Cyber-Threat Newsletter – 28 Mar 16

Threats & Vulnerabilities of the Week:

(U) Highly complex USB trojan targeting air-gapped systems discovered

(U) Security experts are warning organizations about a new USB trojan that is extremely difficult to spot, can target air-gapped systems, and is ideal for cyber and industrial espionage campaigns. Nicknamed USB Thief (detected as Win32/PSW.Stealer.NAI trojan), this is probably the most complex trojan ever discovered, using encryption and self-protection procedures to infect targets and hide from prying eyes. As ESET's Tomáš Gardoň explains, the trojan binds itself on each USB stick, using the USB drive's details (as an encryption key) to hide its malicious files under AES128 encryption. If the trojan is copied to another USB or on a classic storage device, the encryption breaks, and the content of the malicious files cannot be determined. It is clear that USB Thief was implemented for covert operations, where the attacker impregnates one USB at a time, for the sole purpose of targeting one person or organization. Once the USB stick is plugged into a computer, the trojan steals data like pictures and documents, and stores them in an encrypted format on the same USB drive. After the USB is pulled out of the computer, victims or security researchers investigating the attacked system have no clue as to what happened because the trojan leaves no traces behind on the attacked PC. A peculiar USB Thief feature is the presence of a self-protection mechanism that makes reverse engineering extremely difficult. While the above-mentioned infection scenario involves a malicious actor putting the USB Thief-infected trojan in a computer and launching the malicious application, this is not the only attack scenario. Mr. Gardoň says that USB Thief can also be packed as a plugin or add-on for portable applications often installed on USBs, like Firefox, Chrome, TrueCrypt, Notepad++, and so on. An attacker could find ways to deliver the trojan to the victim's USB, hide it as a plugin in one of those portable apps, and let the victim carry the trojan into air-gapped systems and use it in their own time. When the portable app is launched into execution, the trojan would execute as well, the attacker only needing to show patience to let the attack roll out on its on. (Softpedia, 23Mar16)

(U) Wireless mice leave billions at risk of computer hack

(U) Marc Newlin and Balint Seeber are checking how far apart they can be while still being able to hack into each other's computers. It turns out its pretty far -- 180 meters -- the length of a city block in San Francisco. The pair work for Bastille, a startup cyber security company that has uncovered a flaw they say leaves millions of networks and billions of computers vulnerable to attack. Wireless mice from companies like HP, Lenovo, Amazon and Dell use unencrypted signals to communicate with computers. "They haven't encrypted the mouse traffic, that makes it possible for the attacker to send unencrypted traffic to the dongle pretending to be a keyboard and have it result as keystrokes on your computer. This would be the same as if the attacker was sitting at your computer typing on the computer," said Newlin, a security researcher at Bastille. A hacker uses an antenna, a wireless chip called a dongle, both available for the less $20, and a simple line of code to trick the wireless chip connected to the target computer into accepting it as a mouse. "So the attacker can send data to the dongle, pretend it's a mouse but say 'actually I am a keyboard and please type these letters'," added Newlin. "If we sent unencrypted keyboard strokes as if we were a mouse it started typing on the computer, typing at a 1000 words per minute," said Chris Rouland, the CTO and Founder of Bastille. At a thousand words a minute, the hacker can take over the computer or gain access to a network within seconds. Bastille is hoping to cash in on its security flaw findings and offer new types of sensors that take into account more of the threats present in a wireless world. In the meantime, Bastille is keeping tabs on the wireless mouse problem. They say some companies are starting to offer firmware updates to correct the security issues. Bluetooth devices are not vulnerable to this type of attack. (Reuters, 23Mar16)

(U) TeslaCrypt 4 ransomware now even more dangerous for victims

(U) It's been just a year since the first version of TeslaCrypt appeared on the scene, and it's now hit version 4, continuing to threaten victims with sharing their files online, it now boasts what is being referred to as 'unbreakable encryption'. Heimdal Security warns that not only is the ransomware more powerful than ever, it has also been patched with a number of 'bug fixes'. This means that it is now better equipped to deal with very large files, while the use of RSA 4096 means that recovery of data is completely impossible. Specialists at Heimdal Security say that the previously-reliable TeslaDecoder tool is now worthless. Until now, files larger than 4 GB would get permanently damaged when encrypted. As another improvement, this is no longer an obstacle for the attackers. In the case of data compromise, only two options remain: to restore the data from a secure backup or to pay the ransom. Similarly to previous campaign, TeslaCrypt 4 is being dispersed through drive-by attacks carried out using the Angler exloit kit infrastructure. Over 600 domains spreading Angler have been blocked today and the daily average is predicted to increase to up 1200 domains per day, on average. The speed with which TeslaCrypt is being developed is worrying, and it seems all but impossible for anti-malware tools to keep pace. In the event of infection, the only real recourse is to fall back on a backup, so the advice would be to make sure that one exists and is kept up to date. This of course does nothing to mitigate against the damage following the leaking of private data, whether it belongs to an individual or a company. (BetaNews, 21Mar16)

(U) Attackers can hijack 95 percent of all HTTPS connections

(U) HSTS helps webmasters protect their service and their users against HTTPS downgrades, man-in-the-middle attacks, and cookie hijacking for HTTPS connections. According to a recent Netcraft study, 95 percent of all of today's servers running HTTPS either fail to set up HSTS or come with configuration errors that open server-client connections to the above-listed attack scenarios. What's more interesting is the fact that Netcraft has been running the same scan for the past three years, and proper HSTS usage has remained at the same levels. This shows that webmasters aren't learning or being told that they've set up HSTS in an incorrect manner or that they just don't care. The easiest attack scenario against these insecure sites is the HTTPS downgrade attack, during which attackers can choose multiple methods of forcing a seemingly secure HTTPS connection into using no encryption at all or a weaker certificate that can be attacked and broken later on. According to security researchers, among those 95 percent sites that have failed to set up HSTS, you can find a lot of banks and websites that handle financial operations. (Softpedia 19Mar16)

(U) Malware botnet can be abused to launch DDoS attacks

(U) An independent security researcher that goes by the name of MalwareTech has discovered a way in which he could abuse the ZeroAccess malware's botnet to launch reflection DDoS attacks with an above-average amplification factor. ZeroAccess is a trojan that infects Windows computers and then starts communication with a C&C (command and control), which in turn tells the trojan to download various types of other, more dangerous malware, usually clickfraud bots or Bitcoin mining software, operating hidden from the user's view. The ZeroAccess botnet appeared in 2011, and because of an effective rootkit component and P2P-like structure, it even managed to survive a takedown attempt orchestrated by Microsoft in December 2013. MalwareTech discovered that ZeroAccess allowed its bots to relay messages from one to another, some acting like smaller servers (supernodes) while the rest were just end-points (workers). To relay orders from the C&C server to supernodes and workers, ZeroAccess used simple UDP packets. Because of its complex mesh structure, when a UDP packet arrived at a supernode, the bot would add more information to the packet, containing various details about the network's structure. The supernode would add 408 bytes on top of the original 16, for a total of 242 bytes. Since UDP packets can have their destination address spoofed, an attacker that managed to map ZeroAccess' bot network would be able to send UDP packets to its bots, some of which would then amplify the traffic by 26.5, sending it back to the spoofed destination (the victim's IP). This scenario is your typical reflection DDoS attack, carrying a 26.5 amplification factor, which is more than double the typical 2-10 amplification factor seen in other types of reflection DDoS attacks. Theoretically, this wouldn't have been a problem, since most bots infect users that are sitting behind NATs (Network Address Translation), software programs that translate public IPs to private IP addresses, in order to maximize IPv4 address space usage. But, MalwareTech found a way around this issue as well, allowing him to involve ZeroAccess supernode bots into DDoS attacks even if sitting behind a router. All of this is only theoretical since the researcher did not want to commit a crime just to test out his theory. (Softpedia, 18Mar16)

(U) FBI warns automakers and owners about vehicle hacking risks

(U) The FBI and US National Highway Traffic Safety Administration (NHTSA) issued a bulletin Thursday warning that motor vehicles are "increasingly vulnerable" to hacking. "The FBI and NHTSA are warning the general public and manufacturers -- of vehicles, vehicle components, and aftermarket devices -- to maintain awareness of potential issues and cybersecurity threats related to connected vehicle technologies in modern vehicles," the agencies said in the bulletin. In July 2015, Fiat Chrysler Automobiles NV recalled 1.4 million US vehicles to install software after a magazine report raised concerns about hacking, the first action of its kind for the auto industry. Also last year, General Motors Co issued a security update for a smartphone app that could have allowed a hacker to take control of some functions of a plug-in hybrid electric Chevrolet Volt, like starting the engine and unlocking the doors. In January 2015, BMW AG said it had fixed a security flaw that could have allowed up to 2.2 million vehicles to have doors remotely opened by hackers. "While not all hacking incidents may result in a risk to safety -- such as an attacker taking control of a vehicle -- it is important that consumers take appropriate steps to minimize risk," the FBI bulletin said Thursday. The FBI bulletin Thursday warned that criminals could exploit online vehicle software updates by sending fake "email messages to vehicle owners who are looking to obtain legitimate software updates. Instead, the recipients could be tricked into clicking links to malicious Web sites or opening attachments containing malicious software". (Reuters, 18Mar16)

Incidents of Interest:

(U) Hackers modify water treatment parameters by accident

(U) A group of hackers, previously involved in various hacktivism campaigns, have accidentally made their way into an ICS/SCADA system installed at a water treatment facility and have altered crucial settings that controlled the amount of chemicals used to treat tap water. This strange hacking incident is described in Verizon's 2016 Data Breach Digest (page 38, Scenario 8), a collection of case studies that the company's RISK team was brought in to investigate. The victim of the hack is a company that Verizon identified under the generic name of Kemuri Water Company (KWC). As the RISK team explains, the company noticed that, for a couple of weeks, its water treatment center was behaving erratically, with chemical values being modified out of the blue. Suspecting something was wrong -- and something that its IT staff wasn't able to spot -- the company brought in Verizon's RISK team to investigate. Right from the start, the RISK team identified a series of issues. First off, KWC was using extremely outdated computer systems, some of which were running ten-year-old operating systems. Additionally, the entire IT network revolved around a single equipment, an AS400 system, which would interconnect the company's internal IT network and the SCADA systems that managed the water treatment facility (a big no-no in terms of security). Even worse, the same AS400 was also exposed to the Internet because it was routing traffic to a Web server where KWC's customers could check their monthly water bill, their current water consumption level, and even pay bills via a dedicated payments application. But Verizon was about to get a bigger surprise because the company's investigation also discovered that there was only one KWC employee who could manage the AS400 system, meaning that cyber-intrusions when that employee was off-duty would have gone under the radar and could have easily crippled the company's activity. The RISK team discovered that the hackers first breached the system via the Web-accessible payments application, looking for sensitive information about the company's clients. It appears that the hackers discovered a vulnerability in the payments system, which they used to get access to the Web server, where they also found an INI file that contained administrative credentials, in cleartext, for the AS400 equipment. Curious as they were, the hackers accessed the AS400 system, from where they also ended up on the SCADA system and started modifying parameters at random, unknowingly changing water treatment values. Secondary security measures allowed KWC to detect abnormalities in the levels of released chemicals, and aborted the hackers' instructions, but this happened often enough to arouse suspicions that this had to be more than a glitch. "KWC's alert functionality played a key role in detecting the changed amounts of chemicals and the flow rates. Implementation of a layered defense-in-depth strategy could have detected the attack earlier, limiting its success or preventing it altogether," the security investigation team concluded in their report. After Verizon finished their investigation, the RISK team reassured that there was no malevolence from the hackers' side. They also informed the water treatment company that the hackers had access to over 2.5 million customer personal and financial records and provided technical expertise on how KWC could fix their IT system to prevent similar incidents. (Softpedia 22Mar16)

OGA

(U) US charges three Syrian hackers

(U) US authorities have charged three Syrian nationals who are current or former members of the Syrian Electronic Army with multiple conspiracies related to computer hacking, the US Justice Department said on Tuesday. Ahmad Umar Agha, 22, and Firas Dardar, 27, were charged with a criminal conspiracy that included "a hoax regarding a terrorist attack" and "attempting to cause mutiny of the US armed forces," the department said in a statement. Dardar and Peter Romar, 36, were separately charged with other conspiracies, it said. The FBI announced on Tuesday it was adding Agha and Dardar to its Cyber Most Wanted list and offering a reward of $100,000 for information leading to their arrest, the statement said. Agha and Dardar, who are believed to reside in Syria, began their criminal activities in or around 2011 under the name of the Syrian Electronic Army in support of the Syrian government, the statement said. (Reuters 22Mar16)

(U) Five major hospital hacks: horror stories from the cybersecurity frontlines

(U) John Halamka, CIO of Boston hospital Beth Israel Deaconess was speaking on a panel about medical hacking at SXSW Interactive with Kevin Fu, a University of Michigan engineering professor who studies medical device security. Here we bring you the top five major hospital hacks from recent years: 1. Many computers and medical devices in hospitals run ancient operating systems full of security holes, so hospitals don't connect them to their networks or to the Internet. Beth Israel Deaconess had taken this sensible precaution with a computer storing medical records, and everything was fine until it needed a firmware update. The manufacturer sent a technician to do the job. That technician promptly connected the device to the Internet to download the update, then went to lunch. By the time the technician returned, the machine was so packed with malware that it was no longer functional. Someone had also downloaded about 2000 patient X-rays to a computer somewhere in China. Halamka learned some Chinese nationals can't get visas to leave the country because they have infectious lung diseases such as tuberculosis, making a clean lung X-ray valuable. 2. In 2014, Boston Children's Hospital was grappling with a case regarding a teenage girl who'd been taken into state custody; doctors there claimed her ailment was largely psychological and that her parents were pushing for unnecessary treatments. Someone in Anonymous viewed this as an infringement on the girl's rights, and decided to punish the hospital with a DDoS attack. But Anonymous's attack was broader than intended: "They didn't know the IP range of Children's, so they put a DDoS against the entire subnet, which included Harvard University and all of its hospitals." 3. The fake website was nearly perfect and looked almost exactly like the Mass General Hospital's payroll portal -- only the URL was a little different. When doctors received an email instructing them to go to their payroll site to authorize a bonus payment, many of them followed the link and entered their credentials without noticing anything wrong. The hackers who created the facsimile site then used these credentials to change the doctors' direct deposit information in the actual payment system -- and promptly used the doctors' hard-earned cash to buy Amazon gift cards. MGH no longer allows remote access to the payroll site using only a password. 4. A nurse at Beth Israel Deaconess was just looking for a little harmless fun and downloaded Angry Birds to her Android phone. Unfortunately, she downloaded it from a Bulgarian website that delivered malware along with the game. When she logged into her work email account from her phone, a screen scraper program recorded her login credentials. Her account was used to send 1 million spam messages from Harvard.edu, causing Verizon to block Harvard as a spammer. 5. Fu sees ransomware attacks on hospitals as a growing threat. These hackers target private citizens and major organizations. When they go after hospitals, the outages have major repercussions. Fu lists a number of hospitals that have suffered ransomware attacks just in the last few months. In Australia, Royal Melbourne Hospital reportedly paid $17,000 to get its data back after an attack. And in Los Angeles, a Hollywood hospital's network was out for a week when hackers demanded $3.7 million. Hospitals have not made cybersecurity a priority in their budgets, Halamka says: "In healthcare, we spent about 2 percent on IT, and security might be 10 percent of that." Compare that percentage to the security spending by financial firms: "Fidelity spends 35 percent of its budget on IT," he says. -- spectrum.ieee.org. (IDC News Service, 21Mar16)

OGA

OGA

Items of Interest

(U) Nuix helps investigators progress beyond keywords with powerful analytics
(U) Global technology company Nuix announced three upgrades for its investigation product line. These new releases will add new functionality for cybersecurity incident response and data visualizations that help investigators find key facts quickly without relying on keyword searches. They will further enhance Nuix's renowned capabilities for handling the largest volumes and greatest variety of digital evidence. Nuix is releasing three upgraded products in the first half of 2016: [1] Nuix Investigation & Response is a major enhancement to Nuix Investigator Workstation, combining all the functionality of the company's core investigative product with advanced visual analytics and innovative features for cybersecurity incident response. The Nuix Context interface automatically extracts and groups the most important forensic artifacts and gives investigators new ways to slice and dice evidence to get better results, faster. [2] Nuix continues to drive greater speed and scale by offering Elasticsearch as alternative alongside our traditional database structure. This new option in Nuix 7 will make it possible for investigators to search and correlate across even larger volumes of Nuix case files simultaneously. [3] A new user interface for Nuix Web Review & Analytics, as well as further improvements to security controls and a taxonomy system to help automate common workflows. Nuix 7, Nuix Investigation & Response, and the upgraded Nuix Web Review & Analytics will be available in April 2016. The results of Nuix's forensic investigator survey will also be published in April. (PRNewswire, 23Mar16)

(U) DOT is building a cloud sandbox
(U) The Department of Transportation is building an innovation sandbox in its cloud environments to give staff a secure and controlled computing space for short-term data analysis experiments. The sandbox, expected to launch in April, is being built using isolated environments in DOT's Microsoft Azure and Amazon Web Services clouds. Both platforms boast marketplaces offering a variety of free tools with which DOT users can experiment, providing easy access to new technologies, some cutting edge, beta or worthy of review but not yet supported under DOT's enterprise solution or architecture. Ultimately, the sandbox will allow DOT employees with an idea to submit a data-driven hypothesis through a templated form and, once approved, test it over four weeks. The project will be tracked with the Trello collaboration tool, annotating the owner, status, simple notes and lessons learned. "Tracking experiments eliminates duplication and reinforces collaboration and information sharing," Transportation CTO Maria Roat told GCN. The experiments will have no real parameters aside from time limits and metrics or criteria that prove or disprove the hypothesis. Once completed, an experiment can be evaluated to determine whether it warrants a full pilot project or development for production. Roat is also integrating the sandbox with DOT's Idea Hub, the online environment where employees can solicit, post information or ideas. Using the Idea Hub to promote the sandbox can help generate more data-driven projects and connect staff with those who may have more technical skills, she said. (Government Computer News, 23Mar16)

(U) Xorist ransomware family is now decryptable for free
(U) Good news for some ransomware victims, as the security researchers working with the Bleeping Computer crew have managed to find a loophole that they can exploit to decrypt files locked by the Xorist ransomware family. Xorist is a relatively new ransomware variant that was first spotted at the start of the year. Technically, it is a very simple ransomware, less intrusive than Locky, TeslaCrypt or CryptoLocker. What's unique about this threat is the fact that the coder behind it is selling it as an automatic executable builder which allows anyone to generate their own custom version of the ransomware. Those who buy the builder can customize many of Xorist's features, and more importantly the encrypted file extension. The encrypted file extension is the extra extension added at the end of each file after the ransomware locks it. For Locky, the encrypted file extension is ".locky" which makes it easy to detect. The Xorist builder, sold to anyone that wants to enter a life of cyber-crime, allows the crook to customize this file extension at will, along with many more other options. The encrypted file extension is important because users and tech support experts google the term to find out what the ransomware's name is. Xorist can use the TEA (Tiny Encryption Algorithm) or the XOR algorithm to encrypt files, and targets 57 file types by default. Some of the encrypted file extensions seen with Xorist infections these days are .EnCiPhErEd.73i87A, .p5tkjw, and .PoAr2w, but as mentioned above, all these settings can be tweaked via the builder, and there may be more other people affected by this threat. The good news is that Fabian Wosar of Emsisoft has managed to find an encryption flaw for Xorist. The bad news is that this is not a general fix-all solution, and users will have to get in contact with him personally. (Softpedia, 22Mar16)

(U) White House Says Agencies Reported 77,200 Cyber Incidents in 2015

(U) The annual performance review for agency information security is in and, while it does not mention there were big breaches this year, the scores reflect an executive branch in need of a significant IT tune-up. During fiscal 2015, federal departments collectively reported 77,183 cybersecurity incidents, a 10 percent uptick from the number reported the previous year. "The increasing number and impact of these incidents demonstrate that continuously confronting cyberthreats must remain a strategic priority," according to a 18 March report on compliance with agency information security laws. At the Pentagon, the number of reported "social engineering" incidents aimed at tricking personnel into revealing information rose from 182 to 290. The military scored 15 percent on its "anti-phishing" protections against emails and websites that solicit sensitive information. Not said: In July, attackers duped Joint Staff personnel into opening emails that helped a suspected nation state penetrate a Defense Department unclassified network. An overall rise in the number of incidents reported governmentwide over the past three years is partly thanks to agencies enhancing their detection tools and techniques, the White House report states. But cybersecurity awareness is still a sore point, in general. Most major federal agencies -- 21 out of 24 -- earned a two or lower on a five-point scale for the maturity of their real-time "continuous monitoring" of security controls, "which would not be considered effective," an associated audit by department inspectors general found. Another thing left unspoken: The Office of Personnel Management learned last summer that outdated IT and a stolen password facilitated a 2013 attack that had affected 21.5 million people by spring 2015. Federal departments received a D average, or 68 percent, on their ability to detect unauthorized software and prevent it from executing, according to the report. The departments of Defense, Treasury, Energy and State are among the 14 agencies that could not see unauthorized devices on their unclassified networks at the target rate. But it was people, not hardware, who tricked Treasury's IRS.gov identity verification system to access financial information on 700,000 taxpayers. [This incident also was not in the review.] The report highlights a new initiative unveiled in President Barack Obama's 2017 budget, called the Cybersecurity National Action Plan, which requires agencies undertake a number of steps to boost digital security across the government and private sector. The actions "build upon unprecedented progress to strengthen federal cybersecurity that took place in fiscal year 2015 due to the efforts of the Office of Management and Budget, the Department of Homeland Security and other federal agencies," the White House says. It is unclear if agencies would have achieved such progress were it not for the OPM hack. In June, the same month the intrusion was disclosed, OMB launched a 30-day "cyber sprint." The report states, "Agencies immediately took steps to further protect federal information and assets and improve the resilience of federal networks." Civilian agencies followed through on a 2004 mandate that required the use of smartcards for accessing federal networks. Smartcard use increased from 42 percent governmentwide to 72 percent during the emergency fix-it session. As of 16 November 2015, about 81 percent of federal computer users were using cards to log in. Aside from requiring smartcards for network access, agencies were instructed to patch "critical vulnerabilities," which they did by December 2015, reducing 99 percent of the 363 security holes present before the sprint. (NextGov, 21Mar16)

OGA

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424