AccumeView: Executive Cybersecurity Pulse

The monthly executive review is intended to keep you informed of recent threats that can impact the confidentiality, integrity and availability of your data and information systems so that your institution can make the necessary technical and procedural changes to protect your institution.

Perspective: state of the marketplace

A new type of **malware** has been discovered that has been hidden for years, which spreads across routers instead of servers and workstations. Researchers believe that this exceptionally complex program can only have been designed by a nation-state. In the security-world, controlling the router is the same as having the keys to the kingdom. Its primary purpose appears to be espionage: for now businesses should not worry, but we'll be keeping tabs on it's activity.

GDPR, which starts in May, continues to make news as its implementation deadline approaches, and companies continue to make headlines as they stumble for implementation. One of the most visible stumbles is taking place at ICANN, which manages the global Whois service. Its failure to prepare for GDPR may allow a major oversight loophole that hackers can exploit for spam and website spoofing. To prepare for this, talk to your vendors about anticipated issues with email and web-filtering that utilize Whois lookups.

It should be no surprise that financial targets make up more than half of all **phishing attacks.** The human element continues to be the weakest link in security, and until that changes, we will continue to see phishing and social engineering at the top of any security threat list.

DDoS attacks made the news several times this week. New DDoS techniques have enabled the attack to grow in size (the largest on record now at 1.35Tbps), and because of this power, attackers are shaking down companies for ransom to stop such crippling attacks.

Finally, recent news about **Android phones** shipping with pre-Installed malware should remind all companies about the necessity of effective vendor and supply-chain management.

~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.

Security Highlights

Nation-State Hackers Adopt Russian 'Maskirovka' Strategy – A wave of surprising twists in both nation-state and cybercrime-related cyberattacks in the past year, along with increasing overlap in their tools and tactics, has ushered in a new era where all is not what it seems. Positively identifying the actual threat group behind a cyberattack as well as its true intentions is getting harder than ever as nation-state hacker groups out of North Korea and Russia, for example, in 2017 employed tactics typically used by their cybercriminal counterparts, and vice versa. Source: https://www.darkreading.com/threat-intelligence/nation-state-hackers-adopt-russian-maskirovka-strategy/d/d-id/1331150

Whois? More like WHOWAS: Domain Database on Verge of Collapse Over EU Privacy – Governments refuse to get sucked into policy shambles, kibosh DNS GDPR plans. An effort to resolve conflicts between upcoming European privacy legislation and the global Whois service for domain names has, predictably, failed, raising fears that cybercriminals will take advantage of the impasse. At the end of a week of meetings hosted by domain-name overseer ICANN, the US-based organization's proposed interim model lies in tatters, and there is no sign of a forthcoming solution before the May 25 deadline, when the General Data Protection Regulation (GDPR) comes into effect. Source: http://www.theregister.co.uk/2018/03/16/whois_gdpr_icann/

IoT Attacks are Getting Worse – and No One's Listening –If there was one theme at this year's Kaspersky conference, it was the constant reminder that many connected devices have potentially serious gaps in security. There's a running joke regarding connected gadgets and the internet of things: "The 'S' in IoT stands for security." And yes, I'm aware there's no "S" in IoT. Oleg Šelajev a lead developer for Oracle Labs, coined the phrase in 2016, and it pops up almost every time researchers find security flaws with a connected device. And it happens a lot. Think security cameras. Or toys. Or smart locks. Yet homes, businesses and facilities are stocking up on more and more connected devices, the idea being to make people's lives easier. Source: https://www.cnet.com/news/iot-attacks-hacker-kaspersky-are-getting-worse-and-no-one-is-listening/

Potent Malware That Hid for Six Years Spread Through Routers – Researchers have discovered malware so stealthy it remained hidden for six years despite infecting at least 100 computers worldwide. Slingshot – which gets its name from text found inside some of the recovered malware samples – is among the most advanced attack platforms ever discovered, which means it was likely developed on behalf of a well-resourced country, researchers with Moscow-based Kapersky Lab reported Friday. The sophistication of the malware rivals that of Regin – the advanced backdoor that infected Belgian telecom Belgacom and other high-profile targets for years – and Project Sauron, a separate piece of malware suspected of being developed by a nation-state that also remained hidden for years. Source: https://arstechnica.com/information-technology/2018/03/potent-malware-that-hid-for-six-years-spread-through-routers/

Regulatory Headlines

GDPR Puts the Spotlight on Compliance MVPs: Data Protection Officers – The European Union's sweeping data regulations are set to take effect in just a few weeks, forcing many companies to suddenly ask, "Do I have a data protection officer?" If the answer is no, the follow up question is probably "How do I get one?" Data protection and regulatory compliance experts have been around for decades but the implications of the General Data Protection Regulation, set to take effect May 25, is putting these professionals to the test – and finally into the spotlight. Source: https://www.ciodive.com/news/gdpr-puts-the-spotlight-on-compliance-mvps-data-protection-officers/518611/

'No Slowdown' for HIPAA Enforcement, But Audits Ending – So what's next for HIPPA enforcement efforts by the Department of Health and Human Services' Office for Civil Rights? OCR director Roger Severino says there is "no slowdown in our enforcement efforts," and that the agency will continue with the "same enforcement mindset." At the HIMSS18 conference on Tuesday, Severing said: "I come from the Department of Justice Office of Civil Rights; I bring that mindset to OCR. We're still looking for big, juicy egregious cases" for enforcement. Source: https://www.healthcareinfosecurity.com/no-slowdown-for-hipaa-enforcement-but-audits-ending-a-10701

Europe's New Privacy Law Will Change the Web, and More – Consumers have long wondered just what Google and Facebook know about them, and who else can access their personal data. But internet giants have little incentive to give straight answers — even to simple questions like, "Why am I being shown this ad?" On May 25, however, the power balance will shift towards consumers, thanks to a European privacy law that restricts how personal data is collected and handled. The rule, called General Data Protection Regulation or GDPR, focuses on ensuring that users know, understand, and consent to the data collected about them. Under GDPR, pages of fine print won't suffice. Neither will forcing users to click yes in order to sign up. Source: https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/

The Cybersecurity Mandates Keep On Coming – There's a good reason for the proliferation of mandates like the one in New York State, but companies may struggle to answer this question: "Are we in compliance?" Financial organizations are no strangers to regulation, but when it comes to cybersecurity, new mandates keep cropping up, and for good reason. According to a study from Accenture and the Ponemon Institute, the global financial services sector has experienced a 40% increase in the cost of cyberattacks during the past three years. Cyber heists against a string of banks (such as $81 million stolen from the Bangladesh central bank and $6 million from the Russian bank) and high-profile data breaches of well-known global financial organizations have demonstrated that financial companies are top targets for cybercriminals. Source: https://www.darkreading.com/risk/compliance/the-cybersecurity-mandates-keep-on-coming/a/d-id/1331366

Social Engineering

Financial Targets Account for More Than Half of Phishing Attacks – More than half of phishing attacks in 2017 were aimed at getting hold of financial information according to a new report. Kaspersky's Lab's anti-phishing technologies detected more than 246 million user attempts to visit different kinds of phishing pages, with 54 percent being attempts to visit a financial-related website, compared to 47 percent in 2016. Source: https://betanews.com/2018/03/01/phishing-targets-financials/

How to Fight Mobile Number Port-Out Scams – T-Mobile, AT&T and other mobile carriers are reminding customers to take advantage of free services that can block identity thieves from easily "porting" your mobile phone number out to another provider, which allows crooks to intercept your calls and messages while your phone goes dark. Unauthorized mobile phone number porting is not a new problem, but T-Mobile said it began alerting customers about it earlier this month because the company has seen a recent uptick in fraudulent requests to have customer phone numbers ported over to another mobile provider's network. Source: https://krebsonsecurity.com/2018/02/how-to-fight-mobile-number-port-out-scams/

Hackers Continue to Exploit Hijacked MailChimp Accounts in Cybercrime Campaigns – MailChimp, a service that millions of people around the world use to send out email newsletters, is being abused by hackers to spam out malware. A typical attack involves hackers either compromising an existing MailChimp account, or setting up a fraudulent account, from which they then spam out scams or links to malicious content. Why do they do this? Well, many mail providers trust MailChimp because it is so widely used, and are loathe to block newsletters and order confirmations sent via MailChimp for fear of upsetting users and the brands behind the messages. Source: https://hotforsecurity.bitdefender.com/blog/hackers-continue-to-exploit-hijacked-mailchimp-accounts-in-cybercrime-campaigns-19687.html

FTC Study: Millennials are The Biggest Victims of Social Engineering – A report from the FTC found that 40% of adults age 20-29 lost money to fraud, while only 18% of adults over the age of 70 did so, challenging the narrative of older adults falling victims to scams. Report after report has found that younger adults are the biggest victims of scams. IT leaders need to make sure those users are properly trained on cybersecurity policy and treated like all other employees in regards to security. The FTC has issued its annual report of consumer complaints, which shows that young adults are more likely to lose money to fraud than older adults. Source: https://blog.knowbe4.com/ftc-study-millennials-are-the-biggest-victims-of-social-engineering

Internal Threats

Ransomware: Get Ready for the Next Wave of Destructive Cyberattacks – It might look to be out of the limelight compared to 2017, but it would be foolish to write ransomware off yet, as more attacks using the file-encrypting malware are ahead. High profile incidents like WannaCry, NotPetya and Bad Rabbit made ransomware infamous last year. WannaCry and NotPetya have since both been attributed to be the work of nation-states – the former North Korea and the latter to Russia – changing the perception of ransomware from something used by cybercriminals attempting to make a quick buck, to it becoming a tool of cyberwarfare. Source: http://www.zdnet.com/article/ransomware-get-ready-for-the-next-wave-of-destructive-cyberattacks/

Android Phones Caught Selling with Pre-Installed Factory Malware – More than 40 Android phone models, most of them manufactured by companies in China, ship with pre-installed malware that was injected into the firmware straight from the factory. Security company Dr. Web says that it came across a new Trojan called Android.Triada.231 in the firmware of several Android devices back in mid-2017, and after an in-depth research, it discovered that over 40 models are likely to be affected. Source: http://news.softpedia.com/news/android-phones-caught-selling-with-pre-installed-factory-malware-520058.shtml

Top Cybersecurity Evasion and Exfiltration Techniques Used By Attackers – SS8 released its 2018 Threat Rewind Report, which reveals the top cybersecurity evasion and exfiltration techniques used by attackers and malicious insiders. During the past year, SS8 sensors and analytics deployed globally within live production networks have detected a variety of techniques used to compromise and steal data (intellectual property) from organizations in key industries spanning critical infrastructure, enterprises and telecommunications. Source: https://www.helpnetsecurity.com/2018/03/23/exfiltration-techniques/

Researchers Find 29 Types of USB Attacks, Recommend Never Plugging into a USB You Don't Own – If you ever find a lost charger, don't use it. If you need power and are tempted to plug into a public USB port, don't do it. It's long been known that you should never insert an unknown USB drive to your computer because it could be loaded with malware. However, new research from Ben-Gurion University has exposed 29 types of USB attacks, and it extends to your smartphone. It shows that you should never use a USB charger you find lying around or plug into a public USB port. Both can be compromised by attackers… Source: https://www.techrepublic.com/article/researchers-find-29-types-of-usb-attacks-recommend-never-plugging-into-a-usb-you-dont-own/

Preventing Business Email Compromise Requires a Human Touch – The FBI's Internet Crime Complaint Center (IC3) declared Business Email Compromise (BEC) the "3.1 billion dollar scam" in 2016, an amount which then grew in the span of one year into a "5 billion dollar scam." Trend Micro now projects those losses in excess of 9 billion dollars. It's an understatement to say BEC scams and the resulting damages are on the rise. But with cybersecurity spending across all sectors at an all-time high, how is such an unsophisticated threat still costing otherwise well-secured organizations billions of dollars? Unlike the numerous types of attacks that incorporate malware, most BEC scams rely solely on social engineering. In fact, its use of trickery, deception, and psychological manipulation rather than malware is largely why BEC continually inflicts such substantial damages. Source: https://www.securityweek.com/preventing-business-email-compromise-requires-human-touch

Web/Internet Threats

GitHub Hit With the Largest DDoS Attack Ever Seen – GitHub has revealed it was hit with what may be the largest-ever distributed denial of service (DDoS) attack. The first portion of the attack against the developer platform peaked at 1.35Tbps, and there was a second 400Gbps spike later. This would make it the biggest DDoS attack recorded so far. Until now, the biggest clocked in at around 1.1Tbps. Source: http://www.zdnet.com/google-amp/article/github-was-hit-with-the-largest-ddos-attack-ever-seen/

Mobile Banking Trojans Spread Confusion Worldwide – Consumers around the world that use mobile banking apps are at a greater risk of being tricked by cybercriminals and falling victim to mobile banking theft. This is according to new global research from Avast, which asked almost 40,000 consumers in Spain and eleven other countries around the world to compare the authenticity of official and counterfeit banking application interfaces. Source: https://www.helpnetsecurity.com/2018/02/27/mobile-banking-trojans-spread-confusion-worldwide/

Powerful New DDoS Method Adds Extortion – Attackers have seized on a relatively new method for executing distributed denial-of-service (DDoS) attacks of unprecedented disruptive power, using it to launch record-breaking DDoS assaults over the past week. Now evidence suggests this novel attack method is fueling digital shakedowns in which victims are asked to pay a ransom to call off crippling cyberattacks. Source: https://krebsonsecurity.com/2018/03/powerful-new-ddos-method-adds-extortion/

This Android Malware Redirects Calls You Make to Your Bank to go to Scammers Instead – Malware helps scammers trick you into thinking you're speaking to your bank. Researchers at Symantec are warning of a new variant of the Fakebank Android malware family that has an unusual twist. Once installed the malware will intercept mobile calls you attempt to make to your bank, and instead direct them to a scammer impersonating an agent working for the bank. Furthermore, the malware will intercept calls from the *scammers*, and display a fake caller ID to make it appear as though the call is really from the legitimate bank. Source: https://www.grahamcluley.com/this-android-malware-redirects-calls-you-make-to-your-bank-to-go-to-scammers-instead/

Data Breaches

More Than Half of Surveyed Companies Breached in 2017 – More than half of surveyed companies – many with underbudgeted, overwhelmed cybersecurity initiatives – suffered a breach one or more times in 2017, according to new research from Boston-based Cygliant. The hybrid security-as-a-service firm gathered its findings from a study conducted in late 2017 and early 2018. The survey reached more than 165 IT and security professionals at medium-sized companies, including more than 20% from the finance sector (more than any other industry) across the country for Cygliant's Q1, 2018 Cybersecurity Survey. Source: https://www.cutimes.com/2018/03/02/more-than-half-of-surveyed-companies-breached-in-2/

Most Healthcare Breaches Still Come From Hacking – In 2017 the number of individuals affected by breaches within the healthcare sector reached a four-year low. However, 71 percent of breaches in 2017 were due to hacking and IT incidents, a growing proportion growth trend that continued since 2014, according to the Bitglass 2018 Healthcare Breach Report. Source:
https://www.helpnetsecurity.com/2018/03/05/bitglass-2018-healthcare-breach-report/

Frost Bank Announced it Has Suffered a Data Breach That Exposed Check Images – On Friday, Frost Bank announced that it has suffered a data breach that exposed check images, crooks could use them to forge checks. Frost Bank announced on Friday that it has suffered a data breach that exposed check images. The bank is a subsidiary of Cullen/Frost Bankers, Inc., its staff discovered an unauthorized access to its systems containing images of checks. Attackers compromised a third-party lockbox software program, in this way they were able to access the images of checks stored electronically in the database. Source: http://securityaffairs.co/wordpress/70468/data-breach/frost-bank-security-breach.html

Why You Should Never Pay a Ransomware Ransom – A ransomware infection can be a very, very scary situation to deal with. Many victims aren't sure what to do next when ransomware hits. There's one thing that you should never do, and that is pays the ransom. That's a point that cybersecurity experts have been trying to drive home ever since ransomware first started infecting computers. When faced with the frightening reality that treasured family photos or essential business documents have been encrypted, however, not everyone follows that advice. Source:
https://www.forbes.com/sites/leemathews/2018/03/09/why-you-should-never-pay-a-ransomware-ransom/#55ac147d1753

Threat Landscape

Your Entire ID is Worth £820 to Crooks on Dark Web Black Market – Fraudsters operating on the dark web could buy a person's entire identity ("fullz" in the cybercrook lingo) for just £820. Bank account details, Airbnb profiles and even Match.com logins are worth money to bidders that reside on the murkier side of the internet, a study by virtual private network comparison site Top10VPN.com found. Source: http://www.theregister.co.uk/2018/03/08/dark_web_market_price_index/

World's Biggest DDoS Attack Record Broken After Just Five Days – Last week, the code repository GitHub was taken off air in a 1.3Tbps denial of service attack. Arbor Networks is now reporting that a US service provider experienced a 1.7Tbps attack earlier this month. In this case, there were no outages as the provider had taken adequate safeguards, but it's clear that the memcached attack is going to be a feature network managers are going to have to take seriously in the future. Source: http://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days/

So Much for Mac Is More Secure than Windows: macOS Malware Increased by 270% – macOS is generally referred to as a more secure alternative to Windows 10 because, as some people say, Apple's operating system can't be infected by viruses. This isn't only completely false, but simply comparing Windows and macOS in terms of security these days no longer makes so much sense, as both platforms are being attacked by a growing number of malware. Source: http://news.softpedia.com/news/so-much-for-mac-is-more-secure-than-windows-macos-malware-increased-by-270-520171.shtml

Boeing's WannaCry Run-In is a Reminder to Patch Your Systems – WannaCry is making headlines again, and this time it hit a major target: Boeing. The aerospace company quickly contained the infection, which only spread to a couple dozen computers. "Our cybersecurity operations center detected a limited intrusion of malware that affected a small number of systems. Remediations were applied and this is not a production or delivery issue," the company said in a statement. Boeing isn't offering details about the attack, but said initial reports about a devastating attack were "overstated and inaccurate." Only computers with Boeing's commercial airline business were affected; the company's defense and services lines were not. Source: http://www.foxnews.com/tech/2018/03/30/boeings-wannacry-run-in-is-reminder-to-patch-your-systems.html

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.

- Ensure that your institution is aware of its requirements under GDPR and that it is taking the necessary steps for compliance if necessary.
- Ensure that your web filtering system can be dynamically updated against current threats
- Keep anti-virus systems up to date.
- Talk to your security vendors to ensure that they don't rely on Whois lookups for validation or attribution.
- Ensure that your internal and external systems are not using IoT devices.
    1. This should also include items such as door sensors and cameras
- Inform employees about number port out scams to help them protect against this type of attack.
- Discuss MailChimp domains with your email filtering provider to determine appropriate levels of filtering.
- Ensure that your vendor management and supply-chain management policies are up to date, and audited regularly.
- Update your policies on the usage of USB drives, and educate your staff about the dangers of USB drive usage.
- Make sure that your security awareness training includes specific protections against Business Email Compromise (BEC).
- Talk to your ISP about DDoS Protections
- Make sure that your website gets tested regularly as a component of your external penetration testing.
- Explore the use of password management software for users such as "Last Pass" to assist with password security.
- Make sure that your incident response playbook is updated regularly to address the latest threats.

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.

According to the 2017 Identity Theft Resource Center (ITRC) report, 48% of data breaches were caused by Phishing Attacks. A recent study found that 78% of people claim to be aware of the risks of unknown links in emails. And yet they click anyway.

The Odds…

Getting bitten by a Shark
1 in 1.635 Million

Making a hole in one
1 in 12,500

Catch a foul ball
1 in 680

Experiencing a Data Breach
1 in 4

Considering the odds, is your institution prepared to properly respond to security incidents? Accume can help!