Cyber-Threat Newsletter – 31 Oct 16

Threats & Vulnerabilities of the Week:

(U) Pentagon warns military against using Chinese computers

(U) The Pentagon has warned that computer hardware developed by Chinese company Lenovo may be used to spy on the Pentagon -- an intelligence strategy that the US is no stranger to. An internal probe produced by the Pentagon's Joint Staff (J2) claimed that products featuring components from Chinese manufacturing giant Lenovo pose a cybersecurity risk to the Pentagon and US defense contractors. "There is no way that that company or any Chinese company should be doing business in the United States after all the recent hacking incidents," one official, speaking on condition of anonymity, told the Washington Free Beacon. In April, Air Force Cyber Command issued a similar warning, saying that "Lenovo products are being removed from the Approved Products List and should not be purchased for DoD use. "Lenovo products currently in use will be removed from the network". Others have attempted to downplay the report. A Pentagon spokesperson said that the US Defense Department has no interest in a blanket ban on the company, and stressed that cybersecurity "requires the department to perform supply chain risk management functions when acquiring products for us in its national security systems". This is done on a case-by-case basis, the Pentagon spokesperson added. Ray Gorman, a spokesman for Lenovo, has dismissed the allegations. "We have stated many times that we continue to look worldwide for opportunities that make sense for our customers and shareholders, add value to our product portfolio, and help keep us on track for continued profitable growth," he said. (Sputnik 25Oct16)

(U) Researchers find weakness in common computer chip

(U) Researchers from Binghamton University -- State University of New York and the University of California, Riverside have found a weakness in the Haswell central processing unit (CPU) components that makes common computer operating systems vulnerable to malicious attacks. Computer hackers could take control of individual, company and government computers if a weak point in address space layout randomization (ASLR) software is exploited by manipulating a CPU's branch predictor, a piece of hardware designed to improve program performance. Before anyone worries too much, researchers suggested several methods to mitigate the attacks they identified in the paper "Jump over ASLR: Attacking the Branch Predictor to Bypass ASLR," and companies have already started to work on the issues raised. Researchers demonstrated the weakness in commonly-used Linux operating systems using Intel processors. However, the team led by Binghamton PhD candidate Dmitry Evtyushkin, Ponomarev and former Binghamton Computer Science Professor Nael Abu-Ghazaleh think the vulnerability could also apply to other operating systems such as Windows and Android. According to the work, the attack may also be practical on virtualization systems such as Kernel-based Virtual Machines (KVM), which are used in cloud computing systems. ASLR software automatically randomizes information in a computer's memory which protects a machine during crashes and defends against a wide range of malware. The team identified a way to disable and bypass ASLR by attacking the branch predictor hardware. With the ASLR down, a hacker can then perform "buffer overflow" and "code reuse" attacks to gain administrator or "root" level privileges to steal sensitive data. However, another exploitable vulnerability in software is needed to perform a buffer overflow attack. (Binghamton University 25Oct16)

(U) Millennial behavior puts federal IT systems at risk

(U) The security habits of the millennial generation could be putting federal IT systems at risk, if agencies don't adjust their cyber defenses in time. This finding comes from a new study by cyber security company Forcepoint, which examines how members of the millennial generation use technology. Millennials currently make up about 25 percent of federal employees and are expected to represent nearly 75 percent of the workforce by 2025. But while baby boomers are more cautious online, the survey data shows that millennials (those born between 1977 and 1994) are more likely to abandon caution for digital expediency. Federal organizations face millennial workers who believe they are sufficiently educated and confident in security knowledge. Yet the survey's data reveals many do not practice safe behaviors when it comes to technology and the workplace. Millennials acknowledge they use personal devices for both work and play, with nearly a quarter downloading company files and third party apps to personal devices to increase productivity without notifying IT. In addition, while millennials claim to understand and use strong passwords, the results show they frequently use the same passwords for multiple systems and apps and share them with others even after having personally experienced a breach. Forcepoint also surveyed federal IT security officers on how they are adapting their efforts. Current changes primarily relate to flexible scheduling and accessing information on mobile devices. Changes being made on an agency by agency basis include security awareness programs that emphasize secure productivity, and updating BYOD programs with tools allowing for greater visibility by monitoring applications' reach and data flows. The full report is available from the Forcepoint website. (BetaNews 25Oct16)

(U) Researcher finds easy method to bypass PayPal 2FA

(U) UK security researcher Henry Hoggard has found a very simple method of bypassing PayPal's two-factor authentication (2FA) mechanism, allowing an attacker to take over PayPal accounts in less than a minute. The researcher claims to have discovered this method while in a hotel with no telephone signal, and no way to receive the 2FA verification code to his device via SMS. The researcher says the problem was found in the "Try another way" link that appears under the 2FA section of the login screen. PayPal provides this option to PayPal account owners for situations when they can't reach their phone, or they have no signal, as this was the case. In these types of situations, PayPal asks the user to answer his security questions. Hoggard discovered that if the attacker had a proxy server running that can intercept and hold the PayPal server requests, it would allow him to tamper with the HTTP data and trick PayPal into granting him access to the account. All the attacker had to do was to remove the "securityQuestion0" and "securityQuestion1" parameters from the HTTP request. The technical skills needed to carry out such attacks are entry level for any hacker wannabe. Hoggard reported the issue to PayPal on 3 October, and engineers had removed the authentication loophole by 21 October. (Softpedia 24Oct16)

(U) Near-death experience: Hicurdismos tech support scam mimics Microsoft Blue Screen of Death

(U) Microsoft on Friday warned of a malware threat called Hicurdismos that simulates the infamous Windows Blue Screen of Death as part of a tech support scam. Delivered via drive-by download, Hicurdismos appears to be an installer for Microsoft Security Essentials, an anti-malware product for machines operating on Windows 7 and earlier operating systems. In reality, it's a SmartInstaller package that, upon activation, triggers the BSoD and a fake error message with a customer support phone number. Victims who call this number are socially engineered into downloading additional malware purporting to be support tools that supposedly fix the problem. To sell the BSoD effect, the malware also hides the mouse cursor and disables the Task Manager. Real error message screens from Microsoft do not provide support phone numbers, the company stated in a blog post; rather, they include an error code and instructions. (scmagazine.com 24Oct16)

(U) New Kovter trojan variant spreading via targeted email campaign

(U) The Kovter malware sample that has infected systems around the world for the past couple of years is proving to be a case study in how threat actors constantly tweak their malware to keep one step ahead of the defenders. Trojan Kovter surfaced about two years ago as a screenlocker and scareware sample masquerading as a law enforcement tool. Since then it has been used in click-fraud and malvertising campaigns, as data-encrypting ransomware, and a malware installation tool. Kovter's authors have used a variety of ways to distribute the malware, to avoid detection, and to gain persistence on infected systems. For instance, Kovter is among the first file-less malware tools that resides only in memory and runs from the system registry rather than the disk to evade detection by file-based malware detection products. It also has been seen masquerading as Firefox and Chrome updates and as a JavaScript downloader. This week, security firm Morphisec reported yet another tweak to the malicious software. Over a period of four days last week, Morphisec said it identified multiple malicious macro-based documents delivering Kovter via targeted emails. "Compared to the previous wave in July-August, where it was delivered as Chrome or Firefox update or as a zip file, this time it came as a macro with click-based activation documents," says Michael Gorelik, vice president of research and development at Morphisec. "It was not enough to enable the macro content, the user needed to also click on the image inside the macro," Gorelik said of a Kovter sample recovered from one of the company's customers. The new approach allows the malware to bypass security sandbox approaches that are based entirely on macro enablement alone. The macro writers also added a restriction password on image edit to prevent the sandbox from automatically mapping the macro procedures to be activated, Gorelik said in a technical analysis of the malware. The modified macro with the click-based execution is not the only feature that's new in the Kovter sample that Morphisec analyzed last week. In the latest attack, the threat actors behind the campaign also used highly targeted emails to try and lure users into interacting with the macro. Examples of the targeting included the threat actors approaching potential victims using their actual names, job titles, and company names, Gorelik says. "Monitoring the latest campaigns, we found the often-used 'invoice/bill' email pattern," he said in the technical analysis of the malware, as with many spear-phishing campaigns, the content in the emails is designed to convey a sense of urgency and threats of dire consequences for failure to act. (Dark Reading 24Oct16)

(U) Malware authors adopting the freemium model spells bad news

(U) Malware authors offering free-to-download versions of their malicious software lower the bar and skills needed to enter the cyber-crime scene. The freemium model has long been around in software development. Since the early days of e-commerce, software developers have figured out that by offering a free but feature-limited version of their apps, they could draw in more sales later on, as users got accustomed to their software package and wanted access to more features. This hasn't been the case with malware, where crooks were only interested in making a quick buck, and have always been offering malware under a commercial license only. But the freemium model is slowly making its way among malware developers, with negative consequences on the rest of us. One such example is the Italian malware developer Viotto, who claims to be a "cybersecurity consultant" and "malware analyst," but is offering tools such as keyloggers, RATs, spambots, and software crypters on his website. Viotto is also the author of a new RAT that launched over the summer called Remcos, which we covered when it came out. Viotto is offering Remcos under a dual freemium and commercial license, a distribution model he also uses for most of the malicious software on his site. One such example is a recent spear-phishing campaign discovered by the team at PhishMe. Experts say that crooks were spreading a keylogger to victims, which at a later analysis proved to be the feature-limited, but still dangerous Viotto Keylogger, developed by the aforementioned "cybersecurity consultant" Viotto. Despite being limited in features, the keylogger was more than enough to carry out cyber-espionage on infected targets. (Softpedia 23Oct16)

(U) Hacking 3D manufacturing systems demonstrated by researchers

(U) Researchers from three universities combined their expertise to demonstrate the first complete sabotage attack on a 3D additive manufacturing (AM) system, illustrating how a cyber attack and malicious manipulation of blueprints can fatally damage production of a device or machine. In their paper titled "Dr0wned," researchers from Ben-Gurion University of the Negev (BGU), the University of South Alabama and Singapore University of Technology and Design detail how to sabotage the quality of a 3D-printed functional part, which leads to the destruction of a device. Their proof-of-concept video shows how the researchers destroyed a $1,000 quadcopter UAV drone by hacking into the computer used to control the 3D printing of replacement propellers. Once they penetrated the computer, the researchers identified the propeller blueprint file and inserted defects undetectable by visual inspection. During flight tests, the sabotaged propeller broke apart during ascent, causing the drone to smash into the ground. More than 100 industries, including aerospace, automotive and defense, employ additive printing processes. According to the Wohlers Report, the AM industry accounted for $5.165 billion of revenue in 2015. Furthermore, 32.5 percent of all AM-generated objects are used as functional parts. "Imagine that an adversary can sabotage functional parts employed in an airplane's jet engines. Such an attack could cost lives, cause economic loss, disrupt industry, and threaten a country's national security," says Prof. Yuval Elovici. Elovici is a member of BGU's Department of Software and Information Systems Engineering, director of the Deutsche Telekom Innovation Labs @ BGU and the BGU Cyber Security Research Center (CSRC). The CSRC is collaboration between the University and Israel's National Cyber Bureau, focused on advanced cyber security topics. "This is the first experimental proof of a complete attack chain initiated by sabotaging the 3D-printed propeller". The collaborative study addresses the dangerous consequences of cyber attacks, and proposes a systematic approach for identifying opportunities and a methodology for assessing the level of difficulty of an attack involving AM. (helpnetsecurity.com 21Oct16)

(U) In a BIND: Third parties distributed outdated, vulnerable ISC Domain Name System software

(U) The Internet Systems Consortium issued a security advisory on Wednesday, warning that some third parties are distributing outdated versions of ISC's Berkeley Internet Name Domain (BIND) software that contain a high-severity vulnerability, which bad actors can use to remotely trigger an assertion failure. ISC described the issue affecting the open-source Domain Name System software as a packet with a malformed options section. "A server vulnerable to this defect can be forced to exit with an assertion failure if it receives a malformed packet," the advisory states. As of May 2013, the flaw was corrected in ISC-distributed versions of the software, but other entities are distributing software packages that include a vulnerable version of BIND that does not include the patch, identified as fix #3548. Users of ISC-distributed BIND software that predate May 2013 are also susceptible to the vulnerability, designated as CVE-2016-2848. BIND is the open-source software component that implements Domain Name System protocols. Versions 9.1.0 through 9.9.4-P2 and 9.9.0 through 9.9.2-P2 are affected. (scmagazine.com 21Oct16)

Incidents of Interest:

OGA

(U) US takes aim at cyber attacks from connected devices as recalls mount

(U) Obama administration officials sought on Monday to reassure the public that it was taking steps to counter new types of cyber attacks such as the one Friday that rendered Twitter, Spotify, Netflix and dozens of other major websites unavailable. The Department of Homeland Security said it had held a conference call with 18 major communication service providers shortly after the attack began and was working to develop a new set of "strategic principles" for securing internet-connected devices. DHS said its National Cybersecurity and Communications Integration Center was working with companies, law enforcement and researchers to cope with attacks made possible by the rapidly expanding number of smart gadgets that make up the "internet of Things. Such devices, including web-connected cameras, appliances and toys, have little in the way of security. More than a million of them have been commandeered by hackers, who can direct them to take down a target site by flooding it with junk traffic. The disruption had subsided by late Friday night in America, and two of the manufacturers whose devices had been hijacked for the attack pledged Monday to try to fix them. But security experts said that many of the devices would never be fixed and that the broader security threat posed by the internet of Things would get worse before it gets better. "If you expect to fix all the internet devices that are out there, force better passwords, install some mechanism for doing updates and add some native security for the operating system, you are going to be working a long time," said Ed Amoroso, founder of TAG Cyber and former chief security officer at AT&T. Instead, Amoroso said he hoped that government officials would focus on recommending better software architecture and that business partners would insist on better standards. (Reuters 25Oct16)

(U) Mirai botnets linked to massive DDoS attacks on Dyn DNS, Flashpoint says

(U) Mirai botnets like the ones recently used in distributed denial of service (DDoS) attacks on a French internet service provider and a well-known security researcher were at least partly responsible for the waves of DDoS attacks against Dyn DNS that took down Twitter, Spotify, Netflix, GitHub, Amazon and Reddit and other websites Friday, according to a Flashpoint blog post. Mirai does its dirty work on Internet of Things (IoT) devices and "Flashpoint has confirmed that at least some of the devices used in the Dyn DNS attacks are DVRs, further matching the technical indicators and tactics, techniques, and procedures (TTPs) associated with previous known Mirai botnet attacks," the post said. Flashpoint noted that while "Mirai botnets were used in 21 October 2016 attack against Dyn, they were separate and distinct botnets from those used to execute the DDoS attacks against "Krebs on Security" and [French Internet provider] OVH". After "Anna_Senpai," the hacker behind the Mirai botnet used to attack Krebs, released the malware's source code online, "copycat hackers have used the malware to created botnets of their own in order to launch DDoS attacks," making it difficult to draw a relationship between Friday's DDoS attacks, which were still ongoing well into the evening, and previous attacks where Mirai botnets were used. Chris Sullivan, general manager of Intelligence/Analytics at Core Security Inc., said "the really frightening part" of the Friday attacks, which he called a "new breed of very high volume DDoS," is not that organizations "will be struggling with these new attacks for some time, but that the underlying weakness which makes them successful can and will be used to unleash more serious attacks that steal credit cards and weapons designs, manipulate processes like the SWIFT global funds transfers, and even destroy physical things the 30,000 PCs at Saudi Aramco". Current defenses don't cut it against attacks that exploit the security shortcomings of devices like baby monitors and thermostats. "IoT devices don't have the memory and processing to be secured properly, so they are easily compromised by adversaries and it's very difficult to detect when that happens," Sullivan said in comments emailed to SCMagazine.com. Justin Fier, director of cyber intelligence and analysis at Darktrace, said that while IoT makes life easier "it's also putting us at risk -- as it's become painfully apparent how easy it is to hack them". In comments emailed to SCMagazine.com, Fier called for "better visibility into new technology and the environment in which it's becoming entrenched" otherwise, "we'll continue seeing a pool of vulnerable devices that can be harnessed for these malicious botnet attacks". (scmagazine.com 21Oct16)

OGA

(U) Chinese hackers targeting US DoD contractor linked to OPM hack

(U) Investigators have traced a series of malware infections on the systems of two European companies back to a Chinese threat actor, with clues linking the attacks to the same group that was behind the Anthem and OPM hacks. The targets of these two attacks are the US subsidiary of a French company that provides energy management services and a European-based drone maker. The French company is of importance because the company builds critical infrastructure for the US Department of Defense (DoD), says ThreatConnect, the cyber-security firm that uncovered the malware infections. According to the security firm's experts, the infection goes back to June 2016, when their experts discovered "HttpBrowser" on the networks of the two aforementioned companies. HttpBrowser is a malware familiy previously associated with Chinese cyber-espionage groups that can log keystrokes and open connections to infected computers, allowing an attacker to send new commands, download other malware, or steal sensitive data. In the past years, HttpBrowser was also discovered in the arsenal of two other Chinese cyber-espionage groups EMISSARY PANDA (aka APT27 and TG-3390) and DYNAMITE PANDA (aka APT18, Wekby, and TG-0416) HttpBrowser is also sometimes referred to as Token Control or the GTalk trojan. ThreatConnect researchers say the instances of the HttpBrowser malware they discovered contains a series of hard-coded domain names (URLs) where the trojan sent stolen data for storage. Researchers say these domains were registered with the same email address (li2384826402@yahoo.com) as domain names used to exfiltrate data during the Anthem and OPM (United States Office of Personnel Management) data breaches. The only thing that didn't add up was the fact that the OPM hack had been attributed to a threat group known as DEEP PANDA. Nevertheless, Chinese cyber-espionage has been widely believed to be state-controlled, so a tool passing from one group to another is not surprising. Researchers believe that China is trying to find ways around the anti-cyber-espionage pact signed with the US, which prohibits the two countries from spying on each other for economical gains. A ThreatConnect spokesperson said the company believes that Chinese hackers are targeting the French company for military espionage, but that the attacks on the drone vendor are purely for economical gain. (Softpedia 20Oct16)

Items of Interest

(U) US Treasury tells banks to provide details on cyber attacks

(U) The US government on Tuesday told banks to include details about cyber attacks when filing mandatory reports on fraud and money laundering, saying that will help battle digital crimes that pose "a significant threat" to the US financial system. The US government has long required banks to submit confidential reports known as suspicious activity reports, or SARs, in fraud cases involving at least $5,000. The Treasury Department's office of Financial Crimes Enforcement Network, or FinCEN, released an advisory that specifies what details banks should include in SARs when there is a cyber element in the case. "The bank should include all available information," FinCEN said in the advisory. That includes describing how the system was breached, IP addresses of computers used by hackers and device identifiers. (Reuters 25Oct16)

(U) CYBERCOM reaches initial operating capability

(U) US Cyber Command's 133 Cyber Mission Force teams reached initial operating capability last week, the command said in a statement Monday. The milestone comes six years after the new command launched and two years before it's scheduled to reach full operating capability. It also comes as the Pentagon and intelligence agencies are considering whether to recommend decoupling Cyber Command from the National Security Agency with which it currently shares a single leader and numerous resources. That idea faces opposition in Congress, including from Senate Armed Services Chairman Sen. John McCain, R-Ariz., and Sen. Deb Fischer, R-Neb., who chairs the Armed Services subcommittee that oversees cyber operations. Initial operating capability means all cyber teams have reached "a threshold level of initial operating capacity and can execute their fundamental mission," according to a Defense Department statement. CYBERCOM is currently staffed at 5,000 troops with a final goal of 6,200 troops, according to the DOD statement. Even full operating capability is often defined as less than 100 percent staffing because of the basic churn of troops in and out of units. About half of Cyber Mission Force teams have already reached full operating capability, DOD said. "One of the reasons DOD has done exceptionally well to rapidly train and build this force is that each branch of the military services has come to the conclusion that cyber is a mission set that requires dedicated expertise over time," CYBERCOM Chief Adm. Michael Rogers said in a statement. "That wasn't always the case, and I have to compliment the services, the services' cyber component leadership and the entire team for all of the extremely hard work to achieve this goal". CYBERCOM draws troops from all four military services with about 30 percent each coming from the Army, Navy and Air Force and 10 percent from the Marines. The group's primary missions include defending DOD networks, defending combatant commands from cyberattacks and defending US critical infrastructure and launching offensive cyber operations when directed by the president. (NextGov 25Oct16)

(U) Google quietly changed its privacy policy, no longer promises to anonymize your personal information when selling ads

(U) For years, researchers have discussed how the "anonymizing" various companies claim to perform on the data they gather is poor and can be easily reversed. Over the last few years, we've seen multiple companies respond to these problems by refusing to continue anonymizing data at all. Verizon kicked things off, but Vizio has gone down this route as well, and now we know Google has -- or, at the very least, has reserved the right to do so. According to an investigation at Pro Publica, Google has quietly changed its privacy policy at some point over the last few months. When Google bought the advertising firm DoubleClick a few years back, it promised to keep all data gathered by DoubleClick sandboxed and isolated from the data it gathered elsewhere and used for other Google services. The company has since changed the wording of its privacy policy. Google has stated it doesn't use the information gleaned from Gmail scanning to target ads to specific people, but it's not clear what this means for its other services. Google tracks a great deal of information and its email keyword scanning is just one business area. Previously, Google's privacy policy contained a hard line of what it would and would not do. Google has replaced that flat guarantee with a weasel-word "depending on your settings" statement that hides behind the word "may." Speaking of those settings, Google does have a "Privacy Checkup" tool that you can use to hide certain data from being tracked or gathered. It's generally well-designed, but for one major example, shown below. This is a perfect example of what's known as a dark pattern. A dark pattern is a pattern designed to trick you into choosing the "right" option, where "right" is defined as "What the company wants you to pick," as opposed to what you actually want. In this case, boxes are checked by default and you uncheck them to hide information. But if you uncheck the box labeled "Don't feature my publicly shared Google+ photos as background images on Google products & services," you're actually giving Google permission to use your name and profile to advertise products. Google flipped the meaning of the checkbox to make it more likely that someone not reading carefully would click the wrong option. But what's really interesting to me is that the word "Don't" is bolded. You bold something you want to draw attention to -- and that's pretty much the opposite of how a dark pattern works. Huge organizations are much less monolithic than they appear from the outside, and I suspect that what we see here is a tale of two opinions, played out in a single checkbox. By reversing what checking the option does, Google made it more likely that you would give it permission to use your personal likeness and data for advertising. By bolding the word "Don't," Google made it more likely that you'd realize what the box did and set the setting appropriately. In any case, Google's decision to stop anonymizing data should be serious, but there's not much chance people will treat it that way. To-date, people have largely been uninterested in the ramifications of giving corporations and governments 24/7 permission to monitor every aspect of their lives, even when it intrudes into private homes or risks chilling freedom of speech. (extremetech.com 24Oct16)

(U) MBRFilter protects computers from MBR malware and ransomware

(U) Cisco's Talos team released today a new free tool called MBRFilter that protects a computer's MBR sector against unauthorized access, which can be useful for safeguarding PCs against MBR-targeting malware, such as the Petya, Satana, or HDDCryptor ransomware. At its core, the tool is nothing more than a driver that changes your MBR into a read-only mode and prevents any application from modifying or writing data to that particular section of your hard drive. The MBR stands for Master Boot Record and is a special section of all hard disk drives. The MBR is located right at the beginning of the HDD's storage space and keeps information on partitions in a component called the MFT, or the Master File Table. The MBR also stores the computer's bootloader, an OS component responsible for booting the current OS. Ransomware such as Petya, or other MBR malware (bootkits), force computers to restart, and during the subsequent reboot process, they write new data to the MBR, adding their own malicious routines. Cisco says MBRFilter blocks these operations, preventing Petya or other malware from tinkering with a computer's boot record. Cisco has open-sourced the MBRFilter source code on GitHub. Pre-compiled MBRFilter driver installers for Windows 32-bit and 64-bit platforms are also available for download. (Softpedia 19Oct16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424