Cyber Roundup – March 2020

By Thomas J. DeMayo, Principal, Cyber Risk Management

With the exception of the last bulleted item about the proposed federal Data Protection Agency, this month's edition of *Cyber Roundup* soberly sets out various cybercrimes that are morphing into even more destructive acts, resulting in ever-expanding harm to businesses and individuals. The ingenious evil that allows these cyber criminals to swindle money, wreck reputations and cause chaos speaks to the need for vigilance and to the engagement of professionals to help insulate your IT systems, devices and procedures. In order to succeed in the long-term, vigilance and professional help must be ongoing.
Call us.

We also call your attention to our special e-newsletter on the coronavirus in case you missed it.

Key Cyber Events

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

- **According to the FBI's 2019 Internet Crime Report, available here, business email compromise (BEC) accounted for almost half of reported cybercrime losses in 2019.** Business email compromise is the method used by cyber criminals to trick victims into transferring funds. The tactic is usually accomplished by impersonating a legitimate person or company with which the business has a relationship. In total, the FBI received 467,361 complaints with losses totaling more than $3.5 billion. Approximately $1.77 billion is attributable to BEC.

- **The Puerto Rican government reported that they fell victim to business email compromise that resulted in the loss of $2.6 million.** The money was transferred after an email was received claiming a change to banking information associated with a remittance payment.

Tom's Takeaway: In 2014, BEC losses only accounted for approximately $60 million. On average, since 2014, the amount lost has almost doubled. BEC is not going to disappear any time soon; however, with proper employee training and well-established controls, you can avoid becoming a victim. If you need assistance in this area, please contact us.

- **Cybercriminals have modified their demands in a newly identified ransomware variant.** Instead of asking for money, the variant demands that the victim send them explicit photos in exchange for the decryption key. The variant has been dubbed "ransomwared." At this point, the variant does not appear to be widespread or very sophisticated in design.

- **Five U.S. law firms were reported to have suffered a ransomware attack.** The law firms were all impacted by the same ransomware group, known as Maze. The Maze group will not only encrypt their data, but also steal it. Should the infected firms not pay the ransom, the group will publish the stolen data to their website. Often, small portions of the stolen data will be published at first as proof of having the data in order to further entice the victim to pay.

- **A major vulnerability was identified that placed billions of Wi-FI devices at risk of having the communications exposed to a nearby attacker**. The vulnerability, dubbed Kr00k, exists in Apple and Android devices as well as routers from Asus and Huawei. Manufacturers have made patches available.

Tom's Takeaway: As the number of connected devices will inevitably increase, what will be important is that both businesses and consumers have a process of actively identifying and installing security patches issued by the vendors. This will be true for any connected device, be it your phone, your TV, or your refrigerator.

- **According to the 2020 State of Malware report published by Malwarebytes, the amount of malware identified on Macs has exceeded that of Windows.** The report notes that there was a 400% increase in malware on Mac devices from 2018 to 2019, making the average threat per Mac device 11.9. The average threat per Windows device is 5.8.

Tom's Takeaway: Part of the increase, as noted in the report, is the result of more people installing the malware solution on their Macs. That's actually a positive as it indicates that more people are moving away from the flawed notion that Macs are inherently safe from infection. As we have noted in prior *Roundups*, Macs need an anti-malware solution. If you haven't installed one, it is strongly recommended to do so.

- **A United Kingdom police official recently addressed the SINET Global Cybersecurity Innovation Summit.** This official announced that law enforcement has identified criminal gangs actively placing gang members in cleaning companies to target company IT infrastructure and gain access.

Tom's Takeaway: While this issue is happening in the UK, the risk very much exists globally. If an attacker can gain physical access to your infrastructure, you have given a prime opportunity to allow them to bypass many of the logical controls you may have in-place. When we do our assessments, one of the issues we frequently remind management of is that any individual with access to your space, especially cleaning personnel who operate unattended after hours, creates risk that needs to understood and managed.

- **A Florida police department was forced to drop 11 narcotic cases against six suspected drug dealers after losing a crucial evidence file to a ransomware attack**. Unable to recover the file, including photos and video evidence, the U.S. prosecutors could not proceed with the trial and dropped all charges related to the possession, distribution, and manufacturing of narcotics such as crystal meth and cocaine.

- **MGM Resorts, the casino and hotel chain, reported a breach that resulted in the exposure of 10.7 million guest records.** The data – which included such identifiers as names, email addresses, phone numbers, addresses and dates of birth – have been identified circulating in cybercriminal forums. The hotel chain has stated no financial information was impacted. Select customers have been notified in accordance with applicable state privacy laws.

- **U.S. Senator Kirsten Gillibrand proposed the Data Protection Act in an effort to establish a new federal Data Protection Agency.** The DPA would function as an independent agency with the responsibility of protecting individual's privacy and limit the collection and use of personal data. The DPA director would be appointed by the President and confirmed by the Senate to serve a five-year term.

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 29th on *Accounting Today*'s 2019 "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 2020, 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.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.