Cyber-Threat Newsletter – 26 Jul 16

Patches & Updates of the Week:

(U) Oracle issues largest patch bundle ever

(U) Oracle has released a new quarterly batch of security updates for more than 80 products from its software portfolio, fixing 276 vulnerabilities. This is the largest Oracle Critical Patch Update (CPU) to date. The average number of flaws fixed per Oracle update last year was 161, according to security vendor Qualys. Furthermore, out of the 276 security flaws fixed in this update, 159 can be exploited remotely without authentication. At the top of the priority list should be the Java patches, which address 13 new vulnerabilities. That's because Java is used in a lot of applications and is installed on a large number of systems. The Oracle Database Server received patches for nine vulnerabilities, one of which is rated critical with a score of nine out of 10 in the CVSS. Meanwhile, the Oracle MySQL database received fixes for 22 new security issues, four of them with a high severity rating. Fusion Middleware products and components received fixes for a total of thirty-five flaws, five of them rated critical with a CVSS score of 9.8. The Oracle Sun Systems Products Suite also received a large number of patches: 34. This includes fixes for the Solaris OS and networking switches that can be targeted by attackers remotely. Depending on their industry vertical, companies should also look at the fixes for industry-specific products such as Oracle Supply Chain, Oracle Communications, Oracle Banking Platform, Oracle Financial Services Applications, Health Sciences, Oracle Insurance Applications, Oracle Utilities Applications and the Oracle products for the retail sector. Issues were identified and patched in application components like Integration Bus, Order Broker, Service Backbone, and Inventory management. Oracle advises users to install patches without delay, warning that attackers constantly try to exploit flaws for which the company has already released fixes. Sometimes attackers are successful because customers didn't apply the existing patches, the company said. (IDG News Service, 20Jul16)

(U) Cisco patches serious flaws in router and conferencing server software

(U) Cisco Systems released patches this week for several vulnerabilities in its IOS software for networking devices and the Cisco and WebEx conferencing servers. The most serious vulnerability affects the Cisco IOS XR software for the Cisco Network Convergence System (NCS) 6000 Series Routers. It can lead to a denial-of-service condition, leaving affected devices in a nonoperational state. Unauthenticated, remote attackers can exploit the vulnerability by initiating a number of management connections to an affected device over the Secure Shell (SSH), Secure Copy Protocol (SCP), or Secure FTP (SFTP). Because it can affect the availability of a critical piece of equipment, like a router, Cisco has rated this vulnerability as high severity. There is no workaround and customers are advised to install the newly released patches. Another flaw fixed in the Cisco IOS XR software could allow attackers to execute arbitrary commands on the operating system with root privileges. This vulnerability affects IOS XR Software Release 6.0.1.BASE and was rated medium severity because the attacker needs to be authenticated as a local user. A denial-of-service vulnerability was also fixed in the Cisco IOS Software. It can be used to crash devices running affected versions of the software by sending specially crafted Link Layer Discovery Protocol (LLDP) packets to them. Exploitation doesn't require authentication, but requires the attacker to be in a position to send LLDP packets. The firmware of Cisco ASR 5000 Series carrier-class platform which is used in 3G and LTE networks received an update that fixes an insecure SNMP (Simple Network Management Protocol) implementation. The weakness would have allowed attackers to read and modify the device configuration. Cisco's meeting servers were also the focus of this week's patch releases. One vulnerability in the HTTP interface of the Cisco Meeting Server, formerly Acano Conferencing Server, could have allowed attackers to launch persistent cross-site scripting (XSS) attacks against users of the interface. Attackers could exploit this flaw by tricking users to click on maliciously crafted links and could then execute rogue JavaScript code in their browsers in the context of the Cisco Meeting Server interface. This could be used to steal authentication cookies or to force them to perform unauthorized actions. Two XSS vulnerabilities were also fixed in the Cisco WebEx Meetings Server version 2.6, one in its administration interface and one in the user interface. Both could be exploited by tricking users to visit specially crafted links and could lead to further attacks. The Cisco WebEx Meetings Server also received patches for an SQL injection vulnerability that could allow attackers to extract information from its database and for a command injection flaw. (IDG News Service, 15Jul16)

(U) Windows 'critical' security flaw hits all versions of OS

(U) Microsoft has addressed a critical vulnerability affecting every version of its Windows operating system. The company announced a patch entitled "Security Update for Windows Print Spooler Components" on 12 July. It confirmed this update was rated Critical for all supported releases of Windows. If exploited, this vulnerability could have enabled a hacker to assume control over a system and execute a man-in-the-middle (MiTM) attack on a user's workstation or print server. The attacker could have also set up a rogue print server on a network. This type of attack would be possible because the Windows Print Spooler server did not correctly validate print drivers when installing a printer from the server. The remote code execution vulnerability would also have let a hacker view, edit, or delete data, install programs, or create new accounts with full user rights. It's explained more in-depth in a blog post by Vectra Networks security researcher Nicolas Beauchesne, as discovered and reported by ZDNet. The flaw affects all versions of Windows from Windows Vista and later, including Windows Server 2008. Microsoft notes this threat poses the biggest risk to users with administrative access, as opposed to those with fewer user rights. Tuesday's update addresses the problem by correcting how the Windows Print spooler service writes to the file system, and issues a warning to users who attempt to install untrusted printer drivers. The patch is available via Windows Update. (InformationWeek, 14Jul16)

Threats & Vulnerabilities of the Week:

(U) Chrome browser extensions discovered engaging in Facebook click fraud

Google has removed a group of malicious browser extensions from its Chrome Web Store, after an independent Danish security researcher discovered that the programs were hijacking users' Facebook accounts for click fraud purposes, using them to "like" links to sketchy webpages. Maxime Kjaer, a 19-year-old computer science student, reported on his Output blog site that he uncovered the scheme after clicking one of several trashy links on Facebook that a friend of his supposedly liked. The link brought him to an adult-oriented content site requiring an age verification process that could only be completed, strangely enough, by first installing a Chrome extension that asks permission to "read and change all your data on the websites you visit". Needless to say, this is a rather excessive request. The suspicious extension allegedly came from the viral content site Viralands.com, and was available in the Chrome store, along with nine other identical programs that collectively amassed over 132,000 users. After analyzing the extension's metadata, Kjaer determined that the age verification pop-up screen was entirely nonfunctional, merely serving as a decoy that concealed the true motives for obtaining such sweeping user permissions. However, another script within the code was more enlightening: this script was coded to download a payload from an external server and execute it. The payload, naturally, was malicious, designed to send links that direct users to a web page containing Facebook tokens, which the extension program can then grab and exfiltrate to the command-and-control server. Cybercriminals can potentially use these access tokens to hijack victims' accounts and use them to read and post messages, statuses and links -- though it is unclear at this time exactly what the perpetrators did with the stolen tokens. Additionally, the malware instructs the extension to use victims' accounts as bots to generate false likes in Facebook-based click fraud campaigns. The malware's code also contained a function designed to subscribe victims to YouTube channels. (scmagazine.com, 20Jul16)

(U) Security software that uses 'code hooking' opens the door to hackers

(U) Some of the intrusive techniques used by security, performance, virtualization, and other types of programs to monitor third-party processes have introduced vulnerabilities that hackers can exploit. Researchers from data exfiltration prevention company enSilo found six common security issues affecting over 15 products when they studied how software vendors use "hooking" to inject code into a process in order to intercept, monitor or modify the potentially sensitive system API (application programming interface) calls made by that process. Most of the flaws enSilo found allow attackers to easily bypass the anti-exploit mitigations available in Windows or third-party applications, allowing attackers to exploit vulnerabilities that they couldn't otherwise or whose exploitation would have been difficult. Other flaws allow attackers to remain undetected on victims' computers or to inject malicious code into any process running on them, the enSilo researchers said in a report sent via email that's scheduled to be published Tuesday. The hooking method is used extensively in the antivirus world to monitor for potentially malicious behavior, but is also used by anti-exploitation, virtualization, performance monitoring and sandboxing applications. Some malware programs also hook browser processes to launch so-called Man-in-the-Browser attacks. Antivirus programs accounted for most of the affected products the security company identified, but one vulnerability also exists in a commercial hooking engine developed by Microsoft and used by over 100 other software vendors. EnSilo identified affected products from AVG, Kaspersky Lab, McAfee/Intel Security, Symantec, Trend Micro, Bitdefender, Citrix, Webroot, Avast, Emsisoft, and Vera Security. Some of these vendors have released fixes for the flaws, but patching is not easy because it often requires recompiling each affected product individually. Microsoft plans to release patches for its Microsoft Detours hooking engine in August, enSilo said. The researchers plan to release technical details of the vulnerabilities during the upcoming Black Hat security conference in Las Vegas in early August. (IDG News Service, 19Jul16)

(U) Attackers use DNSSEC amplification to launch multi-vector DDoS attacks

(U) DDoS attacks are becoming increasingly sophisticated, combining multiple attack techniques that require different mitigation strategies, and abusing new protocols. Incident responders from Akamai recently helped mitigate a DDoS attack against an unnamed European media organization that peaked at 363G bps (bits per second) and 57 million packets per second. While the size itself was impressive and way above what a single organization could fight off on its own, the attack also stood out because it combined six different techniques, or vectors: DNS reflection, SYN flood, UDP fragment, PUSH flood, TCP flood, and UDP flood. The company has observed the same DNSSEC-configured domain name being abused in DDoS amplification attacks against targets in different industries. A separate Akamai advisory released Tuesday describes several DDoS campaigns this year against the network of the Massachusetts Institute of Technology. One of those attacks occurred in April and used DNS reflection by triggering responses for cpsc.gov and isc.org, two DNSSEC-enabled domain names. "The domain owners themselves are not at fault and don't feel the effects of these attacks," the Akamai researchers said. "Attackers abuse open resolvers by sending a barrage of spoofed DNS queries where the IP source is set to be the MIT target IP. Most of these servers will cache the initial response so multiple queries are not made to the authoritative name servers". Unfortunately, DNS is not the only protocol that can be used for DDoS amplification. The NTP, CHARGEN and SSDP protocols are also commonly used in such attacks and, unfortunately, as long as misconfigured servers and devices are available on the Internet, this technique will continue to be favored by attackers. (IDG News Service, 19Jul16)

(U) New ransomware uses rip and run tactics

(U) A new ransomware variant covertly deletes hijacked files while leading the victim to believe they can still be recovered, according to cybersecurity researchers. Discovered by threat intelligence firm Cisco Talos, the Ranscam variant relies on simple intimidation rather than complexity. In a 11 July post, Cisco Talos threat researchers Edmund Brumaghin and Warren Mercer said Ranscam does not encrypt data and then decrypt it when the hijacker's bitcoin ransom has been paid. Instead, it cuts to the chase -- the payoff. Unlike comparatively courteous crypto-ransomware that decrypts data and gives it back to the user after the ransom has been paid, the researchers said Ranscam locks down a computer and threatens victims with complete data and file deletion at every unverified payment click. The attack has no recovery or decryption functionalities. Ultimately, the researchers said, any data decryption promises made by the hijacker are lies because the program simply deletes data almost from the beginning. Brumaghin and Mercer said the lack of encryption/decryption capabilities suggests that cyber thieves have stripped down the malware to make a quick buck with little trouble. It also suggests that the ransomware is making its way down the cybercriminal food chain to its lowest levels. (fcw.com, 15Jul16)

(U) New Locky ransomware version can operate in offline mode

(U) The creators of the widespread Locky ransomware have added a fallback mechanism in the latest version of their program for situations where the malware can't reach their command-and-control servers. Security researchers from antivirus vendor Avira have found a new Locky variant that starts encrypting files even when it cannot request a unique encryption key from the attacker's servers because the computer is offline or a firewall blocks the communication. Calling home to a server is important for ransomware programs that use public key cryptography. In fact, if they're unable to report back to a server after they infect a new computer, most such programs don't start encrypting files. That's because the encryption routine relies on unique public-private key pairs that are generated by the attackers' servers for each computer. Companies can also quickly cut off a computer from the Internet if a ransomware detection is triggered to try to limit the damage. They can also take the whole network offline temporarily until they can investigate if other computers have also been affected. These measures are no longer viable for Locky, one of the most widespread ransomware threats plaguing users today, because of the changes made to it. The good news is that Locky will start encrypting files using a predefined public key that's the same for all offline victims. This means that if someone pays the ransom and obtains the private key, that key will work for all other offline victims as well. Security researchers from F-Secure have observed two massive spam campaigns distributing Locky this week, one of them reaching 120,000 spam hits per hour, more than 200 times higher than the spam hits on a regular day, the researchers said in a blog post. Both campaigns spread emails with rogue zip attachments that contained malicious JavaScript files. The use of JavaScript files to distribute malware has become an attacker favorite in recent months. Such files can be executed on Windows out of the box, without any special software. (IDG News Service, 14Jul16)

(U) Microsoft discovers new version of Troldesh ransomware

(U) Security researchers from the Microsoft Malware Protection Center (MMPC) have come across a new version of the Troldesh ransomware, also dubbed Encoder.858 and Shade Ransomware. While ransomware variants constantly evolve with small tweaks here and there, this version of Troldesh comes with extensive modifications to the threat's entire mode of operation. This recent version of Troldesh has finally made the jump to the Dark Web, utilizing a dedicated payment portal where users can go, enter a special ID from the ransom note, and receive further instructions on how to pay the ransom. Other changes included with Troldesh is the usage of two creative extensions that are added to the end of encrypted files: .da_vinci_code and .magic_software_syndicate. There are also some errors in the ransom note, but not that significant. Additionally, Troldesh now encrypts even more file type categories and also infects users with additional malware called Mexar. This malware is new, and Microsoft saw it for the first time on 7 July. As such, there are very few details about what this threat does. In statistics released a few days ago, Microsoft ranked Troldesh as the tenth most active ransomware family in the past 30 days. (Softpedia, 14Jul16)

(U) Russian developers behind new WildFire ransomware

(U) Quiet and unknown to many users, there's a new piece of ransomware rising in the shadows. It's called WildFire and is currently spreading using the Kelihos botnet. First signs of WildFire were discovered on 21 June. According to the Cisco OpenDNS team, the crooks behind WildFire use the massive Kelihos botnet to send spam emails that contain malicious Word documents. These documents employ social engineering tricks to convince users to enable macros in Word, which eventually allows the ransomware to take hold. The ransomware's source code is still a mystery right now, as there are a few layers of code obfuscation researchers must go through (ConfuserEx, an unknown crypter, and then .NET Reactor), but malware analysts currently know that WildFire connects to one out of four C&C domain servers, where it registers the infection and receives a password and a user ID. These details are used to lock the user's files, and MalwareHunterTeam tells Softpedia that "without getting the password [WildFire] it's not decryptable". For now, users have to pay 0.5 Bitcoin (~$300) to recover their files, and as is the case with similar ransomware, payment is handled via a Tor-based website. When they inspected the WildFire C&C servers, OpenDNS researchers found comments in Russian, written in the source code of one domain, leading them to believe that a Russian-speaking crew may be behind this threat. Coincidentally, this server was set up on 20 June, just one day before researchers first detected WildFire infections. A later inspection by MalwareHunterTeam revealed that this comment was present in all four C&C domains, and even on the Tor website. Furthermore, MalwareHunterTeam says they found the following string in an older version of the ransomware decrypter: "?????????? ????? ???????, ? ??????????? ?????????" [Russian: "Little thiefs are hung, but bigger thiefs are honored"]. (Softpedia, 14Jul16)

Incidents of Interest:

(U) DDoS attack takes down US Congress website for three days

(U) The US Congress has just recovered after a three-day DDoS attack that has crippled its online portal congress.gov, along with adjacent sites such as the US Library of Congress (loc.gov) and the US Copyright Office (coypright.gov). The attack started on Sunday evening, 17 July, and initially targeted the Library of Congress website, affecting the same server infrastructure on which the other two websites were also hosted. Despite initial defensive measures, the attack slowly escalated in the following days and continued to cause trouble for government officials and site visitors. At the time of writing, all three websites are up and running. No other government portals appear to have been affected following a quick inspection. A US Library of Congress spokesperson said the DDoS flood involved some kind of "DNS attack". (Softpedia, 20Jul16)

(U) Turkey blocks access to WikiLeaks after ruling party email dump

(U) Turkey has blocked access to the WikiLeaks website, the telecoms watchdog said on Wednesday, hours after it leaked thousands of ruling party emails just as Ankara grapples with the aftermath of a failed military coup. Around 50,000 soldiers, police, judges and teachers have been suspended or detained since the attempted coup on the weekend, and Turkey's Western allies have expressed concern over the crackdown's reach. WikiLeaks on Tuesday released nearly 300,000 emails from the AK Party dating from 2010 to 6 July this year. Obtained before the attempted coup, the date of their publication was brought forward "in response to the government's post-coup purges", WikiLeaks said on its website. The source of the emails was not connected to the coup plotters or to a rival political party or state, WikiLeaks said. Turkey's Telecommunications Communications Board said on Wednesday that an "administrative measure" had been taken against the website -- the term it commonly uses when blocking access to sites. Turkey routinely uses Internet shutdowns in response to political events, which critics and human rights advocates see as part of a broader attack on the media and freedom of expression. (Reuters, 19Jul16)

OGA

(U) UK rail hit by four cyberattacks in one year

(U) UK's rail network was hacked at least four times in the past one year, reports The Telegraph, quoting Darktrace, which handles security for the rail network. Appearing to be cyber espionage activity conducted by nation-states, the attacks were exploratory in nature and did not disrupt the rail system, Darktrace said. Kaspersky Lab believes that at the moment, state-sponsored attackers were very active without doing much, but hackers could cause chaos if they managed to enter the rail network system. Network Rail has said cybersecurity would play an important part in their plan to introduce digital train control technology. "Safety is our top priority, which is why we work closely with government, the security services, our partners and suppliers in the rail industry and security specialists to combat cyber threats," added a spokesperson. (Dark Reading, 18Jul16)

(U) Two hacker groups claim responsibility for attacks on Pokemon Go servers

(U) The expected has happened. The servers of the insanely popular augmented reality (AR) game Pokemon Go were brought down in a DDoS (Distributed Denial of Service) attack on Saturday. Now, two hacker groups have claimed the responsibility for these attacks. The hacker group, going by the name PoodleCorp, has posted on Twitter that it was able to take Pokemon Go servers offline. PoodleCorp also retweeted a post from a user who claimed to be the leader of the hacking team. "Just was a lil test, we will do something on a larger scale soon," read the Tweet. OurMine hacker group is the other group to claim responsibility for the attack. The group was recently in news for hacking the social media accounts of Twitter, Google and Facebook CEOs as well as of some other celebrities. The group posted on its website: No one will be able to play this game till Pokemon Go contact us on our website to teach them how to protect it! OurMine also said that it would not stop until the Pokemon Go representatives contact them. So far there are not much details available as to which parts of the world were most affected by the attacks according to The Independent, Pokemon Go players in the US and UK were not able to access the game. (Times of India, 18Jul16)

(U) Hackers steal data from Polish defense ministry

(U) A group of hackers who call themselves "Pravyy Sector" [Right Sector] are extorting the Polish Government on Twitter, threatening to release data stolen from Poland's Defense Ministry if the government doesn't pay $50,000, either to a Ukrainian bank account or a Bitcoin address. The name Right Sector is also used by an extremist Ukrainian nationalist organization activating in Russia, currently outlawed. The hackers claim to represent the group, but there's no evidence to support either their claims or their alleged Ukrainian or Russian nationality. To prove that they are, in fact, in possession of authentic data, the group leaked on Twitter some of the files they supposedly stole from the Defense Ministry. This includes official document scans, screenshots showing the desktop of a Defense Ministry computer, and an Excel file with 1,368 entries that seem to be local Intranet logs containing LDAP paths, login times, incorrect logins, and other similar details. An employee of Polish security firm Niebezpiecznik called the person whose data was leaked by the hackers as proof. That person confirmed the document contained his personal details, except his passport and ID card numbers, which had expired in the meantime. This individual also said that the data included in the leaked forms was from the form that military personnel must fill out when volunteering for service abroad. Moreover, he claimed he served once in Afghanistan and twice in Iraq. Later during the day, the hackers supposedly leaked data that showed Poland's involvement in the US PRISM program. This file has been deleted and is not available online anymore. Niebezpiecznik argued, "the data from PRISM look so crafted / false". Polish newspaper Wyborcza stated that a representative of the Polish Defense Ministry gave a classic answer by saying they neither denied nor confirmed the incident. This is not the first time the Polish Defense Ministry suffers a cyber-attack. In March 2013, a hacker named Alladyn2 made his way into the Ministry's computer network and even got access to the computer of the country's president before having his access cut off. Previously to attacking and breaching the Polish Defence Ministry, Pravyy Sector took responsibility for hacking and dumping data online from Polish telecommunications firm Netia. Several days after leaking the data, Netia confirmed the incident. (Softpedia, 15Jul16)

OGA

OGA

(U) Chinese hackers blamed for multiple breaches at US banking agency

(U) Chinese government hackers were the likely attackers in three breaches in recent years at the Federal Deposit Insurance Corporation, the US agency that insures bank accounts, according to a congressional audit. Breaches at the FDIC in 2010, 2011, and 2013 were caused by an "advanced persistent threat... believed to have been the Chinese government," according to an interim report on the agency's cybersecurity from the House of Representatives Science, Space, and Technology Committee. In the 2013 breach, hackers gained access to the computers of 12 staff computers, including the former chairman, chief of staff and general counsel of the agency, the House report said. FDIC staffers were instructed not to report the 2013 breach because news of it could hurt agency Chairman Martin Gruenberg's confirmation, one witness told House investigators. The agency also delayed reporting two late 2015 breaches to Congress until 2016, even though the personal data of more than 115,000 people was potentially compromised, the report said. The agency has "purposefully evaded" congressional oversight and has a "long-standing history of a lack of transparency" related to cybersecurity issues, the report said. "The FDIC's intent to evade congressional oversight is a serious offense," Committee Chairman Lamar Smith, a Texas Republican, said in an emailed statement. "Major improvements need to be made to the FDIC's cybersecurity mechanisms". The House report went on to rip FDIC security practices and the culture inside the agency. The agency's CIO office is a "toxic work environment," where employees who disagree with leadership are punished, the report said. In addition, the agency has failed to stop employee use of USB thumbdrives and other portable storage devices, despite two 2015 breaches related to those devices, the report said. "The FDIC has still not implemented sufficient precautionary measures to ensure that additional breaches do not occur," the report said. Gruenberg is scheduled to testify before the committee about cybersecurity issues on Thursday morning. (IDG News Service, 13Jul16)

Items of Interest

(U) DARPA awards new contract for behavioral cyberattacks detection

(U) The Defense Department's R&D group is buying a system that could rely on a network's behavioral patterns, and any deviation from those, to detect cyberthreats. The Defense Advanced Research Projects Agency awarded a $6 million contract to Galois, a Portland, Oregon-based computer science company, to build out a product that can identify "advanced persistent threats" -- cyberintrusions that allow the actor to remain in the system for an extended period. The solution would detect "subtle but potentially malicious activities" by tracking the behavioral patterns of a complex network and noting "causality in system activity," according to Galois' description of the project. The company is also working with the National Institute of Standards in Technology on an internet of things pilot. Galois is developing a system that could collect consumer data from smart-home devices and services, while attempting to preserve their privacy. It has also demonstrated software to DOD that could help prevent drones from being hacked. Galois' team includes researchers from the University of Edinburgh, the Oregon State University and Palo Alto-based R&D company PARC, a division of Xerox. The networks in large organizations can be so complex that it's difficult to track activity, David Archer, a research lead at Galois, said in a statement. It's possible for these advanced threats to go unnoticed, and during that time steal data "without triggering traditional detection systems". The system aims to track activity across all of an organization's networks and over long periods of time, according to Galois. The group also plans to trace the root cause of anomalous behavior, and eventually, make recommendations about containing the damage. (NextGov, 19Jul16)

(U) Defense Intelligence Agency is scoping out social media background checkers

(U) The Pentagon is conducting market research for a planned 12-month "social media checks" pilot that would analyze public posts to help determine an employee's suitability for Defense Intelligence Agency classified work. The effort is part of a shift away from screening intelligence and military staff every five years, as is current practice. The program is meant to support "continuous evaluation" through automated searches of various data sources, including social media posts, DIA says. The scope of this particular trial run would involve generating "social media reports" that provide "comprehensive and objective data" and expertise to carry out a "whole of person review," in line with Office of Director of National Intelligence guidelines, states a newly released January draft statement of work. In May, DNI chief James Clapper issued a directive approving the use of social media in the public domain to vet personnel. If DIA goes through with a contract, "at a minimum, the service would have to analyze foreign comments and postings, foreign contacts and any information regarding: allegiance to the United States, foreign influence and/or preference, sexual behavior, personal conduct, financial, alcohol, legal and/or illegal drug involvement, psychological conditions and criminal conduct," the work statement says. A DIA official told Nextgov there is no guarantee the agency will solicit any vendor; rather, DIA is figuring out what features companies might be able to offer. The social media reports would help out that agency's existing Personnel Security, Insider Threat, Continuous Evaluation, Counterintelligence and Investigation program, DIA spokesman James Kudla said. "This is part of the larger government effort" for "continuous evaluation monitoring," Kudla said in a brief interview. It's not restricted to the intelligence community; "it's really part of the Department of Defense program as well". "Social media reports are required to identify national security concerns on individuals who are required to obtain and retain a national security clearance" for handling sensitive material, states a 14 July sources sought notice accompanying the work description. The reports should include checks of "all publicly available social media sites," the work statement says. DIA does not specify particular websites, like Facebook, Twitter or other online networks. The analyses also would cross-check an individual's various online personas through "social media profile comparisons," the work statement adds. Clapper's policy states that security clearance investigators cannot create shadow accounts to "follow" or "friend" an employee under review. In addition, social media content about other people inadvertently collected during a check cannot be retained unless the information is relevant to the review of the employee, the directive says. (NextGov, 18Jul16)

(U) NATO CCDCOE considers cyber-warfare cooperation

(U) The need for international cooperation in training cyber-defense experts was emphasized by Finnish Defense Forces chief of general staff vice admiral Kari Juhani Takanen during his visit to the Tallinn-based NATO Cooperative Cyber Defense Centre of Excellence in Estonia last Thursday. "Finland is building up its cyber-defense capability and we need the most knowledgeable people," Takanen said, adding that international cooperation is essential in training experts to counter hybrid threats Reiterating recent NATO statements on cyber-warfare, Takanen added, "threats in cyber-space are real and it is rightfully becoming a domain of warfare. This means nations have to focus on operational issues in the digital space and laws often need to catch up with events on the ground". The NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) is a NATO-accredited knowledge hub, think-tank and training facility which focuses on interdisciplinary applied research and development, as well as consultation, training and exercises in cyber-security. Last month, ahead of the NATO decision to classify cyber-space a theatre of war, a new cyber-policy brief published by the CCDCOE emphasized that the Alliance needs to clearly recognize that network defense does not equal collective defense in cyber-space and develop the full range of military capabilities to defend the Alliance and its interests. The report, Is NATO Ready to Cross the Rubicon on Cyber Defense? by Matthijs Veenendaal, Kadri Kaska and Pascal Brangetto, looked at NATO and national military cyber-defense policies beyond the Warsaw Summit and lays tracks for the future and considered how Allies could best deploy cyber-capabilities in cooperative defense that goes beyond the current NATO policy on cyber defense. "Recognizing cyber-space as a domain of warfare would be an important step in the right direction. This will impel the Allies to define not only terms and definitions but also to establish common ambitions, procedures, and doctrine," says the cyber-policy brief. "Since 2002, NATO has invested significantly in improving the defense of its networks. However, NATO has shown little inclination to move away from its current purely defensive posture in cyber-defense," the analysis reads. "In order to achieve a more mature and realistic cyber-defense posture, the Alliance must address two important issues. Firstly, it must clearly recognize that network defense does not equal collective defense in cyber-space. Secondly, given that NATO accepts the applicability of collective defense in cyber-space, Allies should develop the full range of military capabilities to defend the Alliance and its interests". The authors also called for developing a doctrine and procedures to allow for the use of cyber-capabilities as operational military capabilities. It needs to distinguish the policy mandate applicable to network defense in peacetime from the policy mandate applicable for cyber-operations in military operations and collective defense to ensure that it has the full range of capabilities necessary to deter and defend against any threat in and through cyber-space. (scmagazine.com, 18Jul16)

(U) Chinese takeover of Norway's Opera fails, but alternative deal set

(U) A $1.24 billion agreed takeover of Norwegian online browser and advertising company Opera Software by a Chinese consortium of internet firms has failed, Opera said on Monday, after warning last week the deal had yet to win regulatory approval. As an alternative, the consortium, which includes search and security business Qihoo 360 Technology Co and Beijing Kunlun Tech Co, a distributor of online and mobile games, will take over certain parts of Opera's consumer business for $600 million, Opera said in a statement. The Norwegian firm did not specify the reasons on Monday for the scuttling of the deal other than to say that conditions to close the public offer were not met. The deal had needed the approval of Chinese and US authorities, but last week Opera warned that regulatory approval had yet to be received, without specifying whether approval from China, the United States, or both, was lacking. The Chinese consortium now plans to acquire Opera's browser business, both for mobile phones and desktop computers, the performance and privacy apps section of the company as well as its technology licensing business and its stake in Chinese joint venture nHorizon, Opera said. It will not acquire Opera's advertising and marketing business, its TV operations, nor the apps that are game-related. "Closing of the transaction is expected to take place during the second half of the third quarter of 2016," it said. The revised deal has been approved by Opera's board of directors, Opera said. (Reuters, 18Jul16)

(U) US Cyber Command readies for first troop deployment

(U) The demand for a cybersecurity component that can be deployed to protect US military infrastructure and combat forces is so strong that Cyber Command will begin deploying its cyber troops even before the complete force is trained and staffed. Admiral Michael Rogers, director of the NSA and Cyber Command, said that even though the full complement of 6,200 troops broken in 133 teams has not yet been met, the need for these forces in the field requires that he send in what cyber soldiers he has that are fully trained to meet the threat, according to an NPR report. The first soldiers deploy this fall with the complete Cyber Mission Force staffed and trained by 30 September 2018, NPR said. At that time about half of the group's members will be employed to defend military networks, 20 percent will work with combat troops, 10 percent will protect the nation's infrastructure and the remainder will be in support roles. (scmagazine.com, 15Jul16)

(U) Researchers detect malware in TLS connections without decrypting traffic

(U) Security researchers discovered a way to detect and block malware in Transport Layer Security (TLS) connections without decrypting the traffic. Cisco's researchers Blake Anderson, Subharthi Paul and David McGrew published a report that highlights ways that malware leaves "recognizable footprints in the traffic, even when it is TLS protected." In a report titled "Deciphering Malware's use of TLS (without Decryption)," the authors examined millions of flows of TLS encrypted traffic and tens-of-thousands of malicious TLS flows. The report authors analyzed 18 malware families, including Bergat, Deshacop, Dridex, Dynamer, Kazy, Parite, Razy, Sality, Skeeyah, Symmi, Tescrypt, Toga, Upatre, Virlock, Virtob, Yakes, Zbot, Zusy. The research team used customized software to analyze data features from live traffic and packet capture files. The researchers were able to determine family attribution with 90.3 percent accuracy when using a single, encrypted flow, and 93.2 percent when using all encrypted flows within a 5-minute window. (scmagazine.com, 15Jul16)

(U) DARPA wants robots to automatically patch cybersecurity holes

(U) Hacking teams and their algorithms will square off in a Las Vegas arena, in a contest sponsored by DARPA. The Pentagon agency that brought you robotic cars will bring robotic hackers to a Vegas resort next month. The $2 million Cyber Grand Challenge, sponsored by the Defense Advanced Research Projects Agency, will pit machines against insecure software to pierce the holes -- and fix 'em. The entire event will be shown on screens in the Paris Las Vegas Hotel's 5,000-person auditorium while sportscasters narrate the competition, according to DARPA organizers. The tournament will run in conjunction with an annual Vegas hacker conference called DEFCON. The hope is that computers will be able to discover and patch bugs, like the Heartbleed vulnerability, in any commercial software, including the variety that goes into the F-35, organizers say. The top seven teams from a 2-year-long contest will let their computers run wild at a daylong Capture the Flag-style tournament of code 4 August. Competitors range from Raytheon contractors to former University of California, Santa Barbara students now flung all over the world. The aim of the competition is to "bring that entire discovery-comprehension-patch-response timeline down from a year to minutes or seconds," said Mike Walker, DARPA program manager for the challenge. Another test for the concept of robot hackers might come as early as the next day. DEFCON, which every year hosts a human capture the flag game among programmers, has invited the winning automaton to vie against fingers and brains 5 August. Walker said he does not expect any machine to win against humans at DEFCON. (defenseone.com, 14Jul16)

(U) New cybersecurity software allows novices to create threat models

(U) ThreatModeler, the first enterprise threat modeling software, redefines threat modeling with its intuitive and easy to use interface allowing security and non-security experts to build a threat model in minutes. ThreatModeler is the first to introduce a Centralized Threat Library and an Intelligent Threat Engine that automates the process of threat modeling. By providing functional information about applications or systems, ThreatModeler automatically identifies threats and classifies each by risk to prioritize mitigation strategy early in the application development cycle. With its actionable output and collaborative platform, various stakeholders can act on threats to reduce overall risk. Since its inception in 2011, ThreatModeler's robust interface and consistent forward-thinking has been fueled by a team of threat modeling experts that specialize in cybersecurity pioneering a completely new way for threat modeling to be done. With ThreatModeler, enterprises can end up saving millions of dollars across its threat modeling initiative and reduce overall risk by more than 70 percent. ThreatModeler is currently partnered with leading Fortune 1000 companies in the financial, medical and IoT industries. The company plans to launch an interactive platform that encourages peers to learn and engage with one another in the coming months followed by a new game-changing feature in fall 2016. For more information on ThreatModeler, please visit http://www.threatmodeler.com. (Government Security News, 13Jul16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424