB parts add the banking Trojan's capabilities to facilitate fraud via infected Internet browsers," said Kessem. "The end result is a new banking Trojan in the wild." GozNym uses its native Nymaim ability to infiltrate its targets through an exploit kit which drops a payload into the system that uses two executables for the infection routine, IBM said. One industry executive said it was disappointing that GozNym has been successful because, while this malware is new, the type of attack has been seen before and the banking industry was told to beware. (scmagazine.com 14Apr16)

(U) Linux computers targeted by new backdoor and DDoS trojan
(U) After being bombarded with new malware towards the end of last year, the Linux ecosystem is rocked again by the discovery of a new trojan family, identified by security researchers as Linux.BackDoor.Xudp. The only detail that matters is that this new threat does not leverage automated scripts, vulnerabilities, or brute-force attacks to infect users and still relies on good ol' user stupidity in order to survive. The infection scenario is simple, with users downloading malicious packages or applications from the Internet, and then giving them root privileges during the installation. Xudp is not distributed directly, but crooks lace these malicious packages with another malware called Linux.Downloader. This is what the infosec community calls a payload downloader, malware that's small enough to fit inside other apps, tasked only with downloading other malware. In this particular case, after the user gives root privileges to an app laced with Linux.Downloader (version 77), this trojan will download an upgraded version of itself (version 116), which includes more features needed during Xudp's installation. As for Xudp's main components, the trojan is split in three major threads. The first is responsible for handling C&C server communications via HTTPS, the second constantly listens to instructions coming from the C&C server, and the third periodically sends data from the infected machine to the attacker's server. Technically, Dr.Web security experts say that Xudp can be used as a backdoor to execute commands on the local machine, or as a bot in coordinated DDoS attacks. At the time of writing, the antivirus maker had detected at least three different versions of Linux.BackDoor.Xudp. (Softpedia 13Apr16)

(U) Facebook scam promises friend's video, delivers malware instead
(U) A new spam campaign tries to fool Facebook users into downloading malware by luring them to a fake YouTube page supposedly featuring a friend's video. According to a scam alert from research firm ESET, victims receive either a false notification that they were tagged in a friend's timeline post, or a message purportedly sent by a friend via Messenger. Typically titled "My first video," "My video," or "Private video," the fake message compels users to click on a link that sends them to the phony YouTube website. There, the user is instructed to install a plug-in to view the content -- but it's actually malware that fills the victim's wall with fake videos and sends the same "My first video" messages to that person's friends, further propagating the threat. To eliminate the threat, ESET advises victims to remove the plug-in, disguised as a "Make a GIF" app, from their browsers. Currently, the threat only impacts users of Google Chrome. (scmagazine.com 14Apr16)

(U) Cisco UCS servers can be hijacked with malicious HTTP request

(U) A data center server platform running Cisco's Unified Computing System (UCS) Central Software can be compromised by unauthenticated, remote attackers with a single, malicious HTTP request, security researcher Gregory Draperi has discovered. The Cisco UCS platform was designed to help organizations efficiently manage distributed Cisco UCS servers at scale. Cisco UCS Central Software helps manage multiple Cisco UCS domains. The vulnerability (CVE-2016-1352) is present in the product's web framework, and it's due to improper input validation. It affects Cisco UCS Central Software releases 1.3 (1b) and prior, and has been patched in versions 1.3 (1c) and later (which can be downloaded from here). No workarounds are available, so upgrading to the newest versions is the only way for admins to plug that hole. Cisco considers the flaw to be high risk, as a successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system. The good news is that there is no evidence that the flaw is being exploited in the wild. This is the third vulnerability in Cisco UCS Central Software reported by Draperi (and patched by Cisco) since July 2015. (helpnetsecurity.com 14Apr16)

Incidents of Interest:

[redacted]

OGA

(U) Security firm discovers secret plan to hack numerous websites and forums

(U) Security researchers from SurfWatch Labs have shut down a secret plan to hack and infect hundreds or possibly thousands of forums and websites hosted on the infrastructure of Invision Power Services, who are the makers of the IP.Board forum platform, now known as the IPS Community Suite. The plan belonged to a malware coder known as AlphaLeon, who, at the start of March this year, started selling a new trojan called Thanatos. Advertised as a MaaS (Malware-as-a-Service) rentable platform, to be attractive to its customers, Thanatos had to run on a very large number of infected hosts. In the infosec community, this structure is called a botnet, and the bigger it is, the easier it is to carry out all sorts of cyber-attacks. In order to increase the size of the Thanatos botnet, AlphaLeon needed to find a way to deliver the trojan to as many users as possible. His idea consisted of finding and exploiting a vulnerability in the infrastructure of Invision Power Services (IPS), who offers its IPS Community Suite as a hosted platform, running on AWS (Amazon Web Services) servers. After establishing a foothold on IPS' servers, AlphaLeon then intended to access the websites of IPS' customers and place an exploit kit on their pages. The exploit kit would automatically infect site visitors with the Thanatos trojan by leveraging vulnerabilities in the visitors (outdated) browsers and browser plugins. IPS customers include large companies such as Evernote, the NHL, the Warner Music Group, Bethesda Softworks, and LiveNation. Besides classic IP.Board forums, IPS also allows customers to set up fully working sites, even e-commerce stores. Researchers contacted IPS, who was unaware of the hacker's breach, discovered the entry point, and shut down his access. This incident happened at the start of April, and IPS is still in the process of investigating the breach. (Softpedia 20Apr16)

[redacted]

OGA

(U) Schools put on high alert for JBoss ransomware exploit

(U) More than 2,000 machines at schools and other organizations have been infected with a backdoor in unpatched versions of JBoss that could be used at any moment to install ransomware such as Samsam. That's according to Cisco's Talos threat-intelligence organization, which on Friday announced that roughly 3.2 million machines worldwide are at risk. Many of those already infected run Follett's Destiny library-management software, which is used by K-12 schools worldwide. "Follett identified the issue and immediately took actions to address and close the vulnerability," the company told Cisco. Follett provides patches for systems running version 9.0 to 13.5 of its software and says it will help remove any backdoors. Its technical support staff will reach out to customers found to have suspicious files on their systems. Governments and aviation companies are also among the organizations affected, Cisco said. (IDG News Service 15Apr16)

Items of Interest

(U) World's largest international cyber-defence exercise underway in Tallinn

(U) Some 26 nations and more than 550 leading computer security professionals are currently engaged in Locked Shields 2016, described as the biggest and most advanced international live-fire cyber-defence exercise in the world, which is hosted annually by the NATO Cooperative Cyber Defense Centre of Excellence (CCD COE). 20 Blue Teams representing 19 nations and NATO Computer Incident Response Capability (NCIRC) are tasked to maintain the networks and services of a fictional country, Berylia under intense pressure. This includes handling and reporting incidents, solving forensic challenges as well as responding to legal, media and scenario injects. While the organizers of the exercise will gather in Tallinn, Estonia, the participating Blue Teams will have online access to the exercise networks and typically work from their home countries. "Locked Shields is unique in forcing the hands-on network defenders from 19 nations and NATO to work together and exchange information. International cooperation is the key to successful cyber-defense and this exercise is a perfect example of doing just that," says Sven Sakkov, director the Tallinn-based NATO CCD COE. "The impact of the exercise, therefore, goes a lot further than technical skills. These computer emergency response teams -- be they civilian or military -- will better know whom to call when needing assistance in the future." "The organizers have built identical virtual networks for all the defensive teams in this scenario-based exercise. They play the role of the rapid reaction teams of the fictional country of Berylia, protecting a total of about 2,000 machines," explains exercise architect Jaan Priisalu, senior fellow at CCD CEO. Locked Shields uses realistic networks, technologies and attack methods on par with real-world developments, Priisalu adds. "We introduced smart phones and critical infrastructure components such as power grid to Locked Shields last year. A central part of the scenario focused on drones and regaining control of our own systems after they have been broken into," Priisalu says. "In 2016, the networks include a variety of operating platforms: Windows 8 and 10, Linux and Apple IOS. The services the Blue Teams have to maintain range from websites, email and online shopping to industrial control systems". (scmagazine.com 20Apr16)

(U) Marines take prominent role in DOD cyber operations

(U) Marine Corps' cyber operatives have been at the forefront of two of the US military's most prominent offensive and defensive cyber missions in the last year, reflecting the kind of maturity of capabilities the Pentagon is counting on to wield power in cyberspace. Pentagon leaders called on a Marine Corps cyber protection team, among other network defenders, to evict hackers that had breached the Joint Chiefs of Staff's unclassified email network last summer, according to Brig. Gen. Lori Reynolds, head of Marine Corps Forces Cyberspace Command, in a 19 April speech to AFCEA's Quantico-Potomac chapter. Media reports have blamed that intrusion, which downed the Joint Chiefs' email network for about two weeks, on Russian spear phishers. Reynolds also shed light on recent offensive operations against the Islamic State terrorist group. "There is a tremendous amount of signals intelligence that goes into developing a cyber target...and so the dependency on the National Security Agency right now is enormous," she said. Reynolds declined to talk further about the counter-ISIS cyber operation after her speech. For her part, Reynolds worried about network visibility. "Our current architecture makes seeing and understanding the battle space a significant challenge," she said. "In many cases I am operating on trust," when asking a domain owner to run a script to test compliance, for example. The Marine Corps Enterprise Network has about 60 domains, Reynolds said, quipping: "that's like 59 too many." Like the other service branches, the Marine Corps is adopting the Joint Regional Security Stacks, a set of servers, switches and software that is tantamount to a big firewall. The Corps has been trying to time the switch from its own firewall to JRSS without sacrificing security. (fcw.com 19Apr16)

(U) Cybersecurity new atom bomb, says Apple co-founder Steve Wozniak

(U) Cybersecurity is the greatest threat since the atom bomb, Apple co-founder Steve Wozniak said in an interview on the Australian TV news show Lateline. And, he said, the threat is "getting worse and worse year by year." In a wide-ranging interview, the man who in the early 1970s developed the first Apple computers with Steve Jobs, said, "Could they really take out our electrical system, turn off our internet?" He also lamented the loss of privacy, saying the US government's attempt to force Apple to decrypt the cell phone used by one of the San Bernardino killers was wrong. "What if the FBI was able to go to any company any time they felt like it and said you have to build a product our way?" he said on Lateline.Wozniak left his R&D role at Apple in the 1980s. He is now an adjunct professor at the University of Technology Sydney. (scmagazine.com 19Apr16)

(U) NSA cyber exercise hones skills at military academies

(U) An annual cybersecurity exercise run by the National Security Agency for the military academies has put students alongside NSA's red team network hunters for the first time. The goal is to expose the future Defense Department cyber workforce to intrusion techniques they'll be called upon to thwart. "To learn defense, you have to know offense," said James Titcomb, an NSA official who was the technical lead for this year's Cyber Defense Exercise. The multiday competition wrapped up on 14 April, with the Army's US Military Academy taking first place for the eighth time. There were a few noticeable changes in CDX this year: An "ethical hacking" challenge was part of the exercise, as was a session tasking graduate students with securing and exploiting drone communications. Additionally, Army Cyber Command had network defenders participating in the exercise for the first time. Teams are graded on their ability to keep networks running and protect confidential data, among other metrics. "It makes it real for them," said Kimberly Beam, NSA's chief of remote deployed operations. "It takes it a little bit out of the academic world in [that] they have a real environment that they're working in and defending." A fake news network pumped out updates during the simulation to mirror the real-life attention agencies receive when they are breached. The adversary was dubbed Synonymous after the infamous hacking collective Anonymous. The Naval Academy won last year because "they stuck to the fundamentals," 1st Lt. Christopher Shields said. "At every single step, they used least privilege," meaning system-administering privileges were minimized to prevent attackers from moving laterally within a network. Shields participated in CDX while at the Air Force Academy and now works at NSA's Information Assurance Directorate, which supplies the network-probing red team. The Naval Academy's Dennis Devey was back at the competition this year defending his title. He said the inter-service rivalries come to the fore during CDX with the scoreboard in plain sight. "Everyone has used a computer before, but there's a huge step up from being good at Excel to being able to do this sort of thing," he added, describing the technical acumen required of participants. Absent from the competition this year was the Air Force Academy, which has a team of cyber cadets that train weekly for this sort of competition. (fcw.com 18Apr16)

(U) Report finds US government worse than all major industries on cyber security

(U) US federal, state and local government agencies rank in last place in cyber security when compared against 17 major private industries, including transportation, retail and healthcare, according to a new report released Thursday. The analysis, from venture-backed security risk benchmarking startup SecurityScorecard, measured the relative security health of government and industries across 10 categories, including vulnerability to malware infections, exposure rates of passwords and susceptibility to social engineering, such as an employee using corporate account information on a public social network. Educations, telecommunications and pharmaceutical industries also ranked low, the report found. Information services, construction, food and technology were among the top performers. SecurityScorecard said it tracked 35 major data breaches across government from April 2015 to April 2016. Federal agencies scored most poorly on network security, software patching flaws and malware, according to SecurityScorecard, which said they may be more vulnerable to risk due to their large size. Of the 600 government entities tracked, NASA performed the worst, the report found. The space exploration agency was vulnerable to email spoofing and malware intrusions, among other weaknesses, according to SecurityScorecard's analysis. Other low-performing government organizations included the US Department of State and the information technology systems used by Connecticut, Pennsylvania, Washington and Maricopa County, Arizona. Government organizations with the strongest security postures included Clark County, Nevada, the US Bureau of Reclamation, and the Hennepin County Library in Minnesota. (Reuters 14Apr16)

(U) Homeland Security announces new cybersecurity risk analysis tool on the commercial market

(U) The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) announced that a fifth cybersecurity technology has been licensed for commercialization as a part of the Cyber Security Division's Transition to Practice (TTP) program. The TTP program builds on the S&T process of funding projects through the full research and development lifecycle through to the commercial marketplace. The Physical and Cyber Risk Analysis Tool (PACRAT) technology, developed by researchers at Pacific Northwest National Laboratory (PNNL), assesses cyber risks simultaneously with physical risks. RhinoCorps, a small business and vulnerability assessment tool developer in Albuquerque, New Mexico, is licensing the tool and plans to integrate PACRAT's capabilities into their physical vulnerability assessment tool called Simajin. The resulting assessment tool will enable users to examine how their cyber security and physical security postures impact one another. In 2013, the TTP program identified PACRAT as a promising candidate for transition to the commercial marketplace. By combing physical and cyber domains into one risk assessment tool, this technology can create simulations for both domains individually as well as the domain cross-over. Each fiscal year the TTP program selects up to nine promising cyber technologies to incorporate into its 36-month program. S&T introduces these technologies to end users around the country with the goal of transitioning them to investors, developers or manufacturers that can advance them and turn them into commercially viable products. (Government Security News 14Apr16)

(U) Obama names cyber experts from business and academia to new panel

(U) The chief executive of MasterCard Inc, the former head of the National Security Agency, and officials from Microsoft and Uber will join a commission to strengthen US cyber defenses, the White House said on Wednesday. After high-profile hacks in the private sector and an embarrassing theft of information from government personnel files, President Barack Obama this year set up a Commission on Enhancing National Cybersecurity. The commission, due to make long-term recommendations by early December on tightening cyber security in the private sector and government, is part of Obama's $19-billion proposal to boost defenses against hackers. The panel will hold its first public meeting on Thursday at the Commerce Department, joined by Obama's counterterrorism adviser Lisa Monaco and Commerce Secretary Penny Pritzker, the White House said in a blog post. As previously announced, the panel will be co-chaired by Tom Donilon, Obama's former national security adviser, and Sam Palmisano, former CEO of IBM. The panel, selected by Obama and congressional leaders from both parties, also includes: Retired General Keith Alexander, former director of the National Security Agency, now CEO of IronNet Cybersecurity; Ajay Banga, CEO of MasterCard; Peter Lee, Corporate Vice President of Microsoft Research; Joe Sullivan, Chief Security Officer of Uber, former Chief Security Officer of Facebook; Maggie Wilderotter, Executive Chairman of Frontier Communications; Steven Chabinsky, General Counsel and Chief Risk Officer of CrowdStrike; Annie Antón, chair of the School of Interactive Computing at Georgia Tech; Patrick Gallagher, Chancellor of the University of Pittsburgh, former Director of the National Institute of Standards and Technology; Herbert Lin, Senior Research Scholar for Cyber Policy and Security at the Stanford Center for International Security and fellow at the Hoover Institution; and Heather Murren, former member of the Financial Crisis Inquiry Commission and co-founder of the Nevada Cancer Institute. (Reuters 13Apr16)

[redacted]

(b)(3) 10 USC ⊥ 424

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

[redacted]

(b)(3) 10 USC ⊥ 424