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: Hack the Human

On June 28, 2018, California enacted the California Consumer Privacy Act of 2018 (CCPA), which provides what is arguably the most restrictive privacy law in the U.S. and would likely have some effect on most businesses across the country. The CCPA, which shares many common requirements as the new European Union General Data Protection Regulation (GDPR), will take effect on January 1, 2020. The time to prepare is now. Accume is developing a white paper on this topic, and developing solutions based on what we have learned through GDPR project implementations.

As the smoke clears from the **City of Altanta's** cyber attack, experts are stating that the damage to City systems is worse than originally thought. A large number of applications are still offline and a significant amount of data is permanently lost, including years of dash-camera video. It will take months to get operations running properly. While this attack appears to be a worst-case scenario for the City, the threat is all too real, and can strike any business, anywhere. This story underscores the necessity for an effective incident response AND business continuity plan: a rapid response paired with proper restoration of data from backups would have prevented such a catastriphic loss to city operations.

Colorado has set a new benchmark for data breach notification. A new regulation stipulates a 30-day notification window, which is the lowest in the country. In addition, it has no exemption for encrypted data, which many other states have. The new regulation takes play September 01, so get your incident response plans updated appropriately if you do business in Colorado.

And just when you thought your personal data was secure, a little-known Florida company may have exposed the personal data of **nearly every American adult**, according to a new report. Exactis, a Palm Coast, Fla.-based marketing and data-aggregation company, had exposed a database containing almost 2 terabytes of data, comprising nearly 340 million individual records, on a public server. That included records of 230 million consumers and 110 million businesses. Get ready for more sophisticated phishing campaigns that will seek to weaponize this data.

~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

Sweeping Data Privacy Bill Approved in California – California will soon have what experts call the nation's most far-reaching law to give consumers more control over their personal data under a bill the governor signed Thursday. The law will compel companies to tell customers upon request what personal data they've collected, why it was collected and what categories of third parties have received it. The new law will take effect Jan. 1, 2020, and lawmakers say they will likely make alterations to improve the policy before then. Consumers will also be able to ask companies to delete their information and refrain from selling it. It's similar to data privacy regulation in the European Union, which also aims to give consumers control over use of their data. Source: https://www.nextgov.com/cybersecurity/2018/06/new-bill-aims-prevent-next-kaspersky-zte/149126/

Federal Judge Strikes Down CFPB Structure - A federal judge in New York ruled Thursday that the makeup of the CFPB violates the constitution because it is governed by a single director who only can be removed by the president for cause. The ruling conflicts with a January ruling by the District of Columbia Circuit Court of Appeals, which ruled that the agency's structure of having one director, who may only be removed for cause, is not unconstitutional. That ruling came in a lawsuit filed by PHH, a mortgage company. The New York ruling throws even more uncertainty into the future of the CFPB. It only covers the Southern District of New York. But the New York decision could lead to more lawsuits being filed challenging the constitutionality of the agency, according to Jeff Sovern, a law professor at the St. John's University Law School. He wrote in a consumer law blog sponsored by Public Citizen that the constitutionality of the agency may end up before the U.S. Supreme Court. Source: https://www.cutimes.com/2018/06/22/federal-judge-strikes-down-cfpb-structure/

New Colorado Law Sets 30-Day Requirement for Data Breach Notification - Colorado Gov. John Hickenlooper last week signed bipartisan bill HB18-1128, "Protections for Consumer Data Privacy," officially setting in place some of the most stringent requirements for personal information data disposal and data breach notification in place in any U.S. state. The new law requires organizations to maintain a policy for disposing documents with consumer data and notify Colorado residents of any potential personal information exposure no later than 30 days after discovering a data breach. The 30-day notification window does not provide for any specific exemptions and is the shortest of any state. The Colorado regulation is set to take effect Sept. 1. The law additionally expands the state's definition of "personally identifying information" and requires organizations to provide Colorado residents affected by data breaches with the estimated date of the breach and a description of what information was likely accessed. Source: https://www.cutimes.com/2018/06/11/new-colorado-law-sets-30-day-requirement-for-data/?slreturn=20180513054758

Social Engineering

Office 365 Users Targeted by Phishers Employing Simply HTML Tricks – Phishers are using a simple but effective trick to fool Microsoft's NLP-based anti-phishing protections and Office 365 users into entering their login credentials into spoofed login pages. The phishing emails landing in targets' inboxes warn potential victims that their email account has reached a "maximum quota limit" and that they should upgrade their account. To the casual observer, the emails appear to be "signed" by Microsoft. Source: https://www.helpnetsecurity.com/2018/06/22/office-365-phishing-tricks/

RSA Fraud Report: Newsjacking-Based Phishing on the Rise – RSA's latest Quarterly Fraud Report shows that so-called "newsjacking" is increasingly empowering phishing attacks, says Angel Grant, RSA's director of identity fraud and risk intelligence. A recent news item leveraged to fuel a massive phishing campaign, she points out, was the relaunch of Canada's Interac payment network. Plus, she anticipates a rise in phishing that involves phony messages about the EU's General Data Protection Regulation now that enforcement has begun. "We're already starting to see an uptick of phishing emails targeting fake GDPR alerts, [especially] privacy notification acceptance emails, because everyone's getting tons of those right now," she says in an interview with Information Security Media Group. "So yes, any kind of major news like that, cybercriminals tend to newsjack based upon that trend, and try to capitalize on that moment." Source: https://www.inforisktoday.com/rsa-fraud-report-newsjacking-based-phishing-on-rise-a-11058

25 Percent of Employees Use the Same Password for Every Account – Employees may be a company's greatest asset, but they also remain the greatest cybersecurity risk, according to a Monday report from OpenVPN. Despite an increased focus on security training, 25% of the 500 US employees surveyed report that they use the same password for every account, the report found. Another 23% of employees said they frequently click on links before verifying that they lead to a legitimate, safe website. Of the employees that use the same password for everything, a whopping 81% said they do not password protect their computer or phone at all, according to the report. Source: https://www.techrepublic.com/article/25-of-employees-use-the-same-password-for-every-account/

Adidas Phishing Campaign Promises Free Shoes, Offers $50 Subscription Instead – An Adidas phishing campaign is offering potential victims a "free" $50 per month subscription all under the promise of free shoes. Threat attackers lure victims with a message suggesting Adidas is giving away 2,500 pairs of shoes to celebrate its 69th anniversary and a homographic link spoofing the appearance a legitimate Adidas website albeit a vertical line with no dot in place of where the "i" would be. Other brands using similar lures and URL spoofs were also exploited in the malicious campaign. Researchers described the attack as appearing fairly well structured and noted its geolocation-based redirections and the checks made to ensure requests are made from a mobile device such as a smartphone. Source: https://www.scmagazine.com/adidas-phishing-campaign-promises-free-shoes-offers-50-subscription-instead/article/773683/

Internet Threats

A Wicked Family of Bots – As we continue to keep track of the latest IoT botnets, the FortiGuard Labs team has seen an increasing number of Mirai variants, thanks to the source code being made public two years ago. Since then, threat actors have been adding their own flavors to the original recipe. Some made significant modifications, such as adding the capability to turn infected devices into swarms of malware proxies and cryptominers. Others integrated Mirai code with multiple exploits targeting both known and unknown vulnerabilities, similar to a new variant recently discovered by FortiGuard Labs, which we now call WICKED. This new variant has added at least three exploits to its arsenal to target unpatched IoT devices. In this article, we will take a look at how it works, the primary purpose of this bot, and how it relates to other known botnets. Source: https://thehackernews.com/2018/05/vpnfilter-botnet-malware.html

Banking Trojans and Cryptojacking on the Rise - A new report analyzes threat data collected from approximately 750,000 Morphisec protected endpoints globally, between January 1 and March 31, 2018, as well as from in-depth investigations conducted by the Morphisec Labs threat research team. The report reveals key trends and definitive changes in the attack landscape for a 90-day span, with technical details on specific attack techniques and tactics used, including a highly unique set of threat analyses on five of the most critical threats to enterprise organizations. The Morphisec Labs team provides a risk-based impact analysis for end-users who could be affected by the threats outlined, along with prescriptive guidance on how to protect critical business assets. Source for this story is included below: https://www.helpnetsecurity.com/2018/06/22/morphisec-labs-threat-report-q1-2018/

What is DMARC?

DMARC (Domain-based Message Authentication, Reporting & Conformance) is a way to make it easier for email senders and receivers to determine whether or not a given message is legitimately from the sender, and what to do if it isn't. This makes it easier to identify spam and phishing messages, and keep them out of peoples' inboxes.

DMARC ensures that legitimate email is properly authenticating against established email standards, and that fraudulent activity appearing to come from domains under the organization's control is blocked.

Why it matters: DMARC is the first and only widely deployed technology that can make the "header from" address (what users see in their email clients) trustworthy. Not only does this help protect customers and the brand, it discourages cybercriminals who are less likely to go after a brand with a DMARC record.

G Suite Admins Need to FTFM – Thousands Expose Internal Emails – If you're sysadmin of an organization using Google Groups and G Suite, you need to revisit your configuration to make sure you aren't leaking internal information. That advice comes from Kenna Security, which on June 1 said it found 31 per cent of a sample of 9,600 organizations leaking sensitive e-mail information. The company explained while previous advisories about the issue (such as this from 2017) have explained how G Suite can leak, sysadmins appear not to be taking the matter seriously. The problem, Kenna said in its post, is that Google

Groups, available to G Suite customers, has "complex terminology" and a clash between "organization-wide vs group-specific permissions". As a result, list admins can "inadvertently expose e-mail list contents" (which were meant to stay inside the organization). Source for this story is included below: https://www.theregister.co.uk/2018/06/04/g_suite_misconfiguration_leaks_data/

Internal Threats

Why You May Want to Update Your Browser in the Next Nine Days – It's time for early Transport Layer Security (TLS) versions to die, die, die… which means that it's time for all of us, if we haven't already, to take our browsers, our projects and/or our organizations and upgrade, upgrade, upgrade. Online merchants have until 30 June to support TLS 1.2 and HTTP/1.1: a kill date that was extended for these security protocols from the original June 2016 deadline, which the PCI Council decided that retailers weren't going to make. Source: https://nakedsecurity.sophos.com/2018/06/21/why-you-may-want-to-update-your-browser-in-the-next-9-days/

Hackers Using KillDisk MBR-wiping Malware to Attack Bank's SWIFT Money Transferring System – New KillDisk Malware is hitting financial institutions in Latin America to attack SWIFT networks and gain access to the systems that connected to the bank with an infected organization. Most of the financial institutions are connected with the SWIFT (Worldwide Interbank Financial Telecommunication's network) network in worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment. Researchers analysis reveal that this is the new variant of the earlier version of KillDisk which is performing MBR-wiping in affected systems. Payload activities make difficult to determine that the attack was motivated by a cybercriminal campaign or coordinated attack. Source: https://gbhackers.com/killdisk-mbr-wiping-malwar/

EU Claims Kaspersky Lab Software 'Confirmed as Malicious' – The anti-Kaspersky Lab rhetoric continues to heat up in Europe, with the European Parliament passing a motion branding the Moscow-based anti-virus firm's software as being "confirmed as malicious." In response, Russia-based Kaspersky Lab says it's halted all work with European institutions, including Europol - the EU's law enforcement intelligence agency - until it receives clarification from the European Parliament. The company says it's also paused its work with the No More Ransom project, which provides free decryption tools to ransomware victims. On Wednesday, members of the European Parliament voted 476 to 151 to approve a nonbinding cyber defense motion that seeks to improve Europe's ability to defend itself against online attacks, hire more cybersecurity experts and get better at sharing information. The motion also singles out Kaspersky Lab. An amendment reportedly added by Polish MEP Anna Elzbieta Fotyga "calls on the EU to perform a comprehensive review of software, IT and communications equipment and infrastructure used in the institutions in order to exclude potentially dangerous programs and devices, and to ban the ones that have been confirmed as malicious, such as Kaspersky Lab." Source: https://www.bankinfosecurity.com/eu-claims-kaspersky-lab-software-confirmed-as-malicious-a-11080

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.
- 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.