Cyber-Threat Newsletter – 11 Jan 16

Threats & Vulnerabilities of the Week:

(U) Researchers uncover JavaScript-based ransomware-as-service
Malware researchers at the anti-virus company Emisoft have uncovered a new "ransomware" package that encrypts the files of victims and demands payment to restore them. Dubbed Ransom32, the malicious code is different from CryptoWall and many other previous ransomware variants in two key ways: it was coded using JavaScript, and it's being offered to would-be cybercriminals as a paid service. In a blog post, Emisoft Chief Technology Officer Fabian Wosar described the malware and its Tor-based administrative Web interface. Users of the service log in with their Bitcoin wallet addresses; once they're connected, they can configure features of the malware "client" for the service such as the messages displayed to victims during the malware installation and how much to demand in ransom for encryption keys. They can also track the payments already made and how many systems have become infected. Once installed, Ransom32 retrieves a 128-bit AES encryption key from the Tor command and control server and starts encrypting a wide range of user files: It uses counter (CTR) block mode to generate a new key for each file. Each key is then encrypted using a public key from the command and control server and stored as part of the encrypted file. Another novel feature of Ransom32 is a sort of "proof of life" capability that demonstrates to victims that their files can be retrieved. The malware "offers to decrypt a single file to demonstrate that the malware author has the capability to reverse the decryption," Wosar noted. "During this process the malware will send the encrypted AES key from the chosen file to the (command and control) server and gets the decrypted per-file AES key back in return." While Ransom32 is Windows-specific, the use of JavaScript and Node.js means that it could potentially be applied to other operating systems with relatively minor modifications. And as ransomware matures, other "ransom as a service" malware packages are sure to join Ransom32. (ars technical, 05Jan16)

(U) Researchers found a way to break through Comcast's home security system
Home intruders no longer need to come in through the kitchen window. Instead, they can waltz right in through the front door, even when a home is protected by an internet-connected alarm system. A vulnerability in Comcast's Xfinity Home Security System could allow attackers to open protected doors and windows without triggering alarms, researchers with cybersecurity firm Rapid7 wrote in a blog post today. The security bug relates back to the way in which the system's sensors communicate with their home base station. Comcast's system uses the popular ZigBee protocol, but doesn't maintain the proper checks and balances, allowing a given sensor to go minutes or even hours without checking in. The biggest hurdle in exploiting the vulnerability is finding or building a radio jammer, which are illegal under federal law. Attackers can also circumvent alarms with a software-based de-authentication attack on the ZigBee protocol itself, although that method requires more expertise. Attackers would also need to know a house was using the Xfinity system before attempting to break in, a major hurdle in exploiting the finding. To prove his findings, Rapid7 researcher Phil Bosco simulated a radio jamming attack on one of his system's armed window sensors. While jamming the sensor's signal, he opened a monitored window. The sensor said it was armed, but it failed to detect anything out of the ordinary. But perhaps even more worrisome than the active intrusion itself is that the sensor had no memory of it happening and took anywhere from several minutes to three hours to come back online and reestablish communication with its home base. The attack plays off a fundamental vulnerability in wireless devices. Anything that relies on wireless communication can be taken offline by a jamming attack. But Rapid7 was surprised by how poorly the Xfinity system responded in the aftermath of such an attack. Comcast did not immediately respond to a request for comment. US-CERT also pushed out a vulnerability notification today and said it did not know of any practical solutions to the issue. (The Verge, 05Jan16)

(U) Cisco Jabber client flaw exposes users to MitM attacks
Cisco's Jabber client for Windows is plagued by a serious security vulnerability that allows attackers to downgrade STARTTLS settings and force communications to take place via cleartext, exposing a user's private conversations and stealing their login credentials. Security researchers Renaud Dubourguais and Sébastien Dudek from Synacktiv discovered the flaw (CVE-2015-6409), which affects versions 10.6.x, 11.0.x, and 11.1.x of Cisco's Jabber client for Windows, an XMPP client used mainly in larger enterprises. According to a technical write-up the two penned in December, an attacker could carry out a simple MitM (Man-in-the-Middle) attack, placing itself between the client and the server, and using the flaw in the Windows client, they could trick the desktop application into exposing sensitive information. Attackers could theoretically obtain the victim's login and password information, conversations, and file transfers. Besides eavesdropping on conversations, attackers would have also had the capability to alter messages passing through the MitM control point. Cisco patched the issue with the release of the Cisco Jabber client for Windows, version 1.0. For users running the affected versions, there's no patch or workaround available, and to avoid having conversations wiretapped by unknown attackers, they should update right away. (Softpedia, 04Jan16)

(U) Scam IRS emails deliver malware payload
Just in time for tax season in the U.S., scammers are once again using fake emails from the Internal Revenue Service (IRS) to launch attacks. The latest phishing campaign, discovered by researchers at Heimdal Security, claims to inform recipients of a refund notification from the IRS. According to a blog post by the research team at Heimdal Security, the emails deliver a very different kind of payload: an attachment that activates Windows PowerShell to download Kovter and CoreBot. The spam email appears to be sent from the IRS and contains a subject line that reads: "Payment for tax refund # 00 [6 random numbers]" and contains a zip attachment that reads as: Tax_Refund_00654767.zip -> Tax_Refund_00654767.doc.js. "If an unsuspecting user opens the attachment -- and ignores several warnings -- then the code will run on the machine with the privileges of the logged in user," Andra Zaharia wrote on the Heimdal blog. "If you're using your admin account on a daily basis, this may prompt you to reconsider." IRS spam emails are a popular method of attaining information from targets. Fake IRS email campaigns have used varied methods such as including links to web pages that download malware, emails that claim to contain stimulus payment information, and spear phishing emails that targeted corporate executives. (scmagazine.com, 04Jan16)

(U) Drug cartels are hacking US border patrol drones

The US Department of Homeland Security (DHS) and the US Customs and Border Protection (CBP) agency are reporting on incidents where drug traffickers have hacked unmanned air vehicles (UAVs, drones) in order to illegally and secretly cross the US-Mexican border. UAVs have become a common presence in the US military, but they have also spread to other US law enforcement agencies like local police and border patrol. Unlike their military counterparts, which cost millions of dollars, the drones used by other law enforcement agencies are much smaller, due to the smaller budgets allocated to the acquisition of such vehicles. Because of this, various standard drone modules had to be removed. One of them is a module that ensures the drone's security against a certain type of attack: GPS spoofing. GPS spoofing is a trivial cyber-attack, which relies on sending GPS receivers fake GPS data. Each UAV has a GPS receiver, used to receive data from off-orbit satellites and navigate along the border, watching for illegal crossers. Drug traffickers have quickly figured this out, and using GPS spoofing techniques are sending UAVs wrong coordinates, made to look like coming from an authentic source. The drone, receiving wrong coordinates, corrects course and leaves its normal patrol area, going to the section it thinks it should be at, based on the wrong coordinates. Once the drone leaves the area of the GPS jammer&spoofing device, it then tries to correct again, going back to its proper patrol area. It follows this back and forwards process until it remains out of fuel and returns to base, or the traffickers safely crossed the border and turn off their jammers. The only way to prevent such scenarios from happening is by using anti-GPS-spoofing hardware within the drone's makeup. As Michael Buscher, CEO of Vanguard Defense Industries told Defense One reporters, this is a very costly module, and also very bulky. Adding such equipment to a drone is not only very expensive but also affects the drone's flight time, something which both the DHS and CBP are not willing to accept. Right now, the only way to plug these security holes is for the DHS to wait for technology to advance and cut down on its manufacturing prices. To accelerate this process, the DHS also started funding a series of research programs. (Softpedia, 01Jan16)

(U) Coming soon to your smart TV: The next wave of cybercrime

Smart TVs are opening a new window of attack for cybercriminals, as the security defenses of the devices often lag far behind those of smartphones and desktop computers. Running mobile operating systems such as Android, smart TVs present a soft target due to how to manufacturers are emphasizing convenience for users over security, a trade-off that could have severe consequences. Smart TVs aren't just consumer items, either, as the devices are often used in corporate board rooms. Sales of smart TVs are expected to grow more than 20 percent per year through 2019, according to Research and Markets. While attacks against smart TVs are not widespread yet, security experts say it is only a matter of time before cybercriminals take note of the weaknesses. "Many of the solutions aren't even adapting the best practices that are already known in the IT world," said Phil Marshall, chief research officer for Tolaga Research. Smart TVs are essentially computers, with USB ports, operating systems and networking capabilities no different than smartphones. But unlike computers and mobile devices, smart TVs often don't require any authentication. Many of the major manufacturers -- Samsung, LG and Sony -- have built app stores for smart TVs, a model pioneered by Apple for smartphones. But users can also be convinced to download malicious apps from third-party app stores, an attack method used against smartphones that could also be used against smart TVs. Some models do not use encryption known as SSL/TLS (Secure Sockets Layer/Transport Layer Security) when downloading updates. (Computer World, 28Dec15)

(U) American infrastructure's cyber-vulnerabilities again in the spotlight

The fear of a state or terror-group-sponsored cyberattack on the nation's infrastructure was again highlighted by a pair of news stories this week that indicated such groups may have accessed the United States' electrical grid as well as a dam in New York State. The Associated Press reported that independent security researcher Brian Wallace found that hackers, possibly Iranian, had opened a pathway into the nation's power grid and taken passwords and schematic drawings enabling a strong follow-up attack. In addition, another group, again possibly Iranian, may have attempted to gain access to a dam located in New York. While there was no sign a breach took place, this incident was described as a probe of the dam's defenses, according to The Wall Street Journal. The current crop of attacks should prompt a response from not only the potential targets, but from government and internet security firms, said industry watchers. "Every critical industry should sit up and take note of this report," John Stroup, CEO of Belden, told SCMagazine.com in an email Monday. These incidents may indicate that the electrical utility and other infrastructure companies not only need to spend more on defensive measures, but do so quickly to head off a disastrous attack, Tim Erlin, director of IT risk and security strategy at Tripwire, said in a statement. Stroup agreed, adding, "The reality is that our current level of investment in industrial cybersecurity is not sufficient. We need cybersecurity solutions that are crafted to address the unique requirements of these industries." "The energy industry, including electrical utilities, requires substantial investment to tilt the playing field toward defense," Stroup said. One of the more straightforward methods of mitigating the problem is to properly "air gap" power and other utilities from the internet -- essentially sealing them off so hackers can't use their normal attack vectors to gain access. Pierluigi Stella, CTO of Network Box USA (left), does not see any reason, other than convenience, for having these systems exposed to the internet. While this is not a perfect fix, it could go far toward protecting these critical systems. (scmagazine.com, 21Dec15)

Incidents of Interest:

OGA

(U) PayPal investigates account compromised twice in one day
PayPal is investigating an incident in which a user's account was compromised and used in a thwarted attempt to send money to a dead ISIS hacker. Despite the use of two factor authentication, a cybercriminal was reportedly able to log into the account of independent security researcher Brian Krebs and add an unauthorized email account, not once, but twice, on Christmas Eve 2015. A PayPal spokesperson told SCMagazine.com via email it appears the company's standard procedures were not followed in this case, but didn't specify whether Krebs or PayPal was at fault. "While Mr. Krebs' funds remained secure, we are sorry that this unacceptable situation arose and we are reviewing the matter in order to prevent it from happening again," the spokesperson said. The security researcher notified the online payment service of the initial unauthorized email change and was assured that his account would be monitored. However, the account was again compromised. The hacker added the same email account and changed the password and allegedly attempted to send money to an ISIS hacker who was killed in a drone strike earlier that year. The account was then shut down. (scmagazine.com, 05Jan16)

(U) ICS/SCADA researchers leak default passwords of popular industry systems
Russian Industrial Controls Systems Supervisory Control and Data Acquisition (ICS/SCADA) researchers posted a list of industrial products that ship with default passwords in an effort to urge vendors to implement better security controls, a move some feel could cause more harm than good. Jonathan Sander, vice president of product strategy at Lieberman Software told SCMagazine.com that "anyone finding themselves at risk for having default passwords needs to look in the mirror" because some of the fault falls on the IT professional who didn't change the credentials after purchasing the systems. Sander said the product list and password dump may cause some companies to take inventory and secure vulnerable systems but added it also created new and unnecessary risks to the companies because it exposes them while they try to identify whether or not their systems are protected by a weak password. "You may not know the name of the vendor for your SCADA stuff because you're buying them in bulk," Sander said. The researchers point with this exercise was to change the mindset of vendors that use simple and default passwords in industrial systems, instead of requiring users to change these items on first login, use complex passwords, according to InformationWeek. The list has been dubbed the "SCADAPass" and contains default credentials for more than 100 products including web servers from vendors such as Allen-Bradley, Schneider Electric, and Siemens. (scmagazine.com, 05Jan16)

(U) Steam confirms info on 34K users likely exposed in Christmas Day DoS attack
Steam confirmed in a statement on its website that a midday denial-of-service attack on Christmas likely exposed the personal information of 34,000 users via store page requests made between 11:52 a.m. and 13:20 p.m. PST. While the statement said the information varied according to page, some pages included a Steam user's billing address, the last four digits of their Steam Guard phone number, the last two digits of their credit card number, and/or their email address." The company assured users that the "cached requests did not include full credit card numbers, user passwords, or enough data to allow logging in as or completing a transaction as another user." Referring to "Steam's troubled Christmas," the statement noted that users who did not browse a Steam Store page with personal data during that time period shouldn't worry that their information had been exposed. Valve, the form behind the Steam gaming platform, and its web caching partner are trying to identify the users affected and will contact them accordingly. No unauthorized activity has been spotted. The statement said the attack that began on Christmas morning "prevented the serving of store pages to users," particularly confounding since the Steam Sale had generated a 2,000 percent increase in traffic to the Steam store. Cache management rules were deployed, in an effort to reroute "legitimate" traffic as well as "minimize the impact on Steam Store servers." But a second caching configuration deployed in response to the second wave of the attack "incorrectly cached web traffic for authenticated users" and inadvertently let some users see "Steam Store responses which were generated for other users." When the error was spotted, the store was shuttered until the company deployed a new caching configuration and remained down until all the caching configurations had been reviewed and confirmation was received that "the latest configurations had been deployed to all partner servers and that all cached data on edge servers had been purged". (scmagazine.com, 31Dec15)

OGA

Items of Interest

(U) Microsoft to pull the plug on Internet Explorer 8, 9, and 10 next Tuesday
Microsoft is ending support for Internet Explorer 8, 9, and 10 next week on 12 January, releasing a final patch encouraging users to upgrade to one of the company's more recent browsers. The end of support means that these older versions of Internet Explorer will no longer receive security updates or technical support, making anyone who uses them much more vulnerable to hackers. A recently-announced patch will deliver the last few bug fixes, as well as an "End of Life" notification telling users to upgrade to IE 11 or Microsoft Edge -- the company's successor to Internet Explorer, built for Windows 10. This move has a been a long time coming, with Microsoft announcing the end of support for IE 8, 9, and 10 back in August 2014. (The Verge, 06Jan16)

OGA

(U) IPv6 celebrates its 20th birthday by reaching 10 percent deployment

Twenty years ago this month, RFC 1883 was published: Internet Protocol, Version 6 (IPv6) Specification. According to Google's statistics, on 26 December, the world reached 9.98 percent IPv6 deployment, up from just under 6 percent a year earlier. Google measures IPv6 deployment by having a small fraction of their users execute a Javascript program that tests whether the computer in question can load URLs over IPv6. During weekends, a tenth of Google's users are able to do this, but during weekdays it's less than 8 percent. Apparently more people have IPv6 available at home than at work. Google also keeps a map of the world with IPv6 deployment numbers per country, handily color-coded for our convenience. More and more countries are turning green, with the US at nearly 25 percent IPv6, and Belgium still leading the world at almost 43 percent. Many other countries in Europe and Latin America and even Canada have turned green in the past year or two, but a lot of others are still stubbornly staying white, with IPv6 deployment figures well below one percent. Some, including China and many African nations, are even turning red or orange, indicating that IPv6 users in those countries experience significantly worse performance than IPv4 users. The past four years, IPv6 deployment increased by a factor 2.5 each year: from 0.4 percent by the end of 2011 to 1 percent in late 2012, 2.5 percent at the end of 2013, and 6 percent a year ago. Having 4 percent of the world's population Google's users gain IPv6 connectivity in a year is a huge number, but considering that outside Africa, there's no more IPv4 addresses to be had, the remaining 90 percent IPv4 users are still in for a rough ride. If a 67 percent increase per year is the new normal, it'll take until summer 2020 until the entire world has IPv6 and we can all stop slicing and dicing our diminishing stashes of IPv4 addresses. (ars technical, 04Jan16)

(b)(3) 10 USC ⊥ 424

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

(b)(3) 10 USC ⊥ 424