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: Scope, Scale and Duration

India's Cosmos Bank was hit with a **coordinated attack** using cloned ATM cards and an attack against the SWIFT system. Of note, the attack involved money mules in 28 different countries, and 15,000 transactions over a seven-hour window of opportunity. The SWIFT transaction involved moving $1.93m to an account at a bank in Hong Kong. While analysis is still underway, a group linked to North Korea is the current suspect.

And finally, On May 27, Justice Department officials asked Americans to reboot their routers because they suspected that **Russian military spy software** is on hundreds of thousands of home routers. However, because of the design of the malware, rebooting is not enough. The FBI recommends upgrading router firmware to their latest version and changing the administrative passwords. Manufacturers have not provided any additional guidance on any permanent fixes or methods of detection at this point, and no timetables have been provided, so advise users to perform updates and password changes at this point in time.

If your systems are using **OpenSSH**, beware that a vulnerability has been detected that affects OpenSSH Versions Since 1999. While this is a specialized attack, the scope is significant in that billions of devices have been using OpenSSH. There is a patch available, but it's best to ensure that your systems and your critical vendors are protected.

Hackers are able to steal more than $1 million from the global economy through cybercrime in **a single minute**, according to areport released by cybersecurity firm RiskIQ. Malware, Phishing, Business Email Compromise and other attacks generate a stunning amount of revenue for criminals. To accomplish this, 1,274 unique types of malware are generated every minute.

DDoS attack volumes have increased by 50% according to a report by Link11. The report also revealed that threat actors targeted organisations most frequently between 4pm CET and midnight Saturday through to Monday, with businesses in the e-commerce, gaming, IT hosting, finance, and entertainment/media sectors being the most affected.

~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

Security Highlights

Hackers Steal More Than $1M From Global Economy in a Single Minute: Analysis - Hackers are able to steal more than $1 million from the global economy through cybercrime in a single minute, according to a new report released Tuesday. Approximately 1,861 people fall victim to cyberattacks in a span of 60 seconds, while some $1.14 million is stolen, cybersecurity firm RiskIQ found. The project aimed to show the magnitude of the issue of global cybercrime by framing it in terms of an "Evil Internet Minute." By analyzing both proprietary and third-party research, the firm's researchers found hackers used a variety of tactics to extract money digitally, including malware, phishing and supply chain attacks that targeted third parties. In addition, cyber criminals issued roughly 1,274 pieces of unique malware each minute. The motives ranged from monetary gain to politics and espionage, RiskIQ found. Source: http://thehill.com/policy/cybersecurity/402716-security-firm-says-hackers-steal-more-than-one-million-dollars-from-the

India's Cosmos Bank Raided for $13M by Hackers - Cosmos Bank in India says that hackers made off with $13.4m in stolen funds over the weekend. Multiple reports out of the country say that a group of attackers used cloned cards to withdraw cash from ATMs at a set time and perform a fraudulent SWIFT money transfer. Together, the efforts resulted in about Rs 94 crore ($13.4m) being stolen from the bank and its account holders. The attack was believed to have taken place in two phases. The first, on Saturday between 1500 and 2200 local time, was an international effort with money mules in 28 different countries, all extracting cash from their local ATMs. According to the Hindustan Times, 15,000 transactions were carried out over the seven-hour period. Source: https://www.theregister.co.uk/2018/08/15/cosmos_bank_raided/

Cloud Computing Remains Top Emerging Business Risk - In Gartner's latest quarterly Emerging Risks Report, 110 senior executives in risk, audit, finance and compliance at large global organizations identified cloud computing as the top concern for the second consecutive quarter. Additional information security risks, such as cybersecurity disclosure and GDPR compliance, ranked among the top five concerns of the executives surveyed. Source: https://www.helpnetsecurity.com/2018/08/16/cloud-computing-business-risk/

Expert Found a Flaw That Affects All OpenSSH Versions Since 1999 - Security expert discovered a username enumeration vulnerability in the OpenSSH client that affects all versions of the software that was released since 1999. Security expert Darek Tytko from securitum.pl has discovered a username enumeration vulnerability in the OpenSSH client. The flaw tracked as CVE-2018-15473 affects all versions of the software that was released since 1999. The vulnerability could be exploited by a remote attacker to guess the usernames registered on an OpenSSH server. OpenSSH maintainers have now released a security fix, but since the OpenSSH client is included in a broad range of software applications many of them could remain vulnerable for a long time. Researchers from Qualys have published a detailed analysis of the vulnerability once discovered that the bug was fixed. The flaw could potentially impact billion of

devices using the vulnerable software. Source: https://securityaffairs.co/wordpress/75596/breaking-news/openssh-cve-2018-15473.html

Regulatory News

Cybersecurity Laws to Cover All Businesses, Angus Taylor Confirms - Any person or organization operating a website in Australia will be captured by sweeping cyber security laws designed to make it easier for police and intelligence agencies to spy on electronic devices and secret communications, the Turnbull government has confirmed. Source: https://www.afr.com/news/cyber-security-laws-to-cover-all-businesses-angus-taylor-confirms-20180814-h13zdo

US Bans Government Personnel From Using Huawei and ZTE Devices - US government employees, contractors and agencies might have to ditch most of their Huawei and ZTE tech. The President has signed the Defense Authorization Act into law, and part of it is a ban on devices and equipment used to route or view user data made by the two companies and some other Chinese manufacturers. Government contractors can still use components that don't handle user data in any way. But since they still have to get rid of existing parts and devices that do, the law includes a directive for agencies to prioritize funding for businesses that have to replace their equipment. Source: https://www.engadget.com/2018/08/14/us-defense-huawei-zte-ban/

The GDPR Ripple Effect - Will we ever see a truly global data security and privacy mandate? The race to comply with the European Union's General Data Protection Regulation (GDPR) by the May 25 deadline is over, but data security and privacy is a marathon, not a sprint. If the ever-evolving regulatory compliance landscape is any indication, GDPR is just the first of many mandates to come. Although it certainly has been a headache for many organizations — with large firms allocating an average of $20 million to $25 million to become GDPR compliant — the GDPR is the catalyst for a much-needed global, all-encompassing data security and privacy law. This is something we need sooner rather than later. Here's the challenge: Companies around the world have long been relying on a patchwork of laws and standards to secure customer data and keep their trust. Source: https://www.darkreading.com/endpoint/privacy/the-gdpr-ripple-effect/a/d-id/1332630

Social Engineering

IT Managers: Are You Keeping Up with Social-Engineering Attacks? Social-engineering attacks are no longer the amateurish efforts of yesterday. Sure, your company may still get obvious phishing emails with blurry logos and rampant misspellings, or the blatantly fake "help desk" calls from unknown phone numbers, but more

sophisticated attacks are becoming the norm. Using both high-tech tools and low-tech strategies, today's social-engineering attacks are more convincing, more targeted, and more effective than before. They're also highly prevalent. Almost seven in 10 companies say they've experienced phishing and social engineering. Source: https://www.darkreading.com/endpoint/it-managers-are-you-keeping-up-with-social-engineering-attacks/

Phishing Attacks Hit Financial Services, Tech Companies Hardest: How to Stay Safe - Phishing attacks skyrocketed in the financial services industry and IT sector early this year, according to the Spam and Phishing in Q2 2018 report from Kaspersky Lab. Over a third (35.7%) of phishing attempts were in the financial services industry, with the IT sector coming in second at 13.83%, according to the report. One of the most popular and easiest methods of cyberattack, phishing is not a new attack vector used by cybercriminals on businesses. In fact, more than half (54%) of companies receive phishing emails regularly, leaving companies at a constant threat of attack. Source: https://www.techrepublic.com/article/phishing-attacks-hit-financial-services-tech-companies-hardest-how-to-stay-safe/

Internet Threats

Web Cache Poisoning Attacks Demonstrated on Major Websites, Platforms - Major websites and platforms may be vulnerable to simple yet devastating web cache poisoning attacks, which could put millions of users in jeopardy. James Kettle, head of research at PortSwigger Web Security, Ltd., a cybersecurity tool publisher headquartered near Manchester, U.K., demonstrated several such attacks during his Black Hat 2018 session titled "Practical Web Cache Poisoning: Redefining 'Unexploitable.'" Kettle first unveiled his web cache poisoning hacks in May, but in the Black Hat session he detailed his techniques and showed how major weaknesses in HTTPS response headers allowed him to compromise popular websites and manipulate platforms such as Drupal and Mozilla's Firefox browser. Source: https://searchsecurity.techtarget.com/news/252446725/Web-cache-poisoning-attacks-demonstrated-on-major-websites-platforms

DDoS Attackers Increasingly Strike Outside of Normal Business Hours - DDoS attack volumes have increased by 50% to an average of 3.3 Gbps during May, June and July 2018, compared to 2.2 Gbps during the previous quarter, according to Link11. Attacks are also becoming increasingly complex, with 46% of incidents using two or more vectors. While attack volumes increased, researchers recorded a 36% decrease in the overall number of attacks. There was a total of 9,325 attacks during the quarter: an average of 102 attacks per day. Source: https://www.helpnetsecurity.com/2018/08/15/ddos-attacks-outside-business-hours/

Russian Military Spy Software is on Hundreds of Thousands of Home Routers - The Russian military is inside hundreds of thousands of routers owned by Americans and others around the world, a top U.S. cybersecurity official said on Friday. The presence of Russian malware on the routers, first revealed in

May, could enable the Kremlin to steal individuals' data or enlist their devices in a massive attack intended to disrupt global economic activity or target institutions. On May 27, Justice Department officials asked Americans to reboot their routers to stop the attack. Afterwards, the world largely forgot about it. That's a mistake, said Rob Joyce, senior advisor to the director of the National Security Agency and the former White House cybersecurity coordinator. Source: https://www.defenseone.com/technology/2018/08/russian-military-spy-software-hundreds-thousands-home-routers/150474/

Internal Threats

Risks Associated With Third-Party Access - We all know that an insider threat is often the biggest challenge an organization needs to be equipped to deal with. Some of the most infamous breaches in recent history have been the result of "trusted" insiders who have turned to the dark side. The other, rather obvious threat is from the unknown attackers who are probing our environment looking for weaknesses and exploiting them for fame, money, or just because. So, is that it? There are only people inside our networks and bad actors outside? Well, according to Joe Campbell, Principal Security Advisor at One Identity, there's a middle ground that we need to remember and that is the 3rd party partner. Source: https://www.csoonline.com/article/3294707/access-control/risks-associated-with-third-party-access.html

Cyber Hygiene Training is Infrequent and Inconsistent. The in-depth study, which surveyed 500 full-time office employees across the US, found that nearly two in five workers admitted to clicking on a link or opening an attachment from a sender they did not recognize. This security slip-up is significant due to the installation of malware on their devices and the harvesting of sensitive corporate data. Source: https://threatbrief.com/cyber-hygiene-training-is-infrequent-and-inconsistent/

New Ransomware Arrives with a Hidden Feature that Hints at More Sophisticated Attacks to Come - A new form of ransomware is spreading to victims around the world and the way it's built suggests those behind it could use it to launch more sophisticated attacks in future. KeyPass ransomware first appeared on 8 August and so far has spread to hundreds of victims in more than 20 countries around the world via fake software installers which download the ransomware onto the victim's PC. Brazil and Vietnam account for the highest percentage of Keypass infections, but victims are reported across the world in regions including South America, Africa, Europe, the Middle East and Asia. Researchers at Kaspersky Lab have examined KeyPass and found that while it's relatively simple, it comes with the additional option for the attackers to take manual control of an infected system, potentially pointing towards the ability to launch more sophisticated attacks on infected networks. Source: https://www.zdnet.com/article/new-ransomware-arrives-with-a-hidden-feature-that-hints-at-more-sophisticated-attacks-to-come/

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 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.