Cyber Roundup – May 2020

By Thomas J. DeMayo, Principal, Cyber Risk Management

As we continue the COVID-19 lockdown, we realize how truly dependent we are on our cyber connections… from ordering food, to entertainment, to schooling and even virtually attending religious services. Since the March issue of our *Cyber Roundup*, I have been working closely with clients to ensure their cybersecurity needs in these circumstances. In this issue, I will catch you up with what's going on in cyberland.

Word of caution: While all industries are monitoring the economic implications of the pandemic and reviewing cost-cutting strategies, be cautious in the areas you plan to reduce spending. Cybercriminals are banking (no pun intended) on a reduction in defenses. While there may certainly be room to optimize cybersecurity strategies, aggressive cuts in this area could very well undermine the very business you are trying to save. As always, if you need assistance in evaluating and navigating the cybersecurity challenges during this time, please feel free to contact us.

Key Cyber Events

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

- **Ransomware attacks continue to surge.** In a survey conducted by Infrascale, 46% of the respondents were successfully targeted and victimized by a ransomware attack with 73% of those victimized paying the ransom. The survey was targeted to the small- to medium-sized market. In a separate study by Coveware, they noted that ransomware payments have increased 33% in the first quarter of 2020, hitting a new average payment of $111,605, up from an average of $33,000 in the 4th quarter of 2019. The following is a summary of the most recent ransomware attacks:

  - **The NJ Trenton Police Department suffered its second cyberattack in six months.** In the midst of the pandemic, the police department was victimized by a ransomware attack disrupting operations. The extent of the damage has not yet been made public.

  - **The City of Durham, North Carolina, suffered a ransomware attack that took down the public safety phone networks.** The attack resulted in the shutdown of the 911 call center as well as the Fire Department's phone service.

  - **The U.S. Cybersecurity Infrastructure and Security Agency and the U.K. National Cyber Security Center issued alerts that various cybercriminal gangs are targeting COVID-19 healthcare treatment and research centers.** The research centers were identified as being targeted by nation state actors as part of espionage efforts. The hospitals and other treatment facilities are being targeted by those hoping for a quick payment as staff need urgent access to the systems while patient cases increase. These warnings came after initial "chatter" in the dark web was identified among select cybercriminal groups.

  - **Insurance firm Chubb and the U.K.-based drug testing firm Hammersmith Medicines Research were both impacted by the Maze ransomware variant.** Unlike traditional ransomware that would simply encrypt the files, the Maze ransomware operators also extract data from the infected companies and threaten to publish the stolen files of their victims on the internet if they do not pay. Often, they will publish small amounts of data at first to further encourage payment before releasing all data.

- **A Colorado Hospital, Parkview Medical Center, suffered a ransomware attack in the midst of their treating COVID-19 patients.** The hospital was forced to leverage paper files as they worked to recover.

- **Over 1,000 publicly-registered companies listed ransomware as a credible and future risk in their SEC filings.** Ransomware is being listed by the companies in their 10-K, 20-F, 10-Q, 8-K, 6-K and S-1 filings. By reporting to investors the risk of ransomware, they are acknowledging that a ransomware attack could result in the company incurring substantial losses.

Tom's Takeaway: Through the good times and the bad, one thing is certain, the cyber threat is not going away. Fear, uncertainty and doubt are the prime ingredients cybercriminals look for to leverage their schemes. The pandemic has created the perfect storm in its global impact, removing localized limitations and leveraging an incident that impacts us all, expanding the number of potential victims.

- **Thousands of Zoom voice recordings have been identified as being exposed across the internet.** The recordings ranged from business meetings, classroom instruction, to medical consultations. The recordings were typically identified as being stored by the various users of the platform in publicly accessible AWS containers. The issue was identified as a result of Zoom saving recorded sessions in an identical pattern. With a known pattern, the internet can easily be searched for that pattern to identify the exposures.

Tom's Takeaway: In this incident, it is easy to focus on Zoom as the root cause given their recent bad press; however, do not misinterpret this issue as solely a Zoom issue, but take it for what it is: user companies stored the recordings in improperly restricted internet accessible locations. I have received a lot of questions regarding the security of Zoom. While Zoom was certainly not perfect from a security perspective, I think the response of Zoom to those findings has warranted giving it a chance to correct them. Over the next month or so as Zoom continues to focus on security improvements, I think a more permanent determination can be made in the coming months on the continued usage of Zoom, after it completes its 90-day commitment to only focusing on security enhancements.

- **SOS Online Backup, a cloud-based backup provider that claims to be "The World's Most Secure Online Backup," exposed 135 million records as a result of incorrectly configured database.** The exposed data consisted of names, usernames, phone numbers, e-mail addresses, and account-specific data. It is not known if the database was accessed by any cybercriminals looking to leverage the data.

Tom's Takeaway: Just as beauty is in the eye of the beholder, so is security these days. Every business now offers a "secure" solution. While it is easy to claim to be secure and with enough "makeup" to appear to be secure; more often than not, it is an illusion. The only way to gain comfort with a vendor you are trusting with your data is through proper due diligence, both operational and security. If you need assistance in how to create a vendor due diligence program or to perform the vendor due diligence on your behalf, please contact us.

- **The FBI issued an alert that cyber criminals are mailing by way of USPS malware infected USB drives.** The hackers will often include additional items like teddy bears or gift cards with the infected drives. One of the tactics was to emulate a Best Buy gift card with a note that the USB drive needed to be plugged in to read the authorized items that can be purchased with the gift card. Although many companies have disabled USB storage devices, these devices do not function as storage, they function as a keyboard tricking the computer. Once connected, the USB drive will execute by way of a virtual key board a series of commands to infect the machine, allowing the cyber criminals into the computer to take control.

- **Walgreens issued an alert that a bug in their app may have resulted in sensitive information, such as names and prescriptions, being disclosed.** Walgreens has since corrected the issue and notified the impacted customers.

Tom's Takeaway: The Walgreens incident serves as a reminder that whenever using any digital system to process our information, we are taking a risk that it may be disclosed. As I have said in many prior posts, every individual needs to be aware of that risk and balance it with the benefit and necessity of the service being provided. I personally use the Walgreens app and knowingly accepted that risk for the convenience it offered; however, more often than not, I will opt out of using any app or the service for the

sake of privacy. The point is: I am in control of that decision because I understand the implications. My hope is that *Cyber Roundup* continues to educate and empower you to make the same informed and balanced decisions.

- **The WHO, CDC, and the Bill and Melinda Gates Foundation – all key players in combating the pandemic – were targeted by a credential dump attack.** The full list consisted of 25,000 e-mail addresses and password combinations. Such usernames and passwords are leveraged to gain remote access to the organizations or extort the employees with e-mails claiming to have infected their machine and stolen their passwords.

Tom's Takeaway: Employee credentials are floating for sale or trade in the dark web for almost every company. While many may be old passwords or belong to former employees, some may not. Cyber criminals primarily use this information in the hope that the password they found may still be used by the individuals and listed across various accounts. Should a more targeted attack occur, as in the above situation, even if the passwords have been changed, an old password can give insight into tendencies a person may use in creating a password, thus increasing the chance of "cracking" the individual's password. While breaches will occur and passwords will circulate, companies should have visibility into their credential exposure. Such insight will allow the company to respond and also can be leveraged to guide their employee training programs. We offer such visibility by way of our Dark Web Monitoring service. Should you be interested in this service and want more information or would like a complimentary report, please contact me.

Contact Us

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 and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today*. In 2021, PKF O'Connor Davies was named one of the 50 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.