Cyber-Threat Newsletter – 04 Apr 16

Patches & Updates of the Week:

(U) Oracle issues emergency Java security update

(U) Oracle has issued an urgent security fix for its cross-OS Java runtime that aims to repair a security flaw that's been lying around for 2.5 years. Identified as CVE-2016-0636, this bug is actually the second fix for CVE-2013-5838, which Oracle supposedly patched in October 2013. At the start of the month, Polish security firm Security Explorations decided to publicly disclose that Oracle failed to properly assess and patch CVE-2013-5838, which they first discovered in early 2013. Oracle had to scramble for a fix as details were made public with no warning. The company candidly admitted that they haven't notified Oracle at all prior to their reveal, explaining that it was Oracle's job to implement and test the patch, and not their responsibility. Two weeks later following this regrettable incident, Oracle is now issuing a new patch for the original problem, via new versions: Java SE 7 Update 99, and 8 Update 77. The company said, this issue, which has a severity score of 9.3/10, is exploitable from remote locations, just by tricking a user into accessing a malicious website. The bug works on Java SE running in Web browsers on desktops, on Windows, Solaris, Linux, and Mac OS. Oracle has made it clear that Java's default security levels and click-to-play policies prevent automatic exploitation of this bug without user interaction. By the use of clever social engineering tricks, attackers could still get around these limitations. All users are urged to update their Java installation as soon as possible. (Softpedia, 24Mar16)

Threats & Vulnerabilities of the Week:

(U) Remaiten Linux bot combines malware features to target weak credentials

(U) ESET researchers have spotted a new variant of malware, dubbed Remaiten, which combines different features from other families of malware and uses a unique method of distribution. The Linux bot performs telnet scans, which are user command and an underlying TCP/IP protocol for accessing remote computers, to search for embedded systems including routers, gateways, wireless access points, and potentially internet of thing devices (IoT) that use default or weak credentials, ESET Malware Researcher Marc-Étienne Léveillé told SCMagazine.com. Once a vulnerable device is found, Remaiten will send a small executable file, dubbed the Remaiten downloader, to the remote device via telnet to fetch the full Remaiten IRC bot malware from the remote command and control server, Léveillé said. He said there are multiple downloaders inside the bot to accommodate the different architectures of embedded devices and the correct bot will push automatically. Léveillé said it is unclear why the malware uses this method, but said it is likely to maximize infection success. The Remaiten is a variant of the Kaiten bot, also known as Tsunami, and combines features of the Gafgyt bot, according to a 30 March ESET blog post. Once a user's device is infected the bot can be used to launch denial-of-service denial of service attacks or download other variants of malware. Léveillé said users can protect themselves from the these kind of attacks by using strong credentials and vendors can help prevent these type of infections by not using default credentials in their products and requiring users to have strong credentials. (scmagazine.com, 30Mar16)

(U) 1,400+ vulnerabilities found in automated medical supply system

(U) Security researchers have discovered 1,418 vulnerabilities in CareFusion's Pyxis SupplyStation system -- automated cabinets used to dispense medical supplies -- that are still being used in the healthcare and public health sectors in the US and around the world. The vulnerabilities can be exploited remotely by attackers with low skills, and exploits that target these vulnerabilities are publicly available, ICS-CERT has warned in an advisory. The worst part of it is that the affected versions of the software are at end?of-life, and won't be receiving a patch even though they are widely used. Developed by CareFusion, which was recently acquired by Becton, Dickinson and Company (BD), the Pyxis SupplyStation system dispenses medical supplies and documents usage in real-time. "The Pyxis SupplyStation systems include automated devices that may be deployed using a variety of functional configurations. [They] have an architecture that typically includes a network of units, or workstations, located in various patient care areas throughout a facility and managed by the Pyxis SupplyCenter server, which links to the facility's existing information systems," ICS-CERT explained. "Exploitation of these vulnerabilities may allow a remote attacker to compromise the Pyxis SupplyStation system. The SupplyStation system is designed to maintain critical functionality and provide access to supplies in 'fail-safe mode' in the event that the cabinet is rendered inoperable. Manual keys can be used to access the cabinet if it is rendered inoperable." Versions 8.0, 8.1.3, 9.0, 9.1, 9.2 and 9.3 that operate on Windows Server 2003/XP of the Pyxis SupplyStation system software are affected. Versions 9.3, 9.4, and 10.0 that operate on Server 2008/Server 2012/Windows 7 do not sport these vulnerabilities. Independent researchers Billy Rios and Mike Ahmadi obtained a Pyxis SupplyStation through a third-party that resells decommissioned systems from healthcare systems, and used an automated software analysis tool to ferret out the vulnerabilities. The flaws are present in seven different third-party vendor software packages bundled in the vulnerable system, including MS Windows XP, Symantec Antivirus 9, and Symantec pcAnywhere 10.5. 715 of the found vulnerabilities are critical or high-severity. CareFusion has been involved in the research, and has confirmed the existence of these flaws. Still, no updates will be offered for these end-of-life systems. Instead, the company has started contacting customers that bought the automated supply cabinets, advising them to upgrade to newer versions and explaining how to do it. But, aware that's not always possible, the company has also issued recommendations on how to minimize the risk of those systems being compromised -- things like monitoring network traffic attempting to reach the affected products for suspicious activity, and isolating them from the business network, untrusted systems and the Internet, but also updating the software packages included in the system software (where possible). More recommendations can be had from the ICS-CERT advisory. (helpnetsecurity.com, 30Mar16)

(U) Petya ransomware leverages Dropbox and overwrites hard drives

(U) Trend Micro researchers spotted a new ransomware variant dubbed Petya that is delivered to victims who believe they are linking to a resume stored on a cloud storage site like Dropbox. Using a cloud storage site as the infection source is not new, but using the cloud storage site to promote ransomware infections appears to be a new technique, Trend Micro Senior Global Marketing Manager Jon Clay said in comments emailed to SCMagazine.com. The ransomware overwrites the affected system's hard drive master boot record (MBR) in order to lock out users, according to a 25 March blog post. The process of overwriting the MBR of the system and putting the ransom note in the startup process of the machine makes this variant of ransomware unique. "It makes the system unusable and will display their ransom note during bootup," Clay said, adding researchers are also seeing new and improved graphics with the ransom notes in their attack, possibly to improve the look and feel of the popups. The scam starts with the attackers using phishing emails disguised to look and read like an applicant seeking a job, researchers said in the blog. The email provides a link to, in the case studied by Trend Micro, a Dropbox storage location. The email is supposed to link to the applicant's resume, but instead the link is connected to a self-extracting executable file that unleashes a trojan into the system. Researchers said the trojan blinds any antivirus programs defending the computer before downloading and executing the ransomware. Trend Micro said the cybercriminals asked for 0.99 Bitcoins to unlock the computer. Once executed, Petya overwrites the entire hard drive MBR to prevent the victim's device from loading Windows normally or even restarting in Safe Mode. If the victim tries to reboot their computer they will be greeted by an ASCII skull and given an ultimatum to pay the ransom or have the files deleted. Trend Micro has informed Dropbox about the malicious files hosted on their service. A Dropbox spokesperson told SCMagazine.com via emailed comments that their team investigated the incident and has since removed the links. Clay said users can avoid infection by improving their email security and implementing messaging solutions that employ advanced detection features specific to phishing and socially engineered emails. (scmagazine.com, 29Mar16)

~~(U//FOUO)~~ New server-side ransomware targets hospitals

~~(U//FOUO)~~ Cisco Talos researchers have discovered the "SamSam" and "Maktub" strains of ransomware that attackers install after exploiting unpatched server vulnerabilities, according to a 29 March online press report. Unlike traditional ransomware that relies on users to execute a malicious e-mail attachment or visit a fraudulent website, attackers using these strains first gain network access before identifying key data systems to encrypt. Attackers have selected hospitals because they are perceived to have weak security and rely on antiquated technology, but researchers warn that other industry sectors will follow. Unlike other ransomware, SamSam and Maktub allow victims to negotiate payments—which are relatively low at present—for bulk decryption. Security firm Check Point said the two strains do not rely on a typical hacker command-and-control backend to encrypt data, and Maktub also compresses the data first to speed up the encryption process. (threatpost.com, 29Mar16)

(U) TreasureHunt POS malware looks to steal your data before it's too late

(U) FireEye researchers spotted a point-of-sale (POS) malware dubbed TreasureHunt that appears to have been custom-built for a "dump shop" that sells stolen credit card data. The malware enumerates running processes, extracts payment card information from memory, and then transmits this information to a command and control (CNC) server, according a 28 March blog post. Cyber crooks are looking to take advantage of memory scrapping POS malware like TreasureHunt before more secure chip and PIN technologies render the data scrapping techniques obsolete, researchers said in the blog. There are currently about 1.2 million merchants that accept the 600 million chip cards now used in the United States. The researchers said cybercriminals often gain access to the POS systems to implant the malware using previously stolen credentials or brute force login attempts with common passwords. (scmagazine.com, 28Mar16)

(U) New ransomware abuses Windows PowerShell and Word document macros

(U) A new ransomware program written in Windows PowerShell is being used in attacks against enterprises, including health care organizations, researchers warn. PowerShell is a task automation and configuration management framework that's included in Windows and is commonly used by systems administrators. It has its own powerful scripting language that has been used to create sophisticated malware in the past. The new ransomware program, dubbed PowerWare, was discovered by researchers from security firm Carbon Black and is being distributed to victims via phishing emails containing Word documents with malicious macros, an increasingly common attack technique. The Carbon Black team found PowerWare when it targeted one of its customers: an unnamed healthcare organization. The malicious Word documents masqueraded as an invoice, the Carbon Black researchers said. When opened, it instructed users to enable Word editing and content, claiming that these actions were necessary to view the files. In reality, enabling editing disables Microsoft Word's "preview" sandbox and enabling content allows the execution of the embedded macro code, which Office blocks by default. If the malicious macro code is allowed to run, it opens the Windows command line (cmd.exe) and launches two instances of PowerShell (powershell.exe). One instance downloads the PowerWare ransomware from a remote server in the form of a PowerShell script and the other instance executes the script. Based on the payment instructions, the attackers use the Tor anonymity network to hide their command-and-control server. The initial ransom is $500, but it goes up to $1,000 after a couple of weeks. PowerWare is not the first ransomware implementation in PowerShell. Security researchers from Sophos found a similar Russian-language ransomware program back in 2013. Then in 2015, they found another one that used the "Los Pollos Hermanos" logo from the Breaking Bad TV show. While PowerShell-based malware is not new, its use has increased in recent months and it is arguably harder to detect than traditional malware because of PowerShell's legitimate use and popularity, especially in enterprise environments. (IDG News Service, 25Mar16)

Incidents of Interest:

OGA

(U) Hackers breach computer networks of some big US law firms

(U) Hackers broke into the computer networks of some big US law firms, including Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP, the Wall Street Journal reported on Tuesday. Federal investigators are looking to see if confidential information was stolen for insider trading, as these law firms represented Wall Street banks and big companies, the Journal said, citing people familiar with the matter. Other law firms were also targeted, but the probe has not amounted to any clear information on what details have been stolen, the newspaper reported. The Federal Bureau of investigation and the Manhattan US attorney's office are investigating the matter, WSJ said. Hackers have threatened more such attacks in postings on the Internet, the Journal said. (Reuters, 30Mar16)

(U) CNBC just collected your password and shared it with marketers

(U) CNBC inadvertently exposed peoples' passwords after it ran an article Tuesday that ironically was intended to promote secure password practices. The story was removed from CNBC's website shortly after it ran following a flurry of criticism from security experts. Vice's Motherboard posted a link to the archived version. Embedded within the story was a tool in which people could enter their passwords. The tool would then evaluate a password and estimate how long it would take to crack it. A note said the tool was for "entertainment and educational purposes" and would not store the passwords. That turned out not to be accurate, as well as having other problems. Adrienne Porter Felt, a software engineer with Google's Chrome security team, spotted that the article wasn't delivered using SSL/TLS (Secure Socket Layer/Transport Layer Security) encryption. SSL/TLS encrypts the connection between a user and a website, scrambling the data that is sent back and forth. Without SSL/TLS, someone one the same network can see data in clear text and, in this case, any password sent to CNBC. The form also sent passwords to advertising networks and other parties with trackers on CNBC's page, according to Ashkan Soltani, a privacy and security researcher, who posted a screenshot. The companies that received copies of the passwords included Google's DoubleClick advertising service and Scorecard Research, an online marketing company that is part of comScore. Despite saying the tool would not store passwords, traffic analysis showed it was actually storing them in a Google Docs spreadsheet, according to Kane York, who works on the Let's Encrypt project. Luckily, the spreadsheet was marked as private, so it wouldn't have been accessible to the public. (IDG News Service, 30Mar16)

OGA

(U) Verizon says security breach leads to customer data leak

(U) Verizon Communications Inc said an attacker had exploited a security vulnerability on its enterprise client portal to steal contact information of a number of customers. The company said the attacker however did not gain access to Customer Proprietary Network Information (CPNI) or other data. CPNI is the information that telephone companies collect including the time, date, duration and destination number of each call and the type of network a consumer subscribes to. Krebs On Security, which first broke the news of the breach, said a member of a underground cybercrime forum had posted a new thread advertising the sale of a database containing the contact information on some 1.5 million customers of Verizon Enterprise. The seller priced the entire package at $100,000, but offered to sell it off in parts of 100,000 records for $10,000 apiece, Krebs added. The vulnerability, which was investigated and fixed, did not leak any data on consumer customers, Verizon said in a statement on Thursday. The company is currently notifying customers impacted by the breach. (Reuters, 25Mar16)

(U) US blames Iran for hacking dozens of banks and New York dam

(U) The Obama administration on Thursday announced the indictment of seven Iranian hackers for a coordinated campaign of cyber attacks on dozens of US banks and a New York dam from 2011 to 2013, signaling an effort by officials to more publicly confront cyber crime waged on behalf of foreign nations. The indictment, filed in a federal court in New York City, described the suspects, who live in Iran, as "experienced computer hackers" believed to have been working on behalf of the Iranian government. The move marks the first time the US government has charged individuals tied to a nation-state with attempting to disrupt critical infrastructure, a vulnerability that security researchers have grown increasingly concerned about in recent months. The charged hackers were identified as Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, Omid Ghaffarinia, Sina Keissar and Nader Seidi, all citizens and residents of Iran. They are accused of conspiracy to commit computer hacking while employed by two Iran-based computer companies, ITSecTeam and Mersad Company. Firoozi is additionally charged with obtaining and abetting unauthorized access to a protected computer. At a news conference announcing the charges, US Attorney General Loretta Lynch said the accused hackers caused tens of millions of dollars in damages in their assault on US banks. But the attack on Bowman Avenue Dam in Rye Brook, New York, was especially alarming to investigators, Lynch said, because the intrusion could have posed a serious threat to the security of Americans. A stroke of good fortune prevented the hackers from obtaining operational control of the flood gates because the dam had been manually disconnected for routine maintenance, she said. The indictment represents the Obama administration's latest attempt to more publicly confront cyber attacks carried out by other countries against the United States. (Reuters, 24Mar16)

(U) Multiple hospitals hit in ransomware attack wave

(U) In the past week alone, three hospitals have reported being victimized by cyber-extortionists. A flurry of ransomware attacks against hospitals in recent weeks suggests that online criminals may have found a new favorite target for cyber-extortion. The latest to get hit are Methodist Hospital in Henderson, Kentucky, and Southern California's Chino Valley Medical Center and Desert Valley Hospital, both of which belong to the Prime Healthcare Service chain. The incident at Methodist Hospital forced it to declare a state of internal emergency earlier this week while administrators tried to restore access to encrypted files and email. Security blog Krebs on Security, which was the first to report on the attack, quoted the hospital's information system director Jamie Reid as describing the malware used in the attack as "Locky," a particularly virulent ransomware sample that surfaced earlier this year. Reid did not respond immediately to a Dark Reading request for comment, so it is unclear if the hospital ended up paying the $1,600 ransom demanded by the attackers to unlock the encrypted files. An attorney for Methodist Hospital interviewed by Krebs on Security had said the hospital had not ruled out paying the ransom. Meanwhile, Fred Ortega, a spokesman for the two California hospitals that were also similarly hit, today claimed the malware did not impact patient safety or compromise health records, staff data, or patient care. Ortega described the attacks as disrupting servers at both hospitals. But measures were quickly implemented that allowed a majority of operations to continue unhindered, he said in comments to Dark Reading."The malware was ransomware," Ortega says. "I can confirm that no ransom has been paid." According to Ortega, in-house IT teams were able to quickly implement certain protocols and procedures to contain and mitigate the disruptions. But he did not elaborate on what those measures were. The attacks on the three hospitals continue a trend that first grabbed attention in February when Hollywood Presbyterian Hospital said it had paid $17,000 in ransom money to regain access to files that had been locked in a ransomware attack. Since then there have been reports of similar attacks on two hospitals in Germany, one at the Los Angeles County health department, and now the three over this past week. Expect such attacks to increase, says James Scott, senior fellow at the Institute for Critical Infrastructure Security (ICIT), which recently released a report on the ransomware threat to organizations in critical infrastructure sectors. (Dark Reading, 24Mar16)

(U) Chinese national pleads guilty to hacking US contractors

(U) A Chinese citizen pleaded guilty 23 March to a "years-long conspiracy to hack into the computer networks of major US defense contractors," the Justice Department announced. The episode is a reminder of the Pentagon's ongoing struggle to keep defense secrets out of the hands of foreign hackers. A 2014 criminal complaint charged Su Bin, whom DOJ described as a "businessman in the aviation and aerospace fields," with being part of a conspiracy to steal technical data related to US military fighter jets and a Boeing Co.-made transport aircraft. In a plea agreement filed 22 March in a US district court, Su admitted to breaking into Boeing's computer networks, among others, from October 2008 to March 2014. Su allegedly emailed co-conspirators tips on what people, companies and technologies to target. He and his Chinese co-conspirators, whom DOJ did not name, emailed reports on what technology that they had stolen to the "final beneficiaries of their hacking activities," according to DOJ. The statement did not name those beneficiaries, saying only that the stolen data was sent to China. About three years after the offenses listed in the plea agreement, China did produce the Y-20 cargo plane, apparently modeled on the Air Force C-17. Su was arrested in Canada in July 2014; he waived extradition and agreed to be brought to the United States in February 2016. Su faces up to five years in prison. His sentencing is scheduled for 13 July. (fcw.com, 23Mar16)

Items of Interest

(U) NASA has a cyber-security problem

(U) Jason Miller, executive editor for Federal News Radio, is saying that the National Aeronautics and Space Administration (NASA) has a severe patching problem that's putting many of its systems at risk. Citing multiple inside sources and internal documents, Mr. Miller is saying that there are hundreds of thousands, if not millions of patches that haven't been applied to NASA IT systems, exposing the company to potential attacks. While NASA's external shield is strong, the investigator says that, once its external protections are penetrated, a skilled attacker would have no barriers if they want to map the agency's entire internal network and access every nook and cranny. Mr. Miller cites various reasons in regard to this situation. First and foremost, NASA is putting missions above everything else. This sometimes means freezing patching operations to mission-related systems in order to avoid any downtime or delays due to bugs or improper patching. Basically, nobody is allowed to touch and patch computers until the mission has ended, leaving systems unprotected for extended periods of time. Additionally, sources inside NASA are also putting the blame on Hewlett Packard Enterprise (HPE), saying the company has been uncooperative and sometimes negligent. HPE won the $2.5 billion ACES (Agency Consolidated End-user Services) contract in 2010 and should have helped NASA revamp its technology infrastructure under the Information Technology Infrastructure Integration Program (I3P). The company has failed to do so, and according to Mr. Miller, it is having trouble keeping up with the massive workload. A NASA spokeswoman has told Federal News Radio, "since the 2015 Cybersecurity Sprint, NASA has made substantial progress in tracking and managing vulnerabilities. This agency effort is reflected in [15 February's] Department of Homeland Security Cyber Hygiene report on NASA, which shows zero critical vulnerabilities older than 30 days since September 2015." In fact, the agency is also preparing to release a new cyber-security tool called Gryphon X, considered by a few experts a cyber-security gamechanger. Mr. Miller has contacted Security Scorecard, a US-based security vendor, who has reinforced his initial investigation by saying that their telemetry data shows over 10,000 constant pings from NASA network to known malware hosts. (Softpedia, 30Mar16)

(U) Cyber insurance rates fall with lull in major hacks

(U) A lull in high-profile data breaches prompted insurers to cut cyber insurance rates for high-risk businesses such as retailers and healthcare companies during the first three months of this year, according to insurance industry brokers. The dip comes after sudden rate hikes for many firms last year in the wake of a spate of attacks on Home Depot Inc, Target Corp, Anthem Inc and others. The average price companies in high-risk industries paid for $1 million in cyber insurance coverage fell 13 percent to $18,756 in the first three months of 2016, according to broker Marsh, a unit of Marsh & McLennan Cos Inc. It said the average premium rose 28 percent last year to $21,642 for comparable buyers in industries such as retail and healthcare. (Reuters, 30Mar16)

(U) Survey finds NIST cybersecurity framework adoption hampered by costs

(U) Security pros consider the NIST framework an industry best practice, yet half of its adopters say its complete implementation involves a high level of investment. US organizations say the major investment required in fully implementing the NIST Cybersecurity Framework is hampering their full adoption of it, according to a survey report released by Tenable Network Security. The Trends in Security Framework Adoption Survey, which includes responses from around 300 US IT and security pros, was conducted to determine patterns in the adoption of various security frameworks. A majority of organizations (84 percent) have at least one security framework in place. While the survey data reveals that 70 percent organizations view NIST's framework as a security best practice, 50 percent see the high level of investment that it requires as a barrier to adoption. The NIST framework was the most popular choice of security frameworks to be implemented over the next year, the study found. Some 64 percent of organizations are using part of the NIST framework and not all of the recommended controls due to the cost and lack of regulatory pressures. Also, 83 percent of those planning to adopt the NIST framework in the coming year say they will take a similar approach -- adopting some and not all of the CSF controls. (Dark Reading, 30Mar16)

(U) UMD startup makes strides in cybersecurity

(U) One of the greatest threats to personal and national security today is malware. It is estimated that nearly one million new malware threats are released each day, leading to annual costs of approximately $4.5 billion in the US alone. SecondWrite, a startup company created by University of Maryland researchers, is working to alleviate threats to computer and software systems one type of malware at a time. UMD Professor of Electrical and Computer Engineering Rajeev Barua, founder of SecondWrite, began researching malware detection in 2014 after realizing his work in program analysis could be applied to cybersecurity. SecondWrite specializes in a certain kind of malware called evasive malware. Cybersecurity software typically detects malware using sandbox space detection, which runs malware in a protected environment in order to catch malicious behavior. However, evasive malware hides from detection by changing its behavior when it is in the sandbox versus when it is running in a live system. Dr. Barua's software forces the evasive malware to behave as it would in a live system while it is in the sandbox, making it easier to detect and stop. SecondWrite is a UMD incubator company through the Maryland Technology Enterprise Institute, or Mtech, which provides support and guidance for entrepreneurs at UMD, and is a member of the National Science Foundation's Innovation Corps (I-Corps) program. SecondWrite has raised nearly $1.5 million from a variety of sources including the National Science Foundation's Small Business Innovative Research (SBIR) program, Maryland's Technology Development Corporation, and private donors. SecondWrite is currently marketing its software to large, established cybersecurity companies with the hopes that the technology will be widely licensed and incorporated into well-known and commonly used malware detection suites. They plan to branch out and explore other kinds of advanced malware detection in the future as the company grows. (University of Maryland, 29Mar16)

(U) Free Bitdefender tool prevents Locky and other ransomware infections

(U) Antivirus firm Bitdefender has released a free tool that can prevent computers from being infected with some of the most widespread file-encrypting ransomware programs: Locky, TeslaCrypt and CTB-Locker. The new Bitdefender Anti-Ransomware vaccine is built on the same principle as a previous tool that the company designed to prevent CryptoWall infections. CryptoWall later changed the way in which it operates, rendering that tool ineffective, but the same defense concept still works for other ransomware families. While security experts generally advise against paying ransomware authors for decryption keys, this is based more on ethical grounds than on a perceived risk that the keys won't be delivered. Many ransomware creators build checks into their programs to ensure that infected computers where files have already been encrypted are not infected again. Otherwise, some files could end up with nested encryption by the same ransomware program. The new Bitdefender tool takes advantage of these ransomware checks by making it appear as if computers are already infected with current variants of Locky, TeslaCrypt or CTB-Locker. This prevents those programs from infecting them again. The downside is that the tool can only fool certain ransomware families and is not guaranteed to work indefinitely. Therefore, it's best for users to take all the common precautions to prevent infections in the first place and to view the tool only as a last layer of defense that might save them in case everything else fails. Users should always keep the software on their computer up to date, especially the OS, browser and browser plug-ins like Flash Player, Adobe Reader, Java and Silverlight. They should never enable the execution of macros in documents, unless they've verified their source and know that the documents in question are supposed to contain such code. Emails, especially those that contain attachments, should be carefully scrutinized, regardless of who appears to have sent them. Performing day-to day activities from a limited user account on the OS, not from an administrative one, and running an up-to-date antivirus program, are also essential steps in preventing malware infections. (IDG News Service, 29Mar16)

(U) Marines forming new cyberwarrior unit

(U) The Marine Corps is standing up a new unit of cyberwarriors as the global battlefield evolves to include more and more computer networks. The Marine Corps Cyberspace Warfare Group was activated Friday in a ceremony at Fort George G. Meade, Md., a Marine Corps statement said. Its mission is to man, train and equip Marine cyberspace mission teams to perform both defensive and offensive operations in support of US Cyber Command and Marine Forces Cyberspace Command. The unit has "a few" cyber teams up and running, the statement said; however, it won't be fully operational until sometime next year. "We've always had the means to communicate and the means to protect that communication, but today we're in an environment where those methods are more and more reliant on a system of transmissions, routers and networks," the unit's commander, Col. Ossen D'Haiti, said in the statement. "So, the ability to protect that, the ability to control that and deny an adversary to interdict that, is crucial to command and control." Everything from power grids, banking, government operations to defense contractor weapons' plans have shifted online in the past few decades. That information is a tempting target for both state-sponsored hackers and criminal organizations that are becoming increasingly sophisticated at cybertheft. During a town hall meeting with Okinawa Marines in November, Marine Corps Commandant Gen. Robert Neller lamented that China had stolen military secrets from the United States. "While we've been fighting, our adversaries, many of them in this part of the world -- pick one: China, North Korea, Iran, Russia -- what have they been doing? Making money, buying new gear, stealing all of our secrets," he said. "Ever look at all the Chinese equipment? What's it look like? It looks like our stuff. How is that? They stole our stuff, fair and square." The Navy, Army, Air Force and Coast Guard are also actively recruiting cyber soldiers and standing up their own cyber units and programs. (Stars and Stripes, 28Mar16)

(U) DOD updates cloud requirements guide

(U) Defense Department IT officials have released an update to a cloud security requirements guide that governs commercial cloud offerings for DOD missions up to the secret level. The SRG helps determine whether defense officials grant commercial cloud firms a provisional authorization to host DOD data. This is the second iteration of the SRG, and it is based on feedback from the first version, released in January 2015. The Defense Information Systems Agency and the DOD CIO's office -- the two organizations that issue the SRG -- are still interested in feedback on the document. "This ongoing public comment period will allow our mission partners to offer changes as they become necessary," said Robert Vietmeyer, associate director for cloud computing and agile development in the DOD CIO's office. DISA also published a history of revisions made to the SRG to track changes to the guidelines. The SRG is part of an ongoing effort by Pentagon IT leaders to better define what cloud computing means for defense missions. That definition can affect how cloud services are implemented. A DOD inspector general audit conducted from December 2014 to October 2015 found that the lack of a standard definition for cloud computing across the department was undercutting the CIO's effort to deploy cloud services. (FCW.com, 28Mar16)

(U) Homeland Security building a massive database to track cyberattacks

(U) The Homeland Security Department wants input on an idea for a broad cybersecurity incident database, accessible by members of the public and private sectors. Businesses could use the database to assess how their cyber practices stack up against competitors, and the federal government could upload its own cyberthreat predictions, DHS suggests in a new white paper fleshing out the concept. Such a repository would ask participants to share specific but anonymized details about cyberincidents and threats, including details such as attack timeline, apparent goal and prevention measures. Until the end of May, DHS is collecting comments on the concept and wants responses on three recent white papers it issued outlining benefits, obstacles and data points participants might be asked to contribute to the repository. There are currently no concrete plans to build or manage that repository, DHS says, and the database could even be managed by a private organization. But the current administration has long encouraged the public and private sectors to share more information about cyberthreats to prevent future incidents. Last February, President Barack Obama issued an executive order directing DHS to promote "Information Sharing and Analysis Organizations" -- sector- or subsector-specific groups sharing information about cyberthreats and practices, and "Information Sharing and Analysis Organizations" that would develop cyber standards. DHS' white papers suggest a shared repository could help organizations calculate the return on their investment in cybersecurity, helping to assess cyber risk. But "unintended consequences" of such a database include the fact that "aggregated data" showing the "total costs or impacts of certain types of incidents to certain industries" could drive up the insurance cost for common cyberincidents, DHS wrote. The department is collecting comment on various points, including: A description of the data points associated with cyberincidents that would be useful to other organizations; potential benefits of a repository not mentioned in the white paper; types of analysis that would be useful to a participating organization; anticipated obstacles that could prevent the repository model from functioning smoothly; and why potential participants might say no to sharing this information. (NextGov, 28Mar16)

(U) FBI wants US businesses to help as cyber extortion gains urgency

(U) The FBI is asking businesses and software security experts for emergency assistance in its investigation into a pernicious new type of "ransomware" virus used by hackers for extortion. "We need your help!" the Federal Bureau of Investigation said in a confidential "Flash" advisory that was dated 25 March and obtained by Reuters over the weekend. Friday's FBI alert was focused on ransomware known as MSIL/Samas.A that the agency said seeks to encrypt data on entire networks, an alarming change because typically, ransomware has sought to encrypt data one computer at a time. The plea asked recipients to immediately contact the FBI's CYWATCH cyber center if they find evidence that they have been attacked or have other information that might help in its investigation. It is the latest in a series of FBI advisories and warnings from security researchers about new ransomware tools and techniques. The FBI first reported on MSIL/Samas.A in a 18 February alert that lacked the urgency of Friday's warning. The February message contained some technicals details but did not call for help. It said that MSIL/Samas.A targets servers running out-of-date versions of a type of business software known as JBOSS. In its latest report, the FBI said that investigators have since found that hackers are using a software tool dubbed JexBoss to automate discovery of vulnerable JBOSS systems and launch attacks, allowing them to remotely install ransomware on computers across the network. The FBI provided a list of technical indicators to help companies determine if they were victims of such an attack. (Reuters, 28Mar16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424