accume partners

AccumeView: Executive Cybersecurity Pulse

The monthly security awareness summary is intended to keep staff informed of recent threats so that they can be properly prepared to defend themselves against the never-ending variety of attacks that they will encounter on a regular basis.

Perspective: There is a storm coming

At least eight Eastern European banks were hacked using **rogue devices** planted inside the network. These devices included cheap laptops, homemade network appliances and usb "Bash Bunnies" to intercept data and provide remote access. Most institutions are not capable of detecting rogue devices and specialized tools such as the bash bunnies, which are usb devices are designed to emulate trusted USB devices so that they can bypass USB port restrictions that many companies use. Once installed, they discretely exfiltrate documents, Install backdoors and perform a variety of exploits.

Last month this brief discussed the probability of "**Vaporworms**," a fileless malware strain that spread like a worm. This month we have reports of a Windows worm propagating through removable drives spreading the BLADABINDI Trojan with backdoor, DDoS and RAT capabilities. While the initial distribution is through removable drives, it is only a matter of time before it's distributed through email and web channels.

A new report states that almost 25% of vulnerabilities discovered in 2018 have no solution for **remediation**. Businesses need to ensure that they are aware of vulnerabilities on their network, and have solutions in place to account for vulnerabilities that don't have a direct method for remediation.

Spectre attacks are becoming more commonplace, with seven new CPU attacks detected that can attack AMD, ARM, and Intel CPUs to various degrees. Malware has been detected for several variations of Spectre, so this should be considered a wakeup call for organizations that have either not patched against Spectre attacks, or who have not established mitigating controls to defend against systems that are unpatched. The time to act is now.

Finally, the **green padlock** icon indicating that a webpage is secure with an SSL certificate is no longer an effective measure of a websites security. A new study indicates that over half of the websites used for phishing are protected with an SSL certificate to appear legitimate. Ensure that your security awareness training is up to date, otherwise users can be lulled into thinking a malicious site is secure.

~Stay Secure

If you found this information valuable, we recommend taking a look at our weekly threat intelligence brief. For more information, contact us here.

Bob Gaines
Director
646.375.9500 x114
rgaines@accumepartners.com

Regulatory News

Congress Approves New DHS Cybersecurity Agency – The United States will soon officially have a singly agency that takes the lead role for cybersecurity. Congress has passed legislation to establish a new cybersecurity agency within the Department of Homeland Security. The House on Tuesday unanimously passed the measure, the CISA Act, which won Senate approval earlier. It now awaits President Trump's signature. The new Cybersecurity and Infrastructure Security Agency will have the same stature as other units within DHS, such as the U.S. Secret Service or Federal Emergency Management Agency. The National Protection and Programs Directorate, or NPPD, will be reorganized into the new agency. Source: https://www.bankinfosecurity.com/congress-approves-new-dhs-cybersecurity-agency-a-11702

GDPR's Impact: The First Six Months – GDPR is now six months old – it's time to take an assessment of the regulation's impact so far. At first blush it would appear very little has changed. There are no well-publicized actions being taken against offenders. No large fines levied. So, does this mean it's yet another regulation that will be ignored? Actually, nothing could be farther from the truth. The day GDPR came into law complaints were filed by data subjects against Facebook and Google. Complaints – that does not sound like action by regulators, in fact it's not – its action taken by lawyers. GDPR is a much-evolved form of European regulation allowing data subjects to file suits against data collectors whom they believe are violating their rights. This battle is going to be fought in 28 EU countries courts much sooner than in their Data Protection commissioners' ministries who enforce the law and handout fines for violations. Source: https://www.helpnetsecurity.com/2018/11/26/gdpr-impact/

Senators Push for Data Breach and Privacy Legislation Following Mariott Breach - U.S. Democrat Senators Mark Warne, Ed Markey, and Richard Blumenthal published statements asking for the passage of data security and consumer privacy legislation by the Congress following the Marriot International hotel chain breach. The Marriott hotel chain disclosed a huge data breach on November 30 which affected 500 million customers who had their data stored in the chain's Starwood guest reservation database. Moreover, the massive security breach happened in 2014, and Marriot found out about it on September 10 following an internal security alert regarding an attempt to access the Starwood reservation database. "Breaches like this can lead to identity theft and crippling financial fraud. They are a black cloud hanging over the United States' bright economic horizon. The American people deserve real action," said Senator Markey. Source: https://news.softpedia.com/news/senators-push-for-data-breach-and-privacy-legislation-following-marriot-breach-524081.shtml

Social Engineering

Offi Report Shows Increase in Email Attacks Using .com File Extensions – The .com file extension designated executable files in DOS and Windows 95, 98 and

Me. It has been replaced by .exe in later versions of the operating system -- for example, the early Windows shell program command.com was replaced by cmd.exe in later versions. However, for backwards compatibility, Windows will still attempt to execute a file with the .com extension. Throughout October, Cofense analyzed 132 unique phishing samples with the .com extension. To put this uptick in context, it found only 34 samples in the entire preceding nine months of 2018. The most popular subject line lures in the new campaign (or campaigns) are 'payment' and 'purchase order' themes. These two make up 67% of the samples analyzed. Other themes include 'shipping', 'invoice' and 'remittance advice', giving the campaign a strong financial bias. Source: https://www.securityweek.com/report-shows-increase-email-attacks-using-com-file-extensions

Half of Phishing Sites Trick You Into Thinking They're 'Secure' - You can't assume that a site is honest because it has that "secure" padlock in the address bar, and PhishLabs just illustrated why. The anti-phishing company has determined that 49 percent of all known phishing sites used Secure Sockets Layer protection (and thus displayed the padlock) as of the third quarter of 2018. That's a sharp rise from 35 percent in the second quarter, and a steep climb from 25 percent a year earlier. They'll still try to trick you into handing over vital details -- it's just that their web traffic will be encrypted while they do it. PhishLabs' John LaCour links the sharp rise to both the attackers themselves and their response to software decisions. Many phishers are buying web domains and promptly creating SSL certificates for them. And while Google was helpful when it started warning Chrome users about non-secure sites, that likely prompted phishers to secure their sites in an attempt to avoid those alerts. Source: https://www.engadget.com/2018/11/26/half-of-phishing-sites-now-show-as-secure/

Losses from Online Payment Fraud to Reach $48 Billion Annually – A new study from Juniper Research has found that annual online payment fraud losses from eCommerce, airline ticketing, money transfer and banking services, will reach $48 billion by 2023; up from the $22 billion in losses projected for 2018. Juniper's new research, Online Payment Fraud: Emerging Threats, Segment Analysis & Market Forecasts 2018-2023, claimed that a critical driver behind these losses will be the continued high level of data breaches resulting in the theft of sensitive personal information. Source: https://www.helpnetsecurity.com/2018/11/23/online-payment-fraud/

Eastern European Banks Lose Tens of Millions of Dollars in Hollywood Style Hacks – Cyber-criminal gangs are believed to have stolen tens of millions of dollars from at least eight banks in Eastern Europe using tactics usually seen only in Hollywood movies. These "hacks" consisted of cyber-criminals entering bank offices to inspect and then leave malicious devices connected to the bank's network. Russian cyber-security firm Kaspersky Lab, which was called to investigate some of these mysterious cyber-heists, says it found three types of devices at central or regional offices at the eight banks it reviewed. These included cheap laptops, Raspberry Pi boards, or malicious USB thumb drives known as Bash Bunnies. Kaspersky said hackers left these devices connected to a bank network or computer, and then connected to the rogue device from a remote location using a GPRS, 3G, or LTE modem. Source: https://www.zdnet.com/article/eastern-european-banks-lose-tens-of-millions-of-dollars-in-hollywood-style-hacks/

Internet Threats

Media Alert: Sophos 2019 Threat Report Unveils the Rise of the Hand-Delivered, Targeted Cyberattacks - Sophos (LSE: SOPH) today launched its 2019 Threat Report providing insights into emerging and evolving cybersecurity trends. The report, produced by SophosLabs researchers, explores changes in the threat landscape over the past 12 months, uncovering trends and how they are expected to impact cybersecurity in 2019."The threat landscape is undoubtedly evolving; less skilled cyber criminals are being forced out of business, the fittest among them step up their game to survive and we'll eventually be left with fewer, but smarter and stronger, adversaries. These new cybercriminals are effectively a cross-breed of the once esoteric, targeted attacker, and the pedestrian purveyor of off-the-shelf malware, using manual hacking techniques, not for espionage or sabotage, but to maintain their dishonorable income streams." - Joe Levy, CTO, Sophos, as referenced in the SophosLabs 2019 Threat Report Source: https://www.apnews.com/6ff3541061b2e28763650edf27efcc3b

Almost 50 Percent of 2018 Vulnerabilities Can be Exploited Remotely - Approximately half of all vulnerabilities disclosed during 2018 come with a remote attack vector while only 13% of them require local access according to Risk Based Security's 2018 Q3 Vulnerability Quick View Report. As reported by Risk Based Security, 16,172 vulnerabilities were published by their VulnDB team until the end of Q3 2018, with a 7% decrease when compared to the total of vulnerabilities unearthed during the time interval in 2017. "The trends through Q3 2018, as compared to 2017, are interesting. Only three months, January (4.5%), February (24.6%), and May (7.6%) showed an increase in disclosures compared to 2017," says Risk Based Security. "The remaining months showed decreases ranging from July with a 1.7% dip, to September with a significant 40.0% drop." Source: https://news.softpedia.com/news/almost-50-percent-of-2018-vulnerabilities-can-be-exploited-remotely-523869.shtml

Talk About a Cache Flow Problem: This JavaScript Can Snoop on Other Browser Tabs to Work Out What You're Visiting – Computer science boffins have demonstrated a side-channel attack technique that bypasses recently-introduced privacy defenses and makes even the Tor browser subject to tracking. The result: it is possible for malicious JavaScript in one web browser tab to spy on other open tabs, and work out which websites you're visiting. This information can be used to target adverts at you based on your interests, or otherwise work out the kind of stuff you're into and collect it in safe-keeping for future reference. Researchers Anatoly Shusterman, Lachlan Kang, Yarden Haskal, Yosef Meltser, Prateek Mittal, Yossi Oren, Yuval Yarom – from Ben-Gurion University of the Negev in Israel, the University of Adelaide in Australia, and Princeton University in the US – have devised a processor cache-based website fingerprinting attack that uses JavaScript for gathering data to identify visited websites. Source: https://www.theregister.co.uk/2018/11/21/unmasking_browsers_side_channels/

Internal Threats

Researchers Discover SplitSpectre, a New Spectre-like CPU Attack – Three academics from Northeastern University and three researchers from IBM Research have discovered a new variation of the Spectre CPU vulnerability that can be exploited via browser-based code. The research team says this new CPU vulnerability is, too, a design flaw in the microarchitecture of modern processors that can be exploited by attacking the process of "speculative execution," an optimization technique used to improve CPU performance. The vulnerability, which researchers codenamed SplitSpectre, is a variation of the original Spectre v1 vulnerability discovered last year and which became public in January 2018. The difference in SplitSpectre is not in what parts of a CPU's microarchitecture the flaw targets, but how the attack is carried out. Source: https://www.zdnet.com/article/researchers-discover-splitspectre-a-new-spectre-like-cpu-attack/

Almost a Quarter of Reported Vulnerabilities Have no Known Solution – The number of reported vulnerabilities in 2018 is seven percent down on the same period last year, according to a new report from Risk Based Security. It's not all good news though, as 24.9 percent of 2018's reported vulnerabilities currently have no known solution which is a reminder that, while patching is very important, it can't be relied on exclusively as a remedy. Vulnerabilities with a CVSSv2 score of 9.0+, often referred to as 'critical', accounted for 15.4 percent of all published vulnerabilities through the third quarter. Also, Risk Based Security's own VulnDB published 4,823 more vulnerabilities than CVE/NVD through the end of Q3 2018. Source: https://betanews.com/2018/11/19/vulnerabilities-no-solution/

Vaporworms: New Breed of Self-Propagating Fileless Malware to Emerge in 2019 – WatchGuard Technologies' information security predictions for 2019 include the emergence of vaporworms, a new breed of fileless malware with wormlike properties to self-propagate through vulnerable systems, along with a takedown of the internet itself and ransomware targeting utilities and industrial control systems. "Cyber criminals are continuing to reshape the threat landscape as they update their tactics and escalate their attacks against businesses, governments and even the infrastructure of the internet itself," said Corey Nachreiner, CTO at WatchGuard Technologies. "The Threat Lab's 2019 predictions span from highly likely to audacious, but consistent across all eight is that there's hope for preventing them. Organizations of all sizes need to look ahead at what new threats might be around the corner, prepare for evolving attacks and ensure they're equipped with layered security defenses to meet them head-on." Source: https://www.helpnetsecurity.com/2018/11/16/self-propagating-fileless-malware/

Recommended Actions to take

The following set of recommendations is based on the information provided above in the brief. For a more detailed set of recommendations, as well as vulnerabilities and indicators of compromise, please refer to Accume's weekly threat intelligence briefings.

- Never trust an unsolicited email
- Never open an attachment from a source that is unknown.
    - If it from a known user, but unsolicited, call the user to verify the nature of the attachment
- Be vigilant when responding to or opening an attachment within a text message
- Don't install software from untrusted sources
- Pay attention to the url address in web pages that you are visiting.
    - Don't trust popups or any automatic re-direction to another page
- Never click a link within an email or web page where the URL has been shortened or hidden (i.e. tinyurl and other services.)
- Be careful when using social media
- Make sure that your incident response playbook is updated regularly to address the latest threats.
- Ensure that your systems are patched and free from configuration-based vulnerabilities
- Make sure that your layered defenses (IDS, Firewall, Web-Filtering) are dynamically updating
- If you see or suspect any suspicious activity when using the internet or email, report it immediately.
- Keep current with emerging state privacy and incident response laws (California and Colorado are mentioned in this issue of AccumeView) to ensure your organization is ready for tightening regulatory requirements.

If you have questions about any of the above recommendations, or about their implementation, feel free to reach out to Accume for additional information.

If you found this information valuable, we recommend our weekly threat intelligence brief, which has additional operational details for you and your staff. For more information, contact us here.