Cyber Roundup – December 2020

By Thomas J. DeMayo, Principal, Cyber Risk Management

If you didn't realize this before, cyber criminals have unlimited felonious imaginations and unmitigated gall, this issue of *Cyber Roundup* will certainly confirm that. Whether using the key fob on a Tesla to open it or actually advertising on Facebook that they are waiting for ransom payment, cyber criminals pose an enormous threat to businesses and individuals. What can you do to avoid victimhood? While there are no guarantees, the team at PKF O'Connor Davies can help your company put together a plan to protect your computer infrastructure and help you develop a strategy in the event your system is compromised. Contact me today so we can get started.

Key Cyber Events

The following is a rundown of what happened during the month of November 2020. We welcome your comments, insights and questions.

- **The FBI, in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), issued guidance on how to avoid becoming a victim of holiday shopping scams.** We encourage you to read the article here.

- **In an interview by CNBC with the SEC Chairman, Jay Clayton, the Chairman made it clear that cybercrime remains a primary threat and organizations must remain vigilant.** In recent months, the SEC has been actively releasing alerts on key threats that businesses must be aware of; specifically, Ransomware and Credential Stuffing.

- **In a report by Helpnetsecurity.com they noted that in Q2 2020, phishing and fraudulent sites created and hosted increased to 1.7 million, a 13.3% increase from Q1 2020.** An average of 18,000 fraudulent sites were created each day. In an unrelated report by Abnormal Security, they noted an increase in business e-mail compromise (BEC) attacks by 155%. BEC attacks are those in which fraudulent payment instructions are received by way of e-mail to divert funds.

  Tom's Takeaway: As we come into the holiday season and move into a second wave of the pandemic, the concerns echoed by the SEC Chairman need to be heeded. Such concerns are supported by the metrics demonstrating the increase of cyber attacks over the past year. Cybersecurity is often considered a non-issue until an incident occurs. It's only when an issue occurs that many businesses begin to fully understand the implications of a cyber attack on their businesses. While you can never ensure that a cyber incident won't occur, you can do your best to protect against it. In order to protect against that threat, you need to first understand it. Please call us if you need help in understanding your cyber risk and effectively managing it.

- **In a closed underground forum, a threat actor has been identified as selling the compromised credentials of C-Suite executives for Office 365 accounts.** The price for the accounts range from $100 to $1,500 depending on the company's size and the specific role of the executive.

- **Spotify, the audio streaming service, reported that approximately 300,000 accounts were impacted as a result of a credential stuffing account.** Credential stuffing is when the cyber criminals utilize databases of known breached passwords to target user accounts. Spotify has forced a password reset for all of the impacted accounts.

  Tom's Takeaway: Credentials will continue to be compromised and sold in various forums. The only effective way to protect yourself is to embrace multi-factor authentication across any remote

access account that you have. Once you embrace multi-factor authentication, the criminals will only have one piece of the necessary pair to access your information.

- **Security researchers identified an exploit that would allow a Tesla Model X to be hacked and stolen by leveraging a vulnerability in the key fob design.** Effectively, the researchers identified that they could manipulate the software installed on the key fob to obtain the necessary unlock messages to access the car. Tesla has since fixed the issue with a software update.

- **Security researchers identified a mechanism to turn a smart vacuum cleaner into a listening device that can record conversations in the room.** The researchers leveraged LIDAR technology to pull off the hack. LIDAR is a technology that allows for the mapping of a room using light detection and ranging. Using this technology, they were able to capture sound waves and translate that back into conversations or noises in the room.

- **Ransomware continues to be a major threat to all entities.** Below is a summary of the businesses impacted by ransomware in November 2020.

  - Managed.com, a large managed web hosting provider, suffered a ransomware attack. The attack impacted the company's public-facing web hosting system and encrypted customer data. Manage.com has currently stated that only select customers have been impacted but took down the entire platform to help contain the incident.

  - Delaware County, PA suffered a ransomware attack on its encrypted key system and data repositories. The cyber criminals demanded $500,000 to unlock the files and give control back to the County. The County does have cyber insurance and was in the process of paying the ransom.

  - Mattel, the global toymaker, suffered a ransomware attack. The disclosure of the incident was made as a result of the SEC filings of the company. The filings note that the attack had minimal impact on the company and was successfully mitigated

  - K12, an online education provider, reported a ransomware attack that impacted the company's back office systems that included employee and student information. The attack did not impact the online programs and its learning management system. K12 was in the process of paying the ransom to regain control of their systems and prevent any potential disclosure of data.

  - The City of Saint John, Canada, suffered a ransomware attack that brought down the entire network, impacting key systems including the website, online payment systems, and e-mail.

- **Security Researchers discovered ransomware variants that have been modified to find and target tax software such as TurboTax.** Cyber threat intelligence analysts from Digital Shadows noted that the trend of targeting individual and business tax programs and filings is increasing. Once found, the criminals may attempt to encrypt and exfiltrate the data to place additional pressure on the victims to pay.

- **The ransomware gang, Ragnar Locker, audaciously posted Facebook ads to remind its victim that it needs to pay.** This was specifically noted in their attack against the Campari Group. Using stolen credentials to pay for Facebook ads, targeted campaigns were launched against Campari Group employees to remind them that the group stole around 2 terra bytes of data and unless they pay, the information will be posted publicly.

  Tom's Takeaway: Four years ago when we started *Cyber Roundup*, ransomware was a blip on the radar of cyber events. Back then, data breaches were the prime topic. Over the past year, ransomware has dominated our monthly cyber newsletter. We can't stress enough that this is a very serious risk to every business – a risk that could very well end your business if not taken seriously. The ransomware gangs do not discriminate. We encourage you to ensure that you have the necessary protections not only to defend, but recover from a ransomware attack. As a board member or a member of senior management, you are encouraged to look for that assurance from an unbiased third party. Don't wait until an incident hits to learn about the company's weaknesses.

Contact Us

The pandemic has thrust upon the world many changes for better or for worse. As a business, this is a time to really step back, evaluate your current technical and data landscape, and make sure you are positioned to come out of this better, stronger, and more efficient. The good news is you don't have to do it alone. At PKF O'Connor Davies, we have the resources to help you navigate your path forward across all facets of your business. We encourage you to contact us **today** as you continue down that path of success.

Thomas J. DeMayo, Principal, Cyber Risk Management
CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE

PKF O'Connor Davies, LLP
665 Fifth Avenue, New York, NY, 10022
212.867.8000 or 646.449.6353 (direct)
tdemayo@pkfod.com

www.pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, twelve offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 800 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 27th on *Accounting Today*'s 2020 "Top 100 Firms" list. It is also ranked among the top 20 best accounting employers to work for in North America by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.