[redacted] Cyber-Threat Newsletter – 02 May 16

Threats & Vulnerabilities of the Week:

(U) ISIS hackers join forces to create mega hacking unit

(U) Through a series of messages posted on official ISIS social media accounts and Telegram channels, the terrorist group has announced the creation of a mega hacking unit called the United Cyber Caliphate (UCC). The new group consists of the Cyber Caliphate Army (CCA), Daesh's main hacking unit, and other pro-ISIS groups that have carried out attacks supporting the terrorists' cause, such as the Sons Caliphate Army (SCA) and Kalacnikov.TN (KTN). Earlier in January 2016, Cyber Caliphate Army also merged forces with Pro-Palestinian hacking group AnonGhost, a former Anonymous division from which the hacktivist group distanced itself. The new hacking group is far from being considered a major threat since none of them has ever carried out anything more than simplistic website defacements and small data leaks. Nevertheless, with all the hackers joining their skills, more dangerous attacks are bound to follow. Since the start of April, security and cyber-intelligence firms like the SITE Intel Group have been tracking UCC's actions. Just in the past days, UCC hackers claimed they've hacked the US State Department and leaked info on 50 staff members, ran a mass defacement campaign against Australian websites, defaced the Russian Federal Customs Service, and leaked information on 18,000 employees of the Saudi Ministry of Defense and Aviation. The group also ran a second mass defacement campaign using the "#KillCrusaders" tag and continued its anti-Christian campaign when it defaced the website of a Michigan church last week, leaving an ominous Jihadi message behind. The biggest data breach since UCC formed also happened last week when the group posted the names and addresses of 3,602 of the "most important citizens of #NewYork and #Brooklyn," asking ISIS sympathizers to use the information and carry out lone wolf attacks. Last year, ISIS had a more reputable cyber division called the Cyber Caliphate (CC) which managed to leak private details of many US servicemen. These leaks got CC's leader, Junaid Hussain, on the US Army's most wanted list. Hussain was eventually killed in a drone strike in Syria last August. Ever since then, the newly formed Cyber Caliphate Army never lived up to the name and reputation set by Hussain and his collaborators, one of which was arrested in February 2016. (Softpedia, 26Apr16)

(U) Microsoft vulnerability lets hackers bypass app whitelisting protections

(U) A researcher has discovered a way for attackers to sneak remotely hosted, unauthorized applications -- more specifically, COM (Component Object Model) objects -- past Microsoft Windows' whitelisting security feature Applocker, by abusing the command-line utility Regsvr32. Normally, Regsvr32 allows users to register Dynamic Link Library (DLL) files and ActiveX controls, but on his blog, Colorado-based researcher Casey Smith recently explained that hackers can place a malicious script block inside the registration tag, and then have Regsvr32 successfully execute the code. The trick works on the business editions of Windows 7 on up. No administrator access is required to perform this workaround, and the process does not alter the system registry, making this vulnerability-based hack a difficult one to detect. (scmagazine.com, 25Apr16)

(U) New technique hides RATs in memory, never touching disk during its execution

(U) Researchers discovered a new trick for concealing the installation of Remote Access Trojans (RATs), after identifying malware samples that never touch the hard drive throughout execution, remaining in memory until the malware is fully enabled and cybercriminals can take control. According to a blog post by SentinelOne, this new under-the-radar technique helps the attack avoid detection from not only traditional antivirus solutions that look for malicious code signatures, but even some next-generation solutions that monitor only file-based threat vectors. Joseph Landry, senior security researcher at SentinelOne, told SCMagazine.com that the technique was first discovered in February, and while it was spotted initially in a handful of Asian countries it has most recently surfaced in the US as well. This novel technique can be applied broadly to any known RAT, although the sample SentinelOne specifically found and analyzed was the malware known as NanoCore. Once downloaded, the malware connects to a command and control server, located on the chickenkiller.com domain, which appears to have been taken down. Upon connection with the C&C server, the payload is not actually written to disk. Instead, it is injected into a new process created in memory instead. To further evade cybersecurity measures, the technique "encodes and encrypts the payload and stores it inside of image files, which would normally looks innocuous to antivirus solutions." This particular malware strain also was programmed to detect and avoid sandbox environments that researchers may have set up to dissect the malicious code. To combat this particular threat, Landry recommended a behavior-based anti-malware solution capable of identifying and analyzing unusual system behavior on a kernel level. (scmagazine.com, 21Apr16)

(U) New CryptoBit ransomware could be decryptable

(U) PandaLabs, Panda Security's anti-malware lab, detected a new type of ransomware that they think could be reverse engineered to allow users to recover their files. Named CryptoBit, this particular ransomware variant infects users via exploits. First infections appeared at the start of April. After infection, CryptoBit will first and foremost scan for files that have particular extensions. By default, it will look for 96 different file types, searching for regular data storage files, such as images, file archives, databases, and office documents. Once CryptoBit identifies all valuable files, it will proceed to encrypt them using the AES algorithm that employs one key for encryption and decryption. The AES encryption key itself is then encrypted with an RSA algorithm, which is a dual-key encryption model that uses a different key for encryption (public key) and decryption (private key). Researchers say the private key is most likely sent to a server under the ransomware author's control. After the encryption process ends, CryptoBit will display a ransom note telling the user their files were encrypted and that they must contact the ransomware's author via an email address or the Bitmessage network, using a special ID. According to PandaLabs researchers, there might be a flaw in CryptoBit's armor. "We notice[d] a specific detail: the absence of calls to the native libraries that encrypt files using the RSA algorithm," PandaLabs researchers say. "CryptoBit uses a series of statically compiled routines that allow you to operate with large numbers ('big numbers'), making it possible to reproduce the RSA encryption algorithm." As it looks right now, it may be possible for security researchers to reverse-engineer the ransomware's custom RSA encryption operations and recover the original AES encryption file. (Softpedia, 21Apr16)

(U) FBI warns farmers about the dangers of hackable IoT farm equipment
(U) Farmers who employ Internet-connected and precision farming equipment should be very mindful of the way they configure their devices, the FBI warned in a public statement advisory at the end of March. The Bureau, together with the US Department of Agriculture (USDA), issued the note on 31 March, as an alert to the growing threat of IoT security. The FBI is particularly warning against data breaches that may expose farming data saved with various companies or on cloud accounts. Additionally, the FBI is also sounding the alarm against hacktivists who might target farmers as a way of protesting against the US' agricultural policies. An incident like this happened last fall, when an Anonymous hacker leaked data of USDA employees to protest against Monsanto. FBI and USDA officials claim they want to prevent a disastrous situation from repeating in the agricultural sector, similar to the one that occurred in the healthcare industry, which was caught unprepared for the arrival of the Internet of Things. For this, the FBI has put forward a series of recommendations on which US farmers can build their cyber-security policies. [1] Monitor employee logins that occur outside of normal business hours. [2] Use two-factor authentication for employee logins, especially remote logins. [3] Create a centralized Information Technology email account for employees to report suspicious emails. [4] Provide regular training to remind and inform employees about current social engineering threats. [5] Monitor unusual traffic, especially over non-standard ports. [6] Monitor outgoing data, and be willing to block unknown IP addresses. [7] Close unused ports. And [7] utilize a Virtual Private Network (VPN) for remote login capability. (Softpedia, 21Apr16)

Incidents of Interest:

OGA

[redacted]

(U) Empty DDoS threats earn extortion group over $100,000
(U) Extorting money from companies under the threat of launching distributed denial-of-service attacks (DDoS) against their online properties has proven lucrative for cybercriminals. So much so that one group has managed to earn over $100,000 without any evidence that it's even capable of mounting attacks. Since early March, hundreds of businesses have received threatening emails from a group calling itself the Armada Collective, asking to be paid between 10 and 50 bitcoins -- US$4,600 to $23,000 -- as a "protection fee" or face DDoS attacks exceeding 1Tbps. While many of them did not comply, some did; the group's bitcoin wallet address shows incoming payments of over $100,000 in total. Yet none of the companies who declined to pay the protection fee were attacked, website protection firm CloudFlare found. The conclusion is that whoever is behind the latest Armada Collective DDoS threats is just reusing the name of a previous group that did attack companies last year, but whose activity ended in November. (IDG News Service, 26Apr16)

(U) Malware shuts down German nuclear power plant on Chernobyl's 30th anniversary
(U) A routine security audit has discovered malware on the computer systems of the Gundremmingen nuclear power plant in Germany. RWE, the plant's operator, shut down the power plant for precaution, despite saying it was nothing serious. According to a press release put out by Gundremmingen power plant officials, the malware was discovered on the plant's Block B IT network that handles the fuel handling system. The malware affected only the computer IT systems and not the ICS/SCADA equipment that interacts with the nuclear fuel. Officials say the equipment's role is to load and unload nuclear fuel from the power plant's Block B and then transfer old fuel to the storage pool. Gundremmingen officials said the IT system was not connected to the Internet and that they suspect someone brought in the malware by accident on a USB thumb drive, either from home or computers found in the power plant's facility. Authorities did not reveal the name of the malware strain but said it was nothing serious, classifying the whole incident as "N" (normal category). The malware infection was discovered Sunday on 24 April, and two days later the power plant is still offline. Today, 26 April 2016, marks 30 years since the Chernobyl nuclear power plant disaster. The nuclear plant is now going through all the security procedures involved with such events, with its staff scanning all other computer systems and going through all the regular checks and motions before putting the plant back into production. (Softpedia, 26Apr16)

(U) Facebook social login bug, now fixed, exposed account holders to potential ID theft
(U) Facebook has updated its social login process - a form of authentication that allows users to sign in to third-party websites via their Facebook social accounts - after a security firm discovered a bug that could have enabled adversaries to steal their victims' online identities undetected. According to a blog post today from Romania-based Bitdefender, a hacker looking to exploit the flaw would require a potential victim's email address -- one that he or she had previously registered with any number of websites that require a user account - just as long as that same email address was not also registered with Facebook. [Of course, many users have multiple email accounts, not all of which are registered with Facebook, meaning it's certainly plausible for an email address to meet this criterion.] Bitdefender vulnerability researcher Ionut Cernica figured out that if a hacker created a brand new, fraudulent Facebook account using a victim's stolen email address, the hacker could then immediately go into account settings and change that email address to his own personal email address - and Facebook would validate and accept both addresses, with the victim's stolen email listed as the primary contact. Simply by swapping in his own email as the primary contact, the hacker would then be able to use Facebook's social login technology to sign in as the victim on certain websites where the victim had previously registered the stolen email address. From there, the bad actor could perform any number of fraudulent acts using the victim's online identity, including purchasing items on e-commerce sites. The Facebook-based login process uses the OAuth protocol as its open standard for account authorization. A source familiar with the vulnerability said if an individual had tried to exploit the flaw, it would not have worked on every website that enables Facebook login - only those whose OAuth-based process failed to properly merge victims' website accounts with their Facebook accounts. Furthermore, there so far are no reports of anyone actually leveraging this exploit successfully. Alexandru Balan, chief security researcher at Bitdefender, said that OAuth security issues will surface from time to time. "On one hand you have isolated issues, which are quickly fixed, in the OAuth provider (Google, Facebook, Twitter, LinkedIn, etc.), with different outcomes - impersonation, for example, in our case," said Balan, in an email interview with SCMagazine.com. "On the other hand, there's the more dangerous scenario where the service using OAuth gets hacked. Let's say, for instance, that you used Twitter to log on somewhere, and the permission [that is] granted, as is very often the case with Twitter, was 'This app can post on my behalf.' If that app or website you logged on to gets hacked, the hackers will be able to post on your Twitter account," Balan continued. Facebook issued the following statement to SCMagazine.com: "This bug was difficult to exploit at a large scale and didn't involve compromising Facebook accounts or company networks. However, we appreciate Ionut's coordination with our bug bounty team to quickly resolve this issue." Balan himself acknowledged that the attack surface for this potential exploit "can be considered to be small, but with high impact" should an attacker have successfully hit on a vulnerable email address. "I think it's important to mention that all major service providers are very responsible with their security," added Balan. "They are open to hearing from independent researchers and fix their stuff very quickly. But I would sincerely recommend that everyone, every now and then, check what apps are enabled in what platform and with what permissions - and what would happen if the provider of one of those apps got hacked". (scmagazine.com, 26Apr16)

(U) Hacker finds Facebook backdoor leaking usernames and passwords
(U) The use of bounty programs to track down security vulnerabilities in websites and software is increasingly common these days, and it's a tactic employed by Facebook. One bounty hunter -- or penetration tester -- hacked his (or her… they are anonymous) way into the social network and made the shocking discovery that someone had already installed a backdoor. Orange Tsai managed to compromise a Linux-based staff server and found there was already a piece of malware in place syphoning off usernames and passwords. These account details were being transmitted to a remote computer, and after revealing this to Facebook, Tsai pocketed $10,000 as a reward. Facebook says that the malware was installed by a security researcher who was trying to earn themselves a bounty. Tsai, who works for Devcore in Taiwan, has provided a detailed write-up of what poking around Facebook servers revealed. Using a reverse lookup, Tsia discovered the existence of files.fb.com which was running Accellion's Secure File Transfer service which is known to suffer from certain vulnerabilities. Using an SQL injection vulnerability, Tsai was able to execute remote code on the server and gain control of it. It was at this point that password-stealing PHP scripts were found to be present. In a statement, Facebook security engineer Reginaldo Silva said: "We're really glad Orange reported this to us. In this case, the software we were using is third party. As we don't have full control of it, we ran it isolated from the systems that host the data people share on Facebook. We do this precisely to have better security." Facebook stresses that no user information was compromised by the backdoor. (BetaNews, 24Apr16)

Items of Interest

(U) DARPA seeks to boost cyber attribution

(U) The US government considers attribution a key element of its strategy to deter hacking by other countries. A broad agency announcement from the Defense Advanced Research Projects Agency seeking technologies to improve the government's ability to attribute a cyberattack to a source. DARPA is looking for technologies that create "operationally and tactically relevant information" about multiple concurrent cyber campaigns, the announcement states. The program also looks for a means of sharing information gleaned from attribution tools with any number of parties without exposing sources and methods. DARPA is seeking technologies to extract biometrics from devices and algorithms for developing behavior profiles related to cyber campaigns, for example. Current means of tracking malicious cyber campaigns, such as using file hashes, aren't good enough because they allow hackers to evade defenders by "superficially changing their tools," according to DARPA. "Malicious actors in cyberspace currently operate with little fear of being caught due to the fact that it is extremely difficult, in some cases perhaps even impossible, to reliably and confidently attribute actions in cyberspace to individuals," the announcement states. The announcement is available at: www.fbo.gov/spg/ODA/DARPA/CMO/DARPA-BAA-16-34/listing.html. (fcw.com, 26Apr16)

(U) CryptXXX ransomware decrypter available for download

(U) Today, Kaspersky Lab has released an updated version of the RannohDecryptor ransomware decryption toolkit that can also handle CryptXXX infections. CryptXXX is one of the most recently discovered ransomware variants that have surfaced in the past week. The ransomware works just like any other piece of crypto-ransomware we've seen on the market in the last few months, but this is not the most dangerous detail about its mode of operation. According to Proofpoint researchers, the ransomware is distributed by a well-oiled cyber-crime machine that has also distributed in the past malware such as the Reventon ransomware and the Bedep clickfraud malware. Besides encrypting files, the ransomware also collects a lot of personal information from infected computers and even tries to steal Bitcoin from cryptocurrency wallets. Nevertheless, Kaspersky researchers were able to find a weak point in the ransomware's operations and have adapted their RannohDecryptor to handle this new threat.In order to discover the encryption key that CryptXXX used to lock the victim's files, users need to have an unencrypted copy of an encrypted file, so the decrypter can compare the two. After RannohDecryptor obtains the decryption key, users only need to tweak the application's settings for their local PC setup and run it to start decrypting files. Depending on the number of files CryptXXX locked, it will take a few hours to decrypt all your data. (Softpedia, 26Apr16)

(U) US cyberbombs ISIS in renewed tech warfare

(U) ISIS has been able to gain notoriety not only because of the atrocities committed, but through incredibly careful and calculated use of technology in general and the internet specifically. The likes of Twitter and Facebook have been embroiled in an on-going battle against terrorist social media accounts, and now the US military is taking the fight online as well. Cyber Command is waging cyber war on Islamic State, trying to cyberbomb the terrorist organization into submission and prevent it from recruiting or spreading propaganda online. Using information gathered from the NSA, Cyber Command has turned its attention away from its usual targets such as Russia and China to focus instead on ISIS. The aim is to use cyberattacks to interfere with the day-to-day operations of ISIS, reports the New York Times -- everything from running payroll to issuing commands. The cyberattacks take a number of forms, including not only intercepting and blocking communication, but also altering messages that are sent. US officials have been surprisingly open in talking about the use of cyberweapons, perhaps an acknowledgement that support for further physical war is on the wane. It also serves as a way for the government to highlight value of surveillance campaigns such as those run by the NSA. If data gathered in this way can be seen to be used against a high-profile target such as ISIS, it will act as quite PR boost at a time when people are more concerned about privacy than ever before. (BetaNews, 25Apr16)

(U) Reserving the right to refuse service, Silicon Valley firms prefer selling tech abroad

(U) According to Defense One, at least three Silicon Valley companies have turned away from US military contracts in favor of foreign buyers. American tech companies cite unreasonable demands, including overly long decision-making cycles, and a rapacious hunger by the Defense Department for the blueprints and schematics of proprietary technology. Defense One names three companies; Liquid Robotics, Savonix and Hytrust, that have sold high-tech suitable for military purposes to foreign clientele. According to representatives of these companies, despite their best efforts to support their country, the US Department of Defense is fast becoming an unwelcome customer. The reasons include taking too long to make decisions, and, most notably, too many demands for proprietary information that is often then offered to third parties as part of a clumsy attempt by the Pentagon to create competition. "We're in almost every country in Asia. And they make decisions, rapid decisions. And we're in, selling our platform. And if we're in, selling our platform and we're not selling it to our government at the same pace, that worries me," said Liquid Robotics CEO Gary Gysin. According to Mylea Charvat, the Savonix founder: "[investors] don't want a sale cycle that's [even as long as] nine to 18 months." "So just think of that, in the context of the prime contract process with the United States government, that can take a decade." According to business observers, these appropriations methods cause Silicon Valley companies to sell their state-of-the-art products to European, African and Asian countries instead. Another, more troubling, obstacle for companies is the Pentagon demand for proprietary information. "They want you to go into the kind of detail that would make a patent officer blush," states Charvat. According to her, the information is typically revealed to third party groups, in an effort to create artificial competition. "What they also want to do is show this to all these other companies and see if they can do it too," she says. A program, seen by many as a personal initiative by US Secretary of Defense Ashton Carter, called DIUx (Defense Innovation Unit Experimental), aims to address these concerns. If the program succeeds, it could close the gap between the DoD and Silicon Valley contractors. However, according to the House Armed Services Committee, "that outreach is proceeding without sufficient attention being paid to breaking down the barriers that have traditionally prevented nontraditional contractors from supporting defense needs, like lengthy contracting processes and the inability to transition technologies," which, in simple English, means the US DoD is having difficulty doing business with the brightest kids in the room. (Sputnik, 23Apr16)

(U) DARPA focuses on denial of service cyber attacks

(U) US military researchers have awarded contracts to two organizations for a cyber security project to develop fundamentally new defenses against distributed denial of service (DDoS) cyber attacks on US military data networks. Officials of the US Defense Advanced Research Projects Agency (DARPA) have awarded contracts to Applied Communication Sciences, a Vencore Labs Company in Basking Ridge, N.J.; and to George Mason University in Fairfax, Va., for the Extreme DDoS Defense (XD3) project. The DARPA XD3 program seeks to develop fundamentally new DDoS defenses that afford far greater resilience to these attacks, across a broader range of contexts, than existing approaches or evolutionary extensions can. Applied Communication Sciences won a total of $15.2 million this month in XD3 contracts -- $5.8 million on 12 April, and $9.4 million on 14 April; while George Mason won $4.4 million in XD3 contracts on 12 April. DDoS attacks are attempts to overwhelm and crash computer network servers with an overwhelming number of online queries from many different nodes on the Internet. Such attacks come from sets of networked hosts that collectively act to disrupt or deny access to information, communications, or computing capabilities, generally by exhausting the target's critical resources such as bandwidth, processor capacity, or memory. Typical victims of these attacks include information storage and computing facilities; servers that handle content distribution, message forwarding, or command and control (C2); and portions of network infrastructure. Botnet-induced volumetric attacks, which can generate hundreds of gigabits per second of malicious traffic, are perhaps the best-known form of DDoS. Low-volume DDoS attacks, however, can be even more difficult because they target specific applications, protocols, or state-machine behaviors while relying on seemingly innocuous message transmission to thwart traditional intrusion-detection techniques. Typical DDoS defenses today rely on combinations of network-based filtering, traffic diversion and scrubbing, or replication of stored data to dilute volumetric attacks and to provide diverse access for legitimate users. Still, existing DDoS defenses have their problems. First, they are too slow; formulation of filtering rules often taking hours to formulate and instantiate, while military communication can't stand disruptions longer than a minute or two. Low-volume DDoS attacks remain exceedingly difficult to identify and block, and mechanisms that rely on in-line data inspection don't handle encryption well and are difficult to scale. In addition, DDoS defenses must work in real time; techniques that are only useful for protecting the storage and dissemination of quasi-static data are insufficient. The XD3 program focuses on three broad areas: thwarting DDoS attacks by dispersing cyber assets to complicate targeting; by disguising defenses to confuse or deceive the adversary; and by adaptive mitigation to blunt the effects of attacks that get through initial defenses. Cyber experts from Applied Communication Sciences and George Mason University are focusing their DARPA XD3 work on manageable dispersion of cyber resources; networked maneuver; adaptive endpoint sensing and response; as well as integrating technologies from these three areas. (militaryaerospace.com, 21Apr16)

(U) New Air Force cyber doctrine stresses resilience

(U) A new Air Force directive makes clear that the service's cyber operatives are expected to keep networks running in the face of hacking attacks. The Air Force shall "develop weapons systems, capabilities, and [tactics, techniques and procedures] to 'fight through' enemy offensive cyberspace operations to ensure continued mission assurance in hostile cyber environments," Air Force Secretary Deborah Lee James declares in the directive. The 12 April document tasks Air Force personnel with "fully exploiting the man-made domain of cyberspace" to support Air Force missions. The instruction shows how the Air Force is adapting its organizational structure to a domain that shapes operations from beginning to end. The sweeping instruction covers all Air Force IT systems and infrastructure. The new policy also highlights the power of select officials: the service's deputy chief of staff for operations, for example, is charged with both developing policies for defensive and offensive cyber operations, and with integrating intelligence and cyber operations. The directive wants both greater data sharing and enhanced security -- and apparently assumes that any tension between those goals in manageable. An accompanying directive covering "information dominance governance and management" lays out how the Air Force will align various cyber programs and capabilities. That memo also instructs personnel to test and evaluate all IT for interoperability and, "as necessary, determine tradeoffs among mission effectiveness, cybersecurity, efficiency, survivability, resiliency and IT interoperability." Steven Aftergood, director of the Federation of American Scientists' Project on Government Secrecy, welcomed the release. Military cyber doctrine "has become one of a number of significant policy areas in which [the Obama] administration is demonstrably 'more transparent' than its predecessors," Aftergood wrote in a blog post about the directive. But the National Security Agency has the last word on the classification of certain cybersecurity-related information. A new memo from the Committee on National Security Systems, a government body chaired by DOD CIO Terry Halvorsen, reminds agency heads that they need to consult with NSA when developing classification guides for information on the cybersecurity of national security systems. (fcw.com, 20Apr16)

[redacted]

(b)(3) 10 USC ⊥ 424

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

[redacted]

(b)(3) 10 USC ⊥ 424