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: Time for a better mousetrap

If your institution uses **Microsoft Exchange 2013** or newer, be aware that there is a new vulnerability that requires attention. Hackers have been able to leverage an NTLM authentication function to perform relay attacks using the Exchange Web Services (EWS) interface. A successful attack could gain domain user administrator privileges. There is NO PATCH, but Microsoft does have some work-arounds.

Email authentication usage is growing, but not fast enough, according to a recent survey. Many organizations remain exposed because they are not using available solutions that can prevent the distribution of fake emails. Considering that 70% or more of incidents begin with a phishing attack, it would seem that email authentication would be a welcome addition for security controls, but adaption is slow in many sectors. Make sure that your institution is leveraging DKIM or DMARC

SMS social engineering attacks (SMiShing) is on the rise. This is another attempt at bypassing corporate security controls by trying to socially engineer users into providing account information or other data points for nefarious purposes. While it is important to ensure that your employees do not fall victim of this type of attack, it may be of value to warn and educate your customers as well so that their trust in your institution is not leveraged against them.

Hospitals have seen a decrease in ransomware attacks recently, but that is not due to them dropping off of the radar. It is due to a shift to more subtle attack methods that allow the attackers to harvest data. New techniques include key logging, lateral movement across the network and advanced reconnaissance to gain entry to higher value assets on the network. These same techniques can be applied to businesses of all types, so it is essential that security teams remain vigilant

Last month a massive set of hacker data called "**Collection #1**" is a set of email addresses and passwords totaling 2,692,818,238 rows found on the cloud service MEGA last week. It represents correlated data taken from previous breaches. There are 1,160,253,228 unique combinations of email addresses and passwords in the data set. The unique email addresses totaled 772,904,991, and there are 21,222,975 unique passwords. This represents a high risk because credential stuffing attacks. https://haveibeenpwned.com/Passwords can help users: they can type in their old password to see if it's shown up on the dark web, and they can validate any attempted new password to ensure it's not on any current list of compromised passwords likely to be reused.

Bob Gaines
Director
Cybersecurity & Privacy
425-518-1974
rgaines@accumepartners.com

AccumeView: Executive Cybersecurity Pulse

Security News

The Attack Surface is Growing Faster Than It Has at Any Other Point in the History of Technology – Avast launched its annual Threat Landscape Report, detailing the biggest security trends facing consumers in 2019 as collected by the Avast Threat Labs team. We foresee the emergence of a class of attacks known as 'DeepAttacks', which use AI-generated content to evade AI security controls. In 2018, the team observed many examples where researchers used adversarial AI algorithms to fool humans. Examples include the fake Obama video created by Buzzfeed where President Obama is seen delivering fake sentences, in a convincing fashion. Source: https://www.helpnetsecurity.com/2019/01/07/avast-threat-landscape-report/

Email authentication use growing steadily in every industry sector - U.S. federal government agencies and many major enterprises have made significant strides to thwart the spread of fake emails, a major cybersecurity attack vector. But many organizations remain susceptible because they're still not using readily available open standards-based technologies that prevent these fakes from reaching end-user inboxes. Valimail's "Email Fraud Landscape, Q4 2018" indicates that the fight against fake email is advancing around the world — but email fraud remains a widespread and pernicious problem. Source: https://www.helpnetsecurity.com/2019/02/04/email-authentication-use-growing/

Hackers carried out a massive cyberattack on Russian Banks – The hacker group Silence made about eighty thousand malicious mailings to employees of Russian Banks reports Group-IB. This marks the first major cyber-attack on credit and financial institutions since the beginning of the New Year. The malicious emails contained an invitation to join a financial forum with a malicious attachment containing TrueBot malware known to be used only by Silence. These attacks follow a series of attacks performed by Silence on Russian Banks at the end of 2018. Source: http://www.ehackingnews.com/2019/01/hackers-carried-out-massive-cyberattack.html

Regulatory and Privacy News

GDPR Compliance Lowers Data Breach Frequency and Impact Says Report - As reported by Cisco in its Data Privacy Benchmark Study, companies that follow the requirements of the General Data Protection Regulation (GDPR) experience benefits such as lower frequency and effect of data breaches, as well as fewer records being impacted in the attacks, shorter downtimes and lower overall costs. The report used the data collected via a double-blind survey which was answered by over 3200 security professionals from 18 countries from all over the world and from all major industries. Source: https://www.bleepingcomputer.com/news/security/gdpr-compliance-lowers-data-breach-frequency-and-impact-says-report/

Proposed N.C. Bill Would Require Ransomware Disclosures – Josh Stein, North Carolina Attorney General, released a report highlighting the impact of data breaches in North Carolina in 2018. The report was paired with a bill to strengthen breach notifications to include ransomware attacks. Under the new bill, organizations would have to report ransomware attacks to affected individuals and the state attorney general's office within 30 days. In 2018, organizations in North Carolina reported more than 1,057 data breaches to the attorney general's office, affecting more than 1.9 million residents in North Carolina, a state with just over 10 million people. Source: https://www.meritalk.com/articles/proposed-n-c-bill-would-require-ransomware-disclosures/

HIPAA: Open Season for Comments - The Office for Civil Rights is now seeking comments on whether certain aspects of the HIPAA privacy and security rules should be modified. The Request for Information is purely a solicitation of comments and ideas from the public on whether or how HIPAA could be modified. That being said, the request is not without any parameters. The request follows similar requests from other agencies within the Department of Health and Human Services seeking to determine whether regulations should be modified to encourage or enable the transition to value-based care. While those requests made more apparent sense in connection with fraud and abuse laws, the same does not necessarily hold true for HIPAA. Source: https://www.hitechanswers.net/hipaa-open-season-for-comments/

AccumeView: Executive Cybersecurity Pulse

Social Engineering

Don't Get Caught in a SMiShing Scam - The word 'SMiShing' may sound like gibberish — we think it's a weird one — but some of the world's largest enterprises are losing millions of dollars to these scams every year. Similar to phishing, the fraudulent act of sending imitation emails claiming to be a corporation in order to obtain personal information from customers, SMiShing uses SMS (short message service) to achieve the same outcome. Scammers are taking to SMS to prey on people's trust, panic or sense of urgency. These messages are disguised as a warning from your bank about an unauthorized charge or an alert about an unidentified user accessing one of your accounts. Source: https://www.tripwire.com/state-of-security/security-awareness/caught-smishing-scam/

Employees report 23,000 phishing incidents annually, costing $4.3 million to investigate - In a survey of more than 300 businesses in the U.S. and U.K., Agari determined that employees at the average company report 23,053 phishing incident reports per year—yet 50 percent are false positive reports. Responding to a phishing incident takes an average of 353 minutes (almost six hours); and even false positives take an average of 238 minutes (four hours). All of these reports and hours add up—at a cost of $253 per phishing incident—or more than $4.3 million per year in SOC costs to required to triage, investigate and remediate phishing incidents. Source: https://www.helpnetsecurity.com/2019/02/01/phishing-incidents-investigation/

Hackers Using Zero-Width Spaces to Bypass MS Office 365 Protection - Security researchers have been warning about a simple technique that cybercriminals and email scammers are already being using in the wild to bypass security features of Microsoft Office 365, including Safe Links, which are originally designed to protect users from malware and phishing attacks. Safe Links has been included by Microsoft in Office 365 as part of its ATP (Advanced Threat Protection) solution that works by replacing all URLs in an incoming email with Microsoft-owned secure URLs. Therefore, every time users click on a link provided in an email, Safe Links first sends them to a Microsoft owned domain, where it immediately checks the original link for anything suspicious. If Microsoft's security scanners detect any malicious element, it then warns the users about it, and if not, it redirects them to the original link. Source: https://thehackernews.com/2019/01/phishing-zero-width-spaces.html

Internal Threats

Attackers scanning unpatched Cisco small business routers after exploit code published - Cisco Systems last week issued security advisories for two dozen vulnerabilities, including two high-severity flaws in its Small Business RV320 and RV325 dual gigabit WAN VPN routers, which attackers are reportedly already trying to exploit with published proof-of-concept code. Source: https://www.scmagazine.com/home/security-news/vulnerabilities/attackers-scanning-unpatched-cisco-small-business-routers-after-exploit-code-published/

You're an admin! You're an admin! You're all admins, thanks to this Microsoft Exchange zero-day and exploit - Microsoft Exchange appears to be currently vulnerable to a privilege escalation attack that allows any user with a mailbox to become a Domain Admin. On Thursday, Dirk-jan Mollema, a security researcher with Fox-IT in the Netherlands, published proof-of-concept code and an explanation of the attack. Source: https://www.theregister.co.uk/2019/01/25/microsoft_exchange_domain_admin_eop/

A vulnerability in Microsoft Office allowed documents with embedded ActiveX controls to leak user information, including sensitive information like passwords – A vulnerability in Microsoft office discovered by Israel based company Mimecast in November allowed documents with embedded ActiveX controls to leak user information including sensitive information like passwords. Microsoft confirmed the vulnerability, stating that it impacts Office 2010, Office 2013, Office 2016, Office 2019, as well as Office 365 ProPlus. Patches have already been released for all listed products. Source: https://news.softpedia.com/news/microsoft-office-vulnerability-exposes-user-data-including-passwords-524496.shtml

Bypassing Network Restrictions Through RDP Tunneling - FireEye has observed threat actors using native Windows RDP utilities to connect laterally across systems in compromised environments. Historically, non-exposed systems protected by a firewall and NAT rules were generally considered not to be vulnerable to inbound RDP attempts; however, threat actors have increasingly started to subvert these enterprise controls with the use of network tunneling and host-based port forwarding. Source: https://www.fireeye.com/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html

AccumeView: Executive Cybersecurity Pulse

Web/Internet Threats

Trojan Malware Tops Ransomware as Biggest Hacking Threat to Healthcare - Trojan malware upended ransomware as the greatest hacking threat to the healthcare sector in 2018, according to a new report from Malwarebytes Labs. Specifically, Emotet and Trickbot hacking trojans were the most common malware strains, while hijackers, rootkits, and riskware rounded out the top threats to the sector. According to the report, the number of trojan attacks have increased by 132 percent since 2017. The report found hackers are steering away from the obvious ransomware attacks that provide only short-term payments and into the subtler, long-lasting trojan attacks to harvest intellectual property, personal data, and more. Source: https://healthitsecurity.com/news/trojan-malware-tops-ransomware-as-biggest-hacking-threat-to-healthcare

Imperva mitigated DDoS attack generated 500 Million Packets per Second, the largest ever - Earlier this month, the cyber security software and services company Imperva mitigated an attack against one of its clients that exceeded 500 million packets per second. This attack was a SYN flood DDoS and it is the largest DDoS attack by packet volume ever observed. The attacker sent both a flood of normal SYN packets and a large SYN flood using two previously known tools. The attacker used highly randomized and likely spoofed set of source ports and addresses to send packets of between 800 and 900 bytes. Source: https://securityaffairs.co/wordpress/80492/hacking/ddos-500m-pps.html

Advertising network compromised to deliver credit card stealing code – A Paris-based online advertising company was hacked, and its infrastructure used to deliver malicious JavaScript code to online stores. The code was designed to steal payment card details entered by users into checkout pages. The hack took place last year, around November 2018, when a cybercriminal group compromised the content delivery network of Adverline, a French company that runs an advertising network with a predominantly EU clientele. The Adverline compromise was first detected by security researchers from Trend Micro and is being referred to as a Magecart or card skimming attack. Source: https://www.zdnet.com/article/advertising-network-compromised-to-deliver-credit-card-stealing-code/

Last year, **71 percent of all targeted attacks** started with **spear phishing**—the oldest trick in the book—to infect their victims.

Data Breach

Palisades Park officials say nearly $500,000 is missing from its accounts in bank breach - Officials in Palisades Park were notified last week that nearly half a million dollars had been drained from its accounts at Mariner's Bank, the borough's mayor and business administrator said Wednesday. Mariner's Bank, which is based in Edgewater and has seven locations in Bergen County, told the officials that $460,000 was missing from the borough's accounts as a result of a fraudulent wire transfer, said Dave Lorenzo, the borough administrator. Source: https://www.northjersey.com/story/news/bergen/palisades-park/2019/01/30/palisades-park-nj-officials-nearly-500-000-missing-bank-breach/2726275002/

Hacker Steals 10 Years' Worth of Data From San Diego School District – A hacker has stolen the personal details of over 500,000 San Diego Unified School District staff and students; the district revealed in a breach notice posted on its website on Friday, before the Christmas holiday. The breach occurred because the attacker gained access to staff credentials via a phishing attack. The attack didn't go unnoticed. Some staff reported the funny-looking emails to IT staff, who investigated and eventually discovered the breach in October this year. District officials said the hacker had access to its network between January 2018 and November 1, 2018, but that he stole student and staff data going back to the 2008-2009 school year. Source: https://www.zdnet.com/article/hacker-steals-10-years-worth-of-data-from-san-diego-school-district/

Collection 1 data breach: what you need to know – Last week, news broke that the largest data dump in history had been discovered, with more than 770 million people's Personally Identifiable Information (PII) decrypted, catalogued, and up for grabs on the Internet. The files, which are being dubbed Collection 1, contains more than 12,000 files and is a whopping 87 gigabytes large. While on paper this sounds beyond alarming, the truth is much more nuanced. The collection is composed of data pulled together from multiple breaches and leaks, many of which contain email addresses and passwords that are at least two to three years old. While much of the data is stale, it can be used successfully in phishing and extortion campaigns. The mere mention of a correct password, even if it's outdated, could coax unsuspecting users into giving up fresh PII or paying ransoms. Source: https://blog.malwarebytes.com/101/2019/01/collection-1-data-breach-what-you-need-to-know/

AccumeView: Executive Cybersecurity Pulse

Vulnerabilities and Indicators of Compromise

- Weekly Vulnerability Summary from US-CERT
- Talos Threat Roundup for January (1) (2)
- GandCrab Ransomware Helps Shady Data Recovery Firms Hide Ransom Costs
- ExileRAT shares C2 with LuckyCat, targets Tibet
- Flaw in SS7 Lets Attackers Empty Bank Accounts
- Remote Hardware Takeover via Vulnerable Admin Software
- Info-Stealing FormBook Returns in New Campaign
- AMP tracks new campaign that delivers Ursnif
- Chinese Hacker Publishes PoC for Remote iOS 12 Jailbreak On iPhone X
- New WhatsApp bug may have been discovered, exposes message history in plain text
- New Systemd Privilege Escalation Flaws Affect Most Linux Distributions
- New WhatsApp bug may have been discovered, exposes message history in plain text
- New Systemd Privilege Escalation Flaws Affect Most Linux Distributions
- New tool automates phishing attacks that bypass 2FA
- Shipping Firms Speared with Targeted 'Whaling' Attacks
- New side-channel leak: Boffins bash operating system page caches until they spill secrets
- Analysis of the latest Emotet propagation campaign

Recommended Actions to Take

- If you have an exposed Cisco Router (RV320 and RV325), change your router's admin and WiFi credentials and consider yourself already compromised: take action as necessary to ensure your local and perimeter security
- If you are concerned about GDPR, now is the time to ensure compliancy or validate that your institution does not fall under the GDPR regulatory umbrella
- If you host an exchange server, read the current advisory and take action
- Inform staff as needed about new phishing and social engineering campaigns
- Check to see if your web filters can detect decryption or deobfuscating scripts in web pages
- Audit your firewalls, routers and switches and wireless networks annually
- Ensure that you have protections in place for mobile users
- Update the firmware on your routers as necessary
- Investigate blocking IP blocks from countries your institution does not do business with as an additional form of protection
- Keep systems patched and up to date
- Consider the implementation of annual threat hunting exercises

Infographic of the Month

Source: Gemalto Breach Level Index, **http://breachlevelindex.com/**

AccumeView: Executive Cybersecurity Pulse

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.

Cybersecurity Lessons Learned in 2018 & Projections for 2019

Join us on Wednesday, February 13th at 12PM ET!
Don't Miss This Special Webinar!

Accume's next webinar will cover the following topics:

- What were the key lessons learned in the area of Cybersecurity in 2018?
- What were the key lessons Accume clients learned in the area of Cyber Incident Response?
- What do we predict to be the key attack vectors in 2019?
- What are the low cost/high return activities that businesses should invest in today?

Hear from the following subject matter expert:

- **Robert Gaines, CISSP, CFSA**, Director, Technology Risk, IT Audit & Cybersecurity

We look forward to your attendance and providing you with guidance to assist your organization's readiness for upcoming Cybersecurity challenges.

We will announce a special service promotion during the presentation for our Webinar attendees!

Register Now