Cyber-Threat Newsletter – 13 Sep 16

Patches & Updates of the Week:

(U) Adobe issued hotfix for critical information disclosure vulnerability in ColdFusion

(U) Adobe Systems today has released security hotfixes for a critical information disclosure vulnerability that exists in ColdFusion versions 10 and 11, across all platforms. The flaw -- officially designated CVE-2016-4264 -- occurs during the parsing of crafted XML entities, according to an Adobe security bulletin. Adobe has classified the threat as "Priority 2," meaning the product has historically been at an elevated risk of attack, although an exploit is not likely imminent. To resolve the issue, Adobe has advised its customers to install Update 10 for ColdFusion 11 and Update 21 for ColdFusion 10, as well as to follow all recommended security configuration settings. The ColdFusion 2016 release is not affected by the vulnerability, Adobe noted. (scmagazine.com, 30Aug16)

(U) Cisco starts patching firewall devices against NSA-linked exploit

(U) Cisco Systems has started releasing security patches for a critical flaw in Adaptive Security Appliance (ASA) firewalls targeted by an exploit linked to the US National Security Agency. The exploit, dubbed ExtraBacon, is one of the tools used by a group that the security industry calls the Equation, believed to be a cyberespionage team tied to the NSA. ExtraBacon was released earlier this month together with other exploits by one or more individuals who use the name Shadow Brokers. The files were provided as a sample of a larger Equation group toolset the Shadow Brokers outfit has put up for auction. ExtraBacon exploits a buffer overflow vulnerability in the Simple Network Management Protocol (SNMP) implementation from Cisco's ASA software. It allows attackers to remotely execute rogue code on the affected devices, as long as they can send traffic to their SNMP interface. This typically requires being on the same internal network as the targeted devices. Even though the ExtraBacon exploit was designed to work for versions 8.4 (4) and earlier of the ASA software, other researchers demonstrated that it can be modified to also work on newer versions. Cisco confirmed in an advisory that all versions of SNMP in Cisco ASA software contain the flaw. On Wednesday, the company updated its advisory to announce the availability of patched versions for different Cisco ASA branches, namely 9.1.7 (9), 9.5 (3), and 9.6.1 (11). Devices using ASA software versions from the 8.x and 7.x branches should be migrated to version 9.1.7 (9), according to the vendor. Also, patched releases for the 9.0, 9.2, 9.3, and 9.4 branches are expected Thursday and Friday. These will be 9.0.4 (40), 9.2.4 (14), 9.3.3 (10) and 9.4.3 (8). In addition to ASA software, which is used in different stand-alone devices and security modules for routers and switches, the Cisco Firepower Threat Defense (FTD) Software, the Cisco Firewall Services Module (FWSM), and Cisco PIX Firewalls are also affected by this vulnerability. Software version 6.0.1 (2) was released for Cisco FTD, but Cisco Firewall Service Modules and Cisco PIX Firewalls have reached their end of life, and no patches will be provided for them. Security researchers have so far established links between the code in the tools leaked by Shadow Brokers and those previously found in the wild and attributed to the Equation group. Furthermore, 14 files leaked by Shadow Brokers contain a 16-character string that NSA operatives are known to have used in their malware and which is listed in an NSA manual leaked by Edward Snowden, The Intercept reported. There is a second Equation exploit in the Shadow Brokers leak that targets ASA software. It is called EpicBanana and exploits a vulnerability that Cisco claims was patched back in 2011 in version 8.4 (3). Nevertheless, the company published a new advisory for the flaw in order to increase its visibility. A third exploit, BenignCertain, affects legacy Cisco PIX firewalls that are no longer supported. (IDG News Service, 26Aug16)

~~(U//FOUO)~~ Microsoft announces new patch release model beginning in October

~~(U//FOUO)~~ Beginning in October, Microsoft will change its existing "patch Tuesday" update model and issue only a monthly patch rollup for non-security updates in Windows 7 and up, according to a 15 August Microsoft blog post. Microsoft also announced that the Security-only update will be available to download and deploy only from the Windows Server Update Service (WSUS), System Center Configuration Manager (SCCM), and Microsoft Update Catalog, and not via the Windows Update feature. The new rollup model offers fewer updates to manage and should enhance Windows reliability by eliminating update fragmentation and providing more proactive patches for known issues, according to the blog post. Microsoft also announced it is revamping its Update Catalog website to allow users to download software patches from any browser by removing the ActiveX control, which currently limits users to Internet Explorer for these downloads. (blogs.technet.microsoft.com, 15Aug16)

Threats & Vulnerabilities of the Week:

(U) Forty percent of enterprise networks show evidence of DNS tunneling

(U) A new report released by network control company Infoblox reveals that 40 percent of the enterprise files it tested in the second quarter of this year show evidence of DNS tunneling. "In the physical world, burglars will go to the back door when you've reinforced and locked the front door. When you then secure the back door, they'll climb in through a window," says Rod Rasmussen, vice president of cybersecurity at Infoblox. "Cybersecurity is much the same. The widespread evidence of DNS tunneling uncovered by the Infoblox Security Assessment report for the second quarter of 2016 shows cybercriminals at all levels are fully aware of the opportunity. Organizations can't be fully secure unless they have tools in place to discover and prevent DNS tunneling". While there are semi-legitimate uses of DNS tunneling, many instances are malicious. There are also several off-the-shelf tunneling toolkits readily available on the internet, so hackers don't always need superior technical skills to mount DNS tunneling attacks. The most common threats uncovered by Infoblox during the quarter are: protocol anomalies (48 percent), DNS tunneling (40 percent), botnets (35 percent), amplification and reflection traffic (17 percent), DDoS) traffic (14 percent), and ransomware (13 percent). "While these threats are serious, DNS can also be a powerful security enforcement point within the network," adds Rasmussen. "When suspicious DNS activity is detected, network administrators and security teams can use this information to quickly identify and remediate infected devices -- and can use DNS firewalling as well to prevent malware inside the network from communicating with command-and-control servers". You can find out more about the findings in the full report on the Infoblox website. (BetaNews 31Aug16)

(U) Researcher claims ambient light sensors could leak data

(U) Independent security researcher Lukasz Olejnik claims Ambient Light Sensors in personal devices could be used to track users and even measure the size of their homes. The sensors allow devices to detect the brightness of their environment but the technology may introduce non obvious and unexpected data leaks such as information about the size of a user's house, what times the user is usually working, what light conditions they prefer, and how often they move between rooms, according to an 31 Aug blog post. Using this information advertisers, or attackers, could potentially profile users and make assumptions about a user's financial situation to serve targeted ads based on assumption such as large house equals wealthy user. The sensor could also be used for cross device aspects including linking and tracking, the post said. To better protect users, Olejnik said the readout of the sensors should be protected. (scmagazine.com 31Aug16)

(U) Redis servers targeted with fake ransomware

(U) A crook is hacking Internet-exposed Redis servers, adding a rogue SSH key on infected systems, deleting user data, and leaving a ransom note behind in an attempt to fool the server owner that his data was encrypted by ransomware. The attacker tells the Redis DB owner he should pay a 2 Bitcoin (~$1,100) ransom to recover his files, but in reality, all the data is gone, according to a honeypot server set up by Duo Security that has captured the crook's real actions. The problem at the core of this issue is the fact that server owners leave crucial and very sensitive Redis databases exposed online. Duo researchers say they've found over 18,000 Redis databases available online that featured no password authentication. Researchers say that they've identified evidence of attacks on 13,000 of these servers (around 72 percent). The evidence they're mentioning is an SSH key which the attacker has left behind after breaking into the vulnerable server. At the start of July, in a similar report, Risk Based Security discovered the same SSH key and the Jabber ID on 6,338 servers, albeit without any clues of the attacker deleting files and asking for ransom. Based on a user comment on Softpedia's 2 August story, fake ransomware seems to have been a recent addition to the crook's mode of operation. According to Duo, after compromising each Redis server, the crook deletes data from the /var/www/, /usr/share/nginx/, /var/lib/mysql/, and /data/ folders. Based on honeypot data, there is no attempt to encrypt any of the data, or back it up on another server. After these operations, the crook rewrites the server's MOTD and adds a file to the server's root folder called READ_TO_DECRYPT. According to Bitcoin blockchain statistics, the crook has received three payments to the Bitcoin address listed inside the ransom note. The crook made 2.5995 Bitcoin (~$1,450). Knowing what the hacker is actually up to, users should not pay the ransom in any way if they discover the "cracka" SSH key on their servers. Users can still recover files from off-site data stores if they regularly create backups for their servers. (Softpedia 31Aug16)

(U) Aviation expert warns, hackers can hijack aircraft using WiFi network

(U) The potential threat of an airplane being hijacked by hackers using WiFi network on-board puts more responsibility on airlines and passengers to ensure safe and secure flights, a senior airline official said on Monday. "Many planes offer on-board WiFi for their passengers and this poses a risk of hacking the plane itself. In the US, for example, two men did a test from their laboratory on the ground and proved that they could hack on to a passenger's device through the internet connection," Dr. Jasem Haji Al Jasem, director of IT at Gulf Air, a Bahrain-based airline, said at the National Security Middle East conference in the capital on Monday. A BBC report last year said the US Federal Bureau of Investigation (FBI) had issued a formal alert telling airlines to be on the lookout for hackers. It followed an on-board tweet from security expert Chris Roberts, who joked about being able to hack into a United Airlines plane's WiFi network. A terrorist could theoretically take over systems by compromising on-board equipment. Aircraft, including Boeing 787 Dreamliner and Airbus 350 and A380, have a single network used by both the pilots to fly the plane and by passengers for their WiFi connections, the BBC report said. (Gulf News 30Aug16)

(U) Flaw in Facebook password resets could allow random account takeovers; severity of bug disputed

(U) An independent researcher found a way to theoretically take over random Facebook accounts by forcing millions of user password resets and then brute-forcing each reset request to check for a specific six-digit authorization code. The researcher, Gurkirat Singh -- by day, a software graphics engineer at Intel -- personally characterized the vulnerability as "critical" because a successful exploit can lead to the total compromise of an affected account. Facebook, however, has classified the bug as low-priority because such an attack would be random, not targeted, and because there are multiple security checks in place that would likely detect and stop it. As Singh explains in a Hacker Noon post, there are exactly one million possible six-digit authorization codes that Facebook can send to a user when he or she requests a password reset. These passcodes do not expire right away; ergo, if more than one million users request password resets within a short period of time, it becomes increasingly likely to exhaust all of the possible active passcodes that Facebook stores in its servers at any given time. This then increases the odds that a hacker could select any random passcode and match it to at least one of these reset accounts. Of course, the odds of over a million people all requesting passwords in a short duration of time is highly improbable -- unless a hacker does something to change those odds. And that's where Singh's research comes in. "I was at a tech conference early this year and as I was talking to one of the Facebook software engineers there. He mention[ed] to me how Facebook's security is really tight and they are proud of that. So I told him that I [would] try to prove him wrong," said Singh in an email interview with SCMagazine.com. "Knowing that finding bugs in companies like Facebook and Google has become a holy grail for security researchers, I took it as a challenge to find a bug in Facebook's website". In order to accrue enough fake accounts to generate copious amounts of password resets, Singh fabricated 100 trillion possible Facebook user ID numbers (which are 15 characters in length) and then used the Facebook Graphic API to validate which of these ID numbers belonged to real accounts. Singh looked up and extracted the user names associated with these accounts from their respective URLs and then used these profiles to simulate sending out 2 million password change requests. Normally, sending out so much traffic at once might result in Facebook blocking the attacker's IP address. To counter this scenario, Singh used a rotating IP service that simulated a normal flow of traffic. He then used a headless browser to write a Java-based script that would submit passcode requests from the collected user accounts, and hosted these scripts on a Google Computer Engine virtual machine, executing at a rate of 923 HTTP requests per second. Upon completing the 2 million reset requests, Singh brute-forced all of the user password requests with the passcode 338625 and -- voila -- found one that was assigned that very code. By entering that code onto the password reset page, an attacker could then have taken over that individual's account. Singh chose the code 338625, theorizing that codes 300,000 through 699,999 had a statistically higher probability of occurring due to a mathematical concept known as the pigeonhole principle. (scmagazine.com 30Aug16)

(U) Trojan uses recently disclosed UAC bypass to install fake Chrome browser

(U) A new trojan identified as Trojan.Mutabaha.1 uses a recently disclosed UAC bypass technique to install a heavily modified Outfire browser that replaces the user's native Google Chrome browser. Outfire, which is a Chromium-based browser, looks very much like Chrome, with minimal changes to its setup. As such, the browser makes a fine choice for tricking the user into thinking they're using Chrome, when they're not. The Mutabaha trojan is one of the latest additions to the malware market. At this moment, researchers don't know how crooks are distributing the trojan to victims, but they found out how it infects their computers. Russian security vendor Dr.Web says the trojan uses a UAC bypass technique to execute a series of files and commands on infected PCs without triggering the Windows UAC (User Account Control) alert. The technique was only recently disclosed by two security researchers on 15 August, two weeks ago. Dr.Web says that Mutabaha appeared just three days after researchers published their UAC bypass method. When users run the trojan, it uses a system registry key to launch a program with elevated privileges that downloads and installs a malware dropper and a BAT file. This malware dropper downloads the Outfire browser and installs it automatically. After the installation ends, the BAT (Windows Batch) file deletes the malware dropper. During installation, Outfire adds itself to the Windows Registry to gain boot persistence, removes Google Chrome shortcuts from the system, and imports Chrome settings into its own. At the end of the installation, Outfire uses a list of 56 names for known browsers and kills all their Windows processes. The modified Outfire version features a non-changeable homepage, a fixed extension that inserts ads on all visited web pages, and a custom search engine instead of Google. (Softpedia 30Aug16)

(U) New FairWare ransomware targets Linux servers

(U) At least three Linux server administrators have complained at the time of writing about a new ransomware variant called FairWare that targets web servers running Linux. Users, who posted their quandary on a ransomware support thread on the Bleeping Computer forum and the Chinese V2EX Q&A site, said that somebody hacked their servers, removed their website root folders, and left a ransom note behind in the /root folder. The ransom note (READ_ME.txt) contained only the following text: "Hi, please view here: http://pastebin.com/raw/jtSjmJzS for information on how to obtain your files!" The PasteBin link includes a longer ransom note, with more details, asking the user to make a 2 Bitcoin (~$1,150) payment to a Bitcoin wallet, and also providing an email address to get in contact with the crook. Malware analyst and Bleeping Computer founder Lawrence Abrams says there is no evidence that FairWare encrypts the user's files. The crook may be just uploading the files to a server under his control and holding them for ransom. He also warns that FairWare's author may also be deleting files for good and that users might get scammed after paying the ransom. In the crook's expanded ransom note, which is embedded in full below, the FairWare author says he will not answer any questions from victims or requests to prove he stole their files. In spite of the crook's claim of not answering emails, users should attempt to get proof that their files still exist before paying the ransom. At the time of writing, there are no payments in the Bitcoin wallet address listed in the ransom note. (Softpedia 29Aug16)

(U) Google Chrome users targeted by tech support scammers

(U) Google Chrome users, beware: tech support scammers are misusing helpful browser features to impersonate Microsoft and to bombard users with pop-ups. In the first instance, the scammers are taking advantage of the browser's full-screen mode. Users who are tricked into visiting a malicious site set up for the scheme can, at first glance, believe that they have landed on a legitimate tech support page by Microsoft: the address bar shows the right URL and the green lock that usually indicates that the site is what it says it is. "This is an interesting one because for years we have been telling people to double check the URL in the address bar to know if a website is really what it claims to be. When this scam page loads it runs in full-screen mode and prevents the user from easily closing it with an infinite loop of alerts," noted Malwarebytes' Jérôme Segura. In the second instance, the scammers make the page show fake alerts saying the users' computer has been blocked because it's infected with spyware, but allow the users to press an OK button to dismiss the alert. This alert has the "Prevent this page from displaying additional dialogues" (sic) option at the end of it checked, but it's a lie. Pressing the OK button will do the complete opposite: it will allow the page to show more similar fake Google Chrome alerts, with more tricks to exasperate the user (such as saying that pressing the ESC key will allow them to close the page, when only the Prevent message and the OK button will do that: Pressing the ESC key will trigger a new onslaught of fake pop-ups, making users more likely to decide to call the fake tech support number provided by the scammers. (helpnetsecurity.com 29Aug16)

(U) Kelihos botnet triples in size in just 24 hours

(U) The Kelihos botnet, sometimes also referred to as Waledac, has been adding new bots all summer and started shifting operations from spamming "pump-and-dump" campaigns to delivering ransomware and banking trojans, security researcher MalwareTech has discovered. Kelihos is one of those old botnets created many years ago, which somehow has managed to avoid quite a few takedown attempts and has come back to life, just like Ramnit. Discovered in 2008, Kelihos has been one of the main sources of pharma and pump-and-dump spam, even as recently as 2016. According to MalwareTech, who owns and operates the Botnet Tracker project, Kelihos operators have shifted their focus to the most lucrative cyber-crime operations around these days: ransomware and banking trojans. Leveraging telemetry data obtained from his botnet tracker, the researcher reports that, at the end of June, Kelihos started spreading the WildFire ransomware. While for many weeks the botnet's size was steady at a lowly 8,000 infected machines, MalwareTech says the botnet received a big boost between 9 and 11 July, when its size almost doubled to 13,000. About the same time, the botnet dropped WildFire, which it had been spamming for some weeks and also started delivering other malware families, including an unspecified Zeus-based banking trojan. This past Monday, on 22 August, the botnet's size grew almost three times from 12,500-13,000 machines to a whopping 36,000 bots, all in a matter of hours. The source of the new bots is currently unknown, and it can be anything from infected web servers to regular desktops. What MalwareTech was able to discover was that this was not a targeted campaign. All the new Kelihos bots were randomly spread across the globe, with the most in low-income, high-population countries such as Turkey, Mexico, India, Iran, Brazil, and Peru. "It's likely that spamming the Wildfire ransomware was the Kelihos operator testing the water and now will likely joined [sic] the rest of the major spam botnets in the continued spamming of ransomware and banking trojans laced emails," MalwareTech noted. "I'd not be surprised if we continue to see further increases in infections as the operator expands the botnet to accommodate higher volumes of spam. (Softpedia 28Aug16)

(U) Dreambot banking trojan adds Tor functionality

(U) Proofpoint researchers spotted new variants of the Gonzi, also known as the Ursnif, banking trojan dubbed "Dreambot," some of which now include Tor communication capabilities and or peer-to-peer (P2P) functionality. Dreambot is still in active development and is spread via numerous exploit kits and via email attachments and malicious links, according to a 25 August blog post. Researchers believe the Tor-enabled versions have been active since at least July 2016 and despite having this function, few variants use it as the primary mode of communication with their command and control (C&C) infrastructure, the post said. It was noted that this feature may be utilized more frequently in the future and if so, would create additional problems for defenders. This is because the nature of Onion sites make it more difficult to take down the command and control of the Tor-enabled variants, Proofpoint Director of Emerging Threats Sherrod DeGrippo said. "In addition, because the communications are encrypted via the Tor protocol, it can be more challenging for researchers to observe the traffic and behavior on the network," DeGrippo told SCMagazine.com via emailed comments. Researchers also noticed a version of the malware which appears to use a peer-to-peer protocol to communicate. "This protocol operates over TCP and UDP and uses a custom packet format," the post said. "Due to the addition of this functionality, the client code surface is almost twice as big as that of the Tor version." Researchers are still investigating this functionality and did not provide additional details. DeGrippo said the recent updates make the malware more difficult to detect once a user is infected. "Protection comes from making sure machines on a network have all software updates, ensuring mail is scanned for malicious attachments and URLs and observing network traffic with intrusion detection to determine which machines are generating traffic of this type," she said. (scmagazine.com 26Aug16)

(U) Cyber criminals using insiders to carry out telecommunications attacks

(U) Cyber criminals are frequently turning to insiders to gain access to telecommunications networks and subscriber data, according to a new report from Kaspersky Lab. According to the report, 28 percent of all cyber-attacks and 38 percent of targeted attacks now involve malicious activity by insiders. Telco providers are some of the top targets for cyber-attacks due to the vast amount of confidential data they collect, so criminals are recruiting employees through underground channels or blackmailing staff with compromising information to carry out their attacks. The blackmailing approach in particular has grown in popularity as a result of breaches that have leaked sensitive or embarrassing data (E.g. the Ashley Madison leak) and insiders are often specifically targeted in order to gain access to the most confidential data or cause the most damage. "The human factor is often the weakest link in corporate IT security. Technology alone is rarely enough to completely protect the organization in a world where attackers don't hesitate to exploit insider vulnerabilities," said Denis Gorchakov, security expert, Kaspersky Lab. In order to help protect themselves, Kaspersky Lab advises organizations to educate staff about cyber security best practices, restrict access to sensitive data and systems and carry out regular security audits. (BetaNews 26Aug16)

Incidents of Interest:

(U) Opera warns sync users to change passwords for every website after hack

(U) Opera warned Friday that users who stored passwords and other data via its cloud services may have had that data compromised during a server breach. Opera said that it detected unauthorized access to the Opera sync system last week via an attack. Though the attack was "quickly blocked," Opera said that it believed that "some of our sync users' passwords and account information, such as login names, may have been compromised." As a precaution, Opera reset all of the account passwords for the sync system, and have asked users to reset their passwords for third-party sites as well. The company said that it sent emails to all Opera sync users to report the incident. "We take your data security very seriously, and want to sincerely apologize for the inconvenience this might have caused," the company said. If you're an Opera user, and you're worried about what might have been stored on Opera's servers, you'll need to first reset your password, and then log in. Next, you'll want to visit Opera's sync page. There, Opera will show you what -- if any -- data was stored there. (PC World 29Aug16)

(U) Cozy Bear suspected of hacking Russia-focused think tanks in DC

(U) The same Russian-backed cybergang which launched cyber attacks against the Pentagon, State Department and DNC is also believed to have targeted Russia-focused think tanks based in Washington DC Last week, attackers from Cozy Bear, or APT29, attacked fewer than five organizations and 10 staffers, all of which were researching Russia, in the highly targeted operation, Crowdstrike Co-founder and Chief Technology Officer (CTO) Dmitri Alperovitch told Defense One. Alperovitch declined to disclose which think tanks and researchers were hit, but did say that all of the organizations were promptly alerted to the attacks and the intruders were unable to exfiltrate any information. The attackers may have been trying to steal information from officials who serve on the boards of the think tanks as many of them are former government officials who still advise current government officials, he said. (scmagazine.com 29Aug16)

(U) FBI: hackers target 2 state election databases

(U) The FBI warned election officials to enhance the security of systems after it found evidence foreign hackers penetrated databases in two state systems, Yahoo reports. An 18 August bulletin from the FBI's Cyber Division stated hackers were able to exploit a Structured Query Language injection vulnerability to exfiltrate data from one state's Board of Election website in July and attempted intrusions on another's in August. The FBI alert lists eight IP addresses for the perpetrators and one used in both incidents, indicating the attacks could be linked. The methods, tools and a previously flagged IP address resemble other suspect Russian state-sponsored attacks, an expert told Yahoo News. Election security has been a hot-button issue a series of suspected Russian-sponsored attacks compromised the Democratic Party and media organizations allegedly to sway voter opinion. Earlier this month, Homeland Security Secretary Jeh Johnson suggested the federal government label elections systems as critical infrastructure. The FBI issued the bulletin three days after Johnson had a call with representatives from National Association of Secretaries of State and US Election Assistance Commission to offer DHS assistance addressing cybersecurity risks within each state's election systems. At the time of the call, per Johnson, DHS was not aware of any credible cyberthreats related to 2016 general election systems. Some swing states declined DHS' assistance, including Georgia and Pennsylvania, stating they will rely on in-house security crews. The FBI bulletin asks states and election boards to review activity logs for similar tools and techniques, and report them to local FBI field offices. (NextGov 29Aug16)

Items of Interest

(U) Rental car or loaner flash drive?

(U) FTC warns rental cars store user data. The Federal Trade Commission is warning consumers to be careful when using the infotainment systems of rental cars. It is possible that the car may be storing user data such as locations entered in the GPS or visited while using the car, FTC Attorney Lisa Weintraub Schifferle said in an 30 August blog post. If the user connects a personal device, even just for charging, it is possible that the device could automatically share contact information, mobile numbers, message logs, and even text messages, Schifferle said in the post. Users are recommended to use a cigarette lighter adapter to charge devices instead of USB ports in the vehicle. A user who must connect a device should check their permission settings to ensure unnecessary data isn't shared and to delete all of their data from the system prior to returning the car. (scmagazine.com 31Aug16)

OGA

(U) DARPA sees IoT and AI as weapons to dominate wars

(U) DARPA wants to exploit the power of the internet of things to help the US dominate battlefields. The Defense Advanced Research Projects Agency will fund the development of sensors and artificial intelligence systems that could help break into, extract and analyze information from enemy devices and communication systems. The components and systems will arm the US with more data to analyze enemy moves and strategy. Information is king in wars. "They are talking about going into any situation and extracting information at any time, [with] artificial intelligence systems that can attack and hack any network," said Jim McGregor, principal analyst at Tirias Research. DARPA wants to fund the development of sensors and electromagnetic systems that could break into point-to-point wired and wireless communications, even ones that are not linked to the internet. The agency had no comment on its research request. DARPA has been researching sensors for a while, most notably working on the successor to GPS. DARPA is funding the development of new location-tracking technology and components that include sensors, high-precision clocks, self-calibrating gyroscopes and accelerometers that can track position accurately over long periods. There are ways to extract information from data feeds and devices. In this case, DARPA is looking at various ways to tap into wired or wireless networks or devices to monitor communications or steal security keys. Beyond breaking in, the components need to be able to process the data gathered and dispatch only relevant chunks of intelligence information. An unmanned aerial vehicle would be a perfect platform, McGregor said. A small drone with the new sensors can fly into any situation, understand the communication and then tap into data feeds using various techniques. Technologies like this could also help fill security holes in communications networks. For example, researchers at the University of California, San Diego on Tuesday announced new circuitry to establish a reliable RF communications network that can't be easily jammed. The research was partly funded by DARPA. For data-gathering instruments, DARPA is also asking researchers to develop "tactical" sensors that are able to parse and extract relevant data from nearby or remote locations. The sensors will need to "exhibit 'selective attention' where they only collect and transmit relevant signals to conserve power," DARPA said in a document inviting proposals from researchers. (IDG News Service 30Aug16)

(U) Report says cyber enhances military power and vulnerabilities

(U) As the Defense Department continues to increase its digital capabilities, adding greater precision and lethality, it is also increasing its vulnerabilities, according to a new report. In "Digitally-Enabled Warfare: The Capability-Vulnerability Paradox," the Center for a New American Security likens DOD to a car that relies so heavily on computer and electronic technology that a system failure or hack could render the vehicle inoperable. "Digital technologies are integrated into every domain, across weapon systems, and across all levels of warfare," the report states. "Because of their ubiquitous nature and infrastructural characteristics, the capabilities and the vulnerabilities they imbue are exponential as opposed to strictly additive." As a result, CNAS said the US needs to strike a balance between developing the military might to achieve its objectives and remaining "able to mitigate network vulnerabilities from an adversary's first-move attack." "The cyber capability/vulnerability paradox is also different than other types of weapons development because the cause of this paradox is not a particular platform or weapon capability, but the way in which cyber creates an infrastructure of capabilities and vulnerabilities that connects to a family of weapons and platforms," the report states. Two systems that add unmatched capabilities but are effectively useless if hacked or if their electronic systems are compromised are the Distributed Common Ground System, which gathers intelligence from a variety of sources, and the F-35 Joint Strike Fighter, which has been beset by technical and software problems. "It is the systematic acquisition and development of similar digitally dependent technologies that moves the United States toward digital dependency and makes the US military highly capable and highly vulnerable," the report states. And the problem goes beyond vulnerability to electronic failures or cyberattacks. The report argues that as a nation like the US increases its digital capabilities, it motivates weaker states to consider a first strike "because the less capable state knows it cannot survive unless it is able to cripple the digitally enabled state's advantage." In theory, the US military's digital dominance will serve as a deterrent. "However, if the United States continues to build weapons and campaigns that move toward digital dependency, then it may find itself in a tenuous situation where it must either strike first or be prepared to function without much of its digital capability," the report states. It recommends that DOD incorporate manual backstops to increase its resiliency. (fcw.com 30Aug16)

(U) Want a Job With FBI's Elite Cyber Team?

(U) You Need These 3 Things. If you want a job one of the FBI's elite Cyber Action Teams -- a growing collection of talent who respond to the nation's most serious hacks -- you're going to need three things. "You need integrity, which is non-negotiable. You need physicality; we're going to give you a gun on behalf of the United States of America and you need to be able to run, fight and shoot. And to be a cyber special agent, you need a highly sophisticated, specialized technical expertise," said FBI Director James Comey, speaking Tuesday at the Symantec Government Symposium in Washington. Comey admitted that finding all three traits in a single person is rare, but he said the FBI is changing its culture to make it a more suitable destination for those unicorns. During the past 18 months, Comey said the FBI has been hiring up talent to staff its cyber action teams, which compete across the agency for cases to handle. These agents "are ready to deploy at a moment's notice to support an investigation," as was the case when California-based Sony was hacked. "Just as in terrorism, we have pre-assigned pools of expertise who can jump on a plane and go anywhere in the world in response to a terrorist threat, we've built that same capability with respect to cyber," Comey said. While Comey advocated for increased industry collaboration with regards to cyberthreats or breaches, he made no bones about competing with industry for cyber talent. "We're focusing on trying to steal the people you're trying to hire," Comey said. While the FBI can't match what industry pays cyber talent, he said the FBI is selling its mission of protecting Americans and upholding the constitution to potential talent. That selling point worked successfully over the past year and a half. The bureau also is working to add a few creature comforts found at startups and popular among millennials. The FBI, he said, wants to be cool. "We're working very hard inside the FBI to be a whole lot cooler than you think we are," Comey said. "We're not all bean bags and granola and a lot of whiteboards yet, but we're working hard and marching in that direction". (NextGov 30Aug16)

(U) US Army to treat Windows 10 upgrade as military operation

(U) The United States Department of Defense (US DoD) announced in February this year that it was moving 4 million devices to Windows 10 as part of a plan to increase the security of its systems, including here laptops, desktops, and smartphones. The US Army is one of the agencies that will migrate to Windows 10, and according to Chief Warrant Officer 5 Brian S. Wimmer, Senior Technical Adviser with NETCOM (the body in charge of the Army Cyberspace), the whole process is treated as a genuine military operation. Wimmer has told Army Times in a statement that the migration to Windows 10 is projected to complete as "rapidly as feasible," but a specific deadline hasn't been offered. All systems are expected to switch to Windows 10 by the end of 2017, though. Soldiers in Europe will be the first to move to Windows 10 this fall, and when their transition is complete, the upgrade will begin for those in the United States and Southwest Asia, according to the aforementioned source citing Army officials. Groups in the Pacific and Korea region will start the migration to Windows 10 in 2017. (Softpedia 30Aug16)

(U) Feds are using big data analytics for cybersecurity, but is it effective?

(U) 81 percent of Feds say their agency is using big data analytics for cybersecurity in some capacity -- 53 percent are using it as a part of their overall cybersecurity strategy and 28 percent are using it in a limited capacity. However, breaches continue to afflict agencies with 59 percent of Feds reporting their agency deals with a cybersecurity compromise at least once a month due to their inability to fully analyze data, according to MeriTalk and Cloudera. It's clear that Feds are struggling to stay afloat. Eighty-eight percent of Federal agencies face challenges drawing cybersecurity intelligence from data and the majority says the task has become more difficult in the past two years. Fewer than half of those using big data analytics for cybersecurity (45 percent) say they trust their efforts to be highly effective. Feds stated the following as top challenges: Sheer volume of cybersecurity data is overwhelming (49 percent) Agencies don't have the right systems in place to gather the cybersecurity information they need (33 percent) Information is no longer timely when it makes it to cybersecurity managers (30 percent). As a result, more than 40 percent of their data goes unanalyzed. In addition to obvious budget issues, Feds' efforts are hindered by: lack of skilled personnel (40 percent), potential privacy concerns (27 percent), and lack of management support/awareness (26 percent). "Internal and external cybersecurity threats will continue to evolve daily and we need to unlock the power of the data in order to regain the advantage," said Rocky DeStefano, Security SME at Cloudera. "Agencies need complete visibility into the data across their enterprise. These teams also need the ability to flexibly analyze that data in a meaningful timeframe so they can detect advanced threats quickly, identify the impact and reduce the associated risk. Accelerating investment in the platforms necessary to collect and analyze this data is critical to the success of these programs". Federal agencies that effectively use big data analytics see improvements in cybersecurity. In fact, 84 percent of big data users say their agency has successfully used big data analytics to thwart a cybersecurity attack and 90 percent have seen a decline in security breaches -- malware (50 percent), insider threats (47 percent), and social engineering (46 percent) -- as a result of using big data analytics. Agencies see the value big data provides -- 94 percent of Feds have plans to invest in big data analytics in the next two years with top planned investments in technology infrastructure (61 percent), hardware (52 percent), and business intelligence tools/analytics (52 percent). (helpnetsecurity.com 30Aug16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424