Cyber-Threat Newsletter – 06 Jun 16

Threats & Vulnerabilities of the Week:

(U) No hacking required: Israeli researchers show how to steal data through PC components

(U) A team of computer science researchers from the Israel Institute of Technology (a.k.a the Technion) developed a series of side-channel-attacks that can steal encryption keys by monitoring acoustic, electric, and electromagnetic signals generated by a PC. Researchers claimed to have carried out the attacks on several public-key encryption schemes and digital-signature schemes using inexpensive and readily available equipment, according to a research paper contributed to the Association for Computing Machinery, a professional association. The attacks are unlikely and difficult to pull off, but possible said industry experts. In one attack, researchers were able to steal encryption keys by monitoring the acoustics of the "coil whine" or vibrations caused by electronic components inside a PC fluctuating as voltages and currents pass through. The coil whines leak keys during cryptographic operations because the noise is correlated with the ongoing computation about what applications are running and what data is being processed, according to the paper. "By recording such noise while a target is using the RSA algorithm to decrypt ciphertexts (sent to it by the attacker), the RSA secret key can be extracted within one hour for a high-grade 4,096-bit RSA key," researchers said in the paper. The attack can be carried out from as far as 10 meters away using a parabolic microphone or from 30cm away through a plain mobile phone placed next to the computer. In another attack, researchers were able to steal RSA and ElGamal keys after measuring how the electric potential energy of a laptop's chassis fluctuates. This can be done directly through a plain wire connected to a conductive part of the laptop, or indirectly through any cable with a conductive shield attached to a port on the laptop, researchers said in the post. An attacker could also steal RSA and ElGamal keys by monitoring the electromagnetic field radiated by the computer using a suitable electromagnetic probe antenna or even a plain consumer-grade AM radio receiver, researchers said. In order to defend against these attacks, hardware counter measures can be taken, such as, the use of sound-absorbing enclosures to protect against the acoustic attacks, Faraday cages against electromagnetic attacks, and insulating enclosures against chassis and touch attacks. However, researchers admitted that these countermeasures are expensive and cumbersome. Software countermeasures include the use of algorithms and other software implementations that are designed so that leakage through the given channel will not convey useful information, researchers said. "Unlike average cybercrime campaigns and hacks, these attacks simply don't scale and aren't worth the attacker's investment," he said. Nunnikhoven did say the attacks could be worth investment for an attacker targeting governments and sensitive industries and that these entities should invest in counter measures such as cable isolation, physically securing systems in data centers. (scmagazine.com, 01Jun16)

(U) Upgraded Dridex malware on the rebound, hitting US banks

(U) A new and more dangerous version of the Dridex banking malware is being used in a new campaign targeting financial institutions, primarily in the United States. After having rently lost its status as a favored attack vector, Dridex has popped back onto the mainstage, Trend Micro researchers Michael Casayuran, Rhena Inocencio and Jay Yaneza wrote in a recent report. A spike in Dridex spam emails was spotted in May, but this new iteration eschewed the old tactic of using fake invoices or notifications to scam the victim and instead attempted to scare the recipients into opening the email and clicking on the infected attachment. "The email message bears the subject heading Account Compromised and contains details of the supposedly logon attempt, including the IP address to make it look legitimate. The spammed message is almost believable except for one missing crucial detail: It doesn't have any information on what type of account (email, bank, social media accounts etc.) is compromised," the researchers wrote. The majority of the attacks (59.7 percent) spotted thus far were against U.S.-based targets with those in Brazil and China a distant second and third, Trend Micro reported. Another major alteration is that Dridex is now paired with the command-line program Certuli, which allows the malware to pass itself off as a legitimate certificate. "As such, this poses challenges in detecting and mitigating DRIDEX," Trend Micro said. "Prior to this new wave, the use of macros enables the threat to bypass sandbox technologies. This clearly indicates that DRIDEX is leveling up its ante to remain a prevalent online banking threat." All of the changes added together have helped make Dridex once again a formidable opponent as a banking threat. Being that the new Dridex has just hit the web Trend Micro is still unsure whether it is more effective than the previous incarnation. Christopher Budd, global threat communications manager, told SCMagazine.com in an email, "It's a new tactic and it will work with some people more than others. In reality, the only ones that can answer that question exactly are the attackers". (scmagazine.com 01Jun16)

(U) Windows zero-day affecting all OS versions on sale for $90,000

(U) A hacker going by the handle BuggiCorp is selling a zero-day vulnerability affecting all Windows OS versions and that can allow an attacker to elevate privileges for software processes to the highest level available in Windows, known as SYSTEM. Security firm Trustawave discovered the bug this past May, advertised on a Russian underground hacking forum for $90,000. The forum post's latest update was on 23 May, and the initial price was of $95,000. BuggiCorp also posted two YouTube videos of the zero-day in action, one escalating the privileges of an application in Window 10 with the latest May 2016 security patch installed, and another video showing his exploit bypass all security features included in Microsoft's newest version of the EMET toolkit. The crook wants payment in Bitcoin and is willing to provide escrow via the forum's administrator if needed. BuggiCorp says he'll sell the exploit to only one person, and that the buyer will get the exploit's source code, a fully functional demo, the Microsoft Visual Studi0 2005 project file, and free future updates for any Windows version the exploit may fail to run on. The seller wanted to be very clear that his exploit works on all Windows versions, which, according to Microsoft's statistics, may affect over 1.5 billion users. Trustwave and other infosec experts think the zero-day is overpriced, but they believe someone will eventually pay it. (Softpedia 31May16)

(U) Microsoft warns of ZCryptor ransomware with self-propagation features

(U) Microsoft has released an alert today warning about a new ransomware variant called ZCryptor, which comes with the ability to self-propagate via removable and network drives. A security researcher named Jack, behind the MalwareForMe blog, first discovered and wrote about this threat on 24 May. Three days later, Microsoft 's security team also took note of the new wave of infections. "We are alerting Windows users of a new type of ransomware that exhibits worm-like behavior," Microsoft's Malware Protection Center alert reads. "This ransom leverages removable and network drives to propagate itself and affect more users." The company says that crooks use fake installers, usually for Adobe Flash, along with macro-based booby-trapped Office files to distribute the Zcryptor ransomware. Once the user installs the fake Adobe Flash update or allows an Office file to run macros, the Zcryptor ransomware is installed on the user's computer. The first thing the ransomware does is to gain PC restart persistence by adding a key to the computer's registry. After this, it starts to encrypt files. The most peculiar thing, the one that caught our attention, was Microsoft saying the ransomware has "worm-like behavior," meaning it can spread by itself to nearby targets. Such behavior is novel for ransomware families, and it appears that this is one of the first ransomware variants to feature such a function. MalwareHunterTeam also said "that it [ZCryptor] has the codes to copy itself to removable devices." A subsequent analysis by Trend Micro, also released today, has reinforced Microsoft's findings, categorizing the threat as a "worm," with self-propagation features. (Softpedia 27May16)

(U) Knock Knock! Unique new backdoor Trojan infecting computers

(U) Backdoors normally implement remote control tool TeamViewer in order to get unauthorized access to an infected computer. However, a newly-discovered Trojan, BackDoor.TeamViewer.49, uses the tool for less obvious reasons. Doctor Web specialists detected the new Trojan being covertly installed on computers by another malicious application called Trojan.MulDrop6.39210, a fake update of Adobe Flash Player. The executable file installs the player on Windows, saves it on the disk without the user's knowledge, runs them every three seconds and removes the original Flash Player file. During installation, a legitimate installer window of Flash Player is displayed on the screen. BackDoor.TeamViewer.49 uses different internal functions of the program's process. Once TeamViewer is launched, the Trojan removes its icon from the Windows notification area and disables error reporting and implements a special mechanism meant to prevent it from being restarted on an infected computer. "BackDoor.TeamViewer.49 registers itself in autorun and then, operating in infinite loop but with specified time intervals, assigns the folder, which contains its executable file, the malicious library and the configuration file, with the "hidden" and "system" attributes. If it fails to assign these attributes, the Trojan starts removing all the TeamViewer keys from the system registry," said Doctor Web researchers. Another encrypted library is also hard-coded in the body of the Trojan and responsible for performing malicious activity such as establishing connection and authorization to the server and redirecting traffic from the server to the specific remote server through the infected computer, allowing cyber-criminals to remain anonymous on the internet. Doctor Web anti-virus detects and removes the malicious applications. (scmagazine.com 27May16)

(U) ICS-CERT warns about vulnerable SCADA system that can't be updated

(U) A web-based SCADA system deployed mainly in the US energy sector sports vulnerabilities that may allow attackers to perform configuration changes and administrative operations remotely. What's worse is that these holes can't be plugged because the device has nowhere to put an update. "Independent researcher Maxim Rupp has identified data controller vulnerabilities in the Environmental Systems Corporation (ESC) 8832 Data Controller," ICS-CERT has noted in an advisory published on Thursday. "ESC acknowledged that Balazs Makany reported these vulnerabilities on 18 February 2015. ESC has stated the ESC 8832 Data Controller has no available code space to make any additional security patches; so, a firmware update is not possible." The data controllers are used for automation and monitoring in various environments. The two vulnerabilities are present in ESC 8832 Version 3.02 and earlier. Exploiting one allows for the bypassing of the authentication process for configuration changes, and exploiting the other allows an attacker to gain access to functions which are not displayed in the menu. There is currently no indication that vulnerable systems are being attacked, but as detailed vulnerability information is publicly available, it could be just a matter of time until some of them are. ICS-CERT judges that low-skilled attackers would be able to exploit them. According to the manufacturer's website, the 8832s are no longer manufactured or sold by them (they stopped in 2013). "Though we will not be manufacturing new 8832s, ESC will continue to support the 8832 in future versions of our StackVision software until 1 January 2019. We will also continue to repair and service existing 8832 Data Controllers for as long as we can reasonably continue to get repair parts," they state. Environmental Systems advises organizations -- and has been advising them for a while -- to ditch these controllers altogether and upgrade to newer products (their 8864 data controller, for example). If that's not possible, they advise blocking Port 80 with a firewall in front of the device, and educating operators and users to not use the web interface for device management. (helpnetsecurity.com 27May16)

(U) New Locky ransomware campaign sets sights on Amazon customers

(U) Amazon customers are the target of a wide-ranging phishing email scam intended to fool recipients into opening up a malicious attachment that results in the downloading of Locky ransomware. Comodo Threat Research Labs detected the attack earlier this week, according to an article in Comodo's new Defend magazine. The seemingly benign email arrives with the sender email address auto-shipping@amazon.com, and the subject line: "Your Amazon.com order has dispatched," along with an order code. The body is empty, but it's the attachment users have to look out for. The attachment is a Word document containing malicious macro codes, which if enabled execute downloading of the Locky payload. Recipients are prompted upon opening the document to change Microsoft's settings to enable these macros -- a tactic that has had a recent resurgence in popularity among cybercriminals. (scmagazine.com 27May16)

OGA

(U) Research finds critical out-of-the-box vulnerabilities on big name laptops

(U) When you buy a new PC it inevitably comes with a range of extra software -- bloatware if you will -ranging from the maker's own updater tools to trials of antivirus and other products. Trusted access provider Duo Security has carried out some research into how this extra software could be making users more vulnerable and invading their privacy. It tested a total of 10 new laptops from Acer, Asus, Dell, HP and Lenovo and found that all the vendors had at least one vulnerability that allowed for a complete compromise of the affected machine. Most of the vulnerabilities found in the study needed little sophistication or effort and little to no cost to exploit. This is particularly significant for companies with BYOD policies whose employees are using their laptops with default settings, in the workplace. The vulnerable devices can open an entire organization up to an attack resulting in a data breach. The Duo team reported the vulnerabilities to all five vendors at least 90 days ago. At the time of writing, HP has responded and fixed the high risk vulnerabilities. Acer and Asus have responded, but have not yet released their fix timetables. Lenovo has removed the vulnerable software from its systems, effectively making those machines no longer vulnerable. More detail on the vulnerabilities can be found on the Duo blog along with a link to download the full report. (BetaNews, 18May16)

Incidents of Interest:

OGA

(U) Malware attack shutters University of Calgary

(U) Network Computer systems at the University of Calgary were partially operational on Monday following a virus attack that knocked its network offline over the weekend, according to Global News. Students and staff received the following warning on Saturday: "Do not use any UCalgary-issued computers for any purpose." A malware attack was believed responsible for disabling IT services, including email, Skype VPN, secure wireless and Active Directory. One professor, commenting on video, believed because most systems affected were Microsoft-based, the malicious software targeted Windows systems or an exploitable flaw in Windows. It will be a few days before systems are fully operational, the university stated, and an investigation has been launched to determine who hacked in and why. By yesterday, the university's AirUC secure wireless and Office 365 email were functioning and officials informed students and staff that it was again safe to use university-issued computers to access networks and applications. (scmagazine.com 31May16)

(U) 65 million Tumblr users' email addresses, passwords sold on dark web

(U) Email addresses and hashed and salted passwords of 65 million Tumblr users are being sold online by "peace_of_mind," aka "Peace", the individual that recently offered for sale LinkedIn users' data dating back to a 2012 breach. The account credentials stolen from Tumblr are also old -- according to researcher Troy Hunt, they were stolen in the site's February 2013 breach. Tumblr warned about it earlier this month, but neglected to tell how many users are affected. "We recently learned that a third party had obtained access to a set of Tumblr user email addresses with salted and hashed passwords from early 2013, prior to the acquisition of Tumblr by Yahoo. As soon as we became aware of this, our security team thoroughly investigated the matter. Our analysis gives us no reason to believe that this information was used to access Tumblr accounts. As a precaution, however, we will be requiring affected Tumblr users to set a new password," they said. Peace is selling the lot for less than half a bitcoin (around $150), so it seems that the passwords are relatively safe from cracking but, as many have pointed out, a list of emails of 65 million Tumblr users can come in handy for mounting phishing attacks -- something that the Tumblr team failed to warn about. Hunt notes that all of these breaches (including the MySpace one announced recently) date back a few years. "There's been some catalyst that has brought these breaches to light and to see them all fit this mould and appear in such a short period of time, I can't help but wonder if they're perhaps related. One explanation may be related to the presence of these breaches being listed for sale on the dark market," he mused. "These 3 are all listed by peace_of_mind and by all accounts, this individual is peddling a quality product. Apparently, buyers are happy. Now this is not to say that peace is the guy who's hacking into these sites and indeed attribution can be hard, particularly after so much time has passed by since the sites were actually attacked. But certainly there's a trend here which is hard to ignore." Time will tell if there will be other similar revelations. In the meantime, you can check via the Have I been pwned? service whether these latest data offered for sale contains your email address and password. (helpnetsecurity.com 31May16)

Items of Interest

(U) NATO likely to designate cyber as operational domain of war

(U) NATO members will likely agree during a summit meeting in Warsaw next month to designate cyber as an official operational domain of warfare, along with air, sea, land and space, a senior German defense ministry official said Wednesday. Major General Ludwig Leinhos, who heads the German military's effort to build up a separate cyber command, told a conference at the Berlin air show that he expected all 28 NATO members to agree to the change during the coming Warsaw summit. Leinhos, who previously held a senior job at NATO headquarters, said he also expected NATO members to agree to intensify their efforts in the cyber security arena. (Reuters 01Jun16)

(U) Russia calls for routine cybersecurity meetings with US

(U) Russia is calling for regular cybersecurity meetings with the United States, including on the military level, Special Representative of the President of the Russian Federation for International Cooperation in Information Security Andrei Krutskikh said. At bilateral consultations held on 21 April to 22 April in Geneva, high-ranking Russian and US officials agreed to boost practical cooperation in the fight against cyberthreats. "In what concerns the Russian side, we have long advocated for such meetings to be regular. For them becoming routine. And we are talking about meetings at all levels -- high political (like it was in Geneva), expert, and on the level of individual departments. In addition, we need to have the militaries talk to each other," Krutskikh said in an interview with the Russian Kommersant newspaper. Moscow and Washington discussed improving information exchanges via channels of communication in line with 17 June 2013, joint statement on cooperation to counter terrorism. (Sputnik 27May16)

(U) NDAA amendment would elevate Cyber Command to Combatant Command

(U) An amendment to the National Defense Authorization Act (NDAA) introduced by a bipartisan group of senators Thursday would compel President Obama to raise Cyber Command to a Combatant Command. "With the advice and assistance of the Chairman of the Joint Chiefs of Staff, the President, through the Secretary of Defense, shall establish under section 161 of this title a unified combatant command for cyber operations forces," the amendment reads. "The principal function of the command is to prepare cyber operations forces to carry out assigned missions." Calling cyber attacks a growing threat to national security," Sen. Richard Blumenthal (D-Conn.) said in a press release announcing the amendment, "Elevating CYBERCOM to a Combatant Command will enhance its ability to protect Americans from cyber threats." Senators Barbara Mikulski (D-Md.), Steve Daines (R-Mon.), Michael Bennet (D-Colo.), Ben Cardin (D-Md.), Mark Warner (D-Va.) and Joni Ernst (R-IA) joined Blumenthal in supporting the amendment. (scmagazine.com 27May16)

(U) Pentagon is building massive hub of insider threat data

(U) The Defense Department is building a massive information-sharing system detailing national security personnel and individuals cleared for accessing US secrets, to flag who might be potential turncoats or other "insider threats." The "DOD Component Insider Threat Records System" is part of the US government response to the 2010 leaks of classified diplomatic cables by former Pfc. Chelsea Manning. A 2011 so-called WikiLeaks executive order called for an "insider threat detection" program. A review of the 2013 Washington Navy Yard shootings found the department still lacked "a centralized hub" to obtain a holistic view into potential threats, Defense spokeswoman Linda Rojas told Nextgov in an email. Now the Pentagon is establishing a team of "cross-functional experts" -- aided by the new workflow technology -- to help fill that gap, she said. The Pentagon expects to enter information gleaned, in part, from a new "continuous evaluation" approach to screening clearance-holders that uses automated data checks, according to a 19 May Privacy Act notice. The system also will share data from public social media posts and "user activity monitoring" of employees' private digital habits at work. Surveillance of military networks may include keystrokes, screen captures, and content transmitted via email, chat, and data import or export. Director of National Intelligence James Clapper signed a policy that would authorize investigators to vet public social media posts when conducting background checks of national security personnel. In the privacy notice, Aaron, alternate defense Federal Register liaison officer, describes user activity monitoring as the technical capability to "record the actions and activities of all users, at any time, on a computer network controlled by DOD." The technology would disseminate equal employment opportunity complaints, security violations and personal contact records. Logs of printer, copier and fax machine use would be shared. Public information from professional certifications would be fair game too. According to the privacy notice, the system will be governed under the following definition of "insider threat:" The threat that an insider will use his or her access, wittingly or unwittingly, to do harm to the security of the United States. This threat includes damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of government, company, contract or program information, resources, or capabilities. German said personnel who ruffle the feathers of managers while trying to root out government abuses could be tracked. If national security personnel know their criticisms will be widely circulated, they might shy away from reporting problems, German said. Defense officials said only military-affiliated personnel falling under certain criteria will be entered. Only personnel trained in insider threat, privacy and civil liberties, and intelligence oversight, who are approved by the department, will be allowed to use the system, Rojas said. The system will not be activated until after a public comment period ending 20 June. (NextGov 27May16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424