Cyber Roundup – February 2021

By Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory

Be wary. Be skeptical. Be proactive. Anything digitalized can be breached, information obtained, and criminal activity pursued. Throughout this month's edition are some tips in dealing with the cyber world. As you will see, the takeaways are based on actual, current, real life events. Like the President not able to bring his Peloton exercise bike into the White House, or the warning about not posting a picture of yourself on the web with your COVID-19 vaccination card, or avoiding the spreading of misinformation by not relying on one single source. And, importantly, advising the authorities of cybercriminal activity of which you become aware (links are below).

Key Cyber Events

The following is a rundown of what happened during the month of January 2021. We welcome your comments, insights and questions.

- **In a report released by Avira, crypto-mining malware increased by 53% in the last three months of 2020.** Crypto-mining malware is designed to leverage the victim's computing power to mine cryptocurrency. When a computer mines cryptocurrency, it performs calculations to try and solve a mathematical problem, consuming the victim's processing power.

  Tom's Takeaway: Crypto-mining malware first appeared and exploded back in 2017 when crypto-currencies started to experience high spikes in value. The past few months emulate that pattern and has again incentivized the cyber actors to re-focus their efforts on the distribution of crypto-mining malware.

- **In 2020, approximately $200 million in fines have been issued as a result of non-compliance with the European Union's General Data Protection Regulation (GDPR), a 39% increase from the prior 20 months.** Some of the largest fines were issued to major names such as H&M, Marriott, and British Airways. GDPR is a privacy regulation designed to ensure appropriate and legitimate processing of European resident personal data.

  Tom's Takeaway: The GDPR regulation went into effect in May 2018. Many of you may remember getting bombarded with updated privacy policies and requests to continue to receive e-mail from vendors at that time. What is often forgotten is that GDPR has implications outside the EU. U.S. businesses that process EU resident data in the course of their operations may also be subject to the legislation and the potentially hefty fines that come along with it. Privacy is a pressing issue that will only ramp up over the coming years. If your business processes personal information in any capacity, if you have not done so already, ensure you have an updated privacy policy and program in place. If you need assistance in how to design and manage your privacy program, please contact us.

- **As the COVID-19 vaccines have begun distribution, the Better Business Bureau issued an alert on an identified trend of the recipients.** Across the various social media platforms, recipients of the vaccine were posting pictures showing their vaccination record cards. While this may seem benign, the BBB is encouraging the public not to do so as the card has various personal information that could be used by scammers.

- **In a coordinated global effort by law enforcement, the notorious Emotet malware infrastructure was taken down.** Emotet was first identified in 2014 and has continued to evolve and increase in sophistication in its stealth, persistence, and malicious capabilities. The original focus of Emotet was to steal credentials and function as a banking Trojan. To quote Europol, "The Emotet infrastructure essentially acted as a primary door opener for computer systems on a

global scale. What made Emotet so dangerous is that the malware was offered for hire to other cybercriminals to install other types of malware, such as banking Trojans or ransomware, onto a victim's computer."

Tom's Takeaway*:* While the bad cyber events often dominate the headlines, it is important to remember that law enforcement is actively trying to manage and deal with the cyber threat. Which is why it is also important that should you be a victim of a cybercrime you report it. While law enforcement won't be able to address every report, the information they obtain can be very valuable in helping them trend and attribute actions to specific cyber actors. Reporting may also allow for the retrieval of stolen funds. To report a cybercrime, file a report with the Internet Crime Complaint Center here. Also, as part of your incident response plan, be sure to include and have a relationship with your local FBI field office which can be found here.

- **In an effort to incite fear and mistrust in the COVID-19 vaccine, stolen regulatory data has been found circulating with altered information.** In December, cyber criminals breached the European Medicines Agency and obtained various confidential documents relating to the evaluation process of the COVID-19 vaccines. The documents were found to be circulating in the dark web with information manipulated in a way to undermine the public's trust in the vaccines.

  Tom's Takeaway: Disinformation is one of the biggest threats society is going to face in the coming years. The power of the internet and social media has such tremendous influence on people's decisions in ways that can pose serious political, economic, and social disasters. As you navigate the web and read articles and view social posts on controversial matters, do so with an open skepticism and don't always rely on a single source.

- **One of the largest dark web carding marketplaces, Joker's Stash, is shutting down.** A carding marketplace is where you can go on the dark web to purchase stolen credit card information. The site first started operating in 2014 and has generated over $1 billion in revenue since then. The exact reason for the close is not clear; however, the operator has left with one piece of advice as quoted on thehackernews.com:

  > "We also want to wish all young and mature ones cyber-gangsters not to lose themselves in the pursuit of easy money (sic)," the post concluded. "Remember, that even all the money in the world will never make you happy and that all the most truly valuable things in this life are free."

- **As President Biden transitioned to the White House, he had to do so without his Peloton bike.** Peloton is an exercise bike that can be connected to the internet and comes with an integrated camera and microphone to allow for the immersive experience that defines the Peloton experience. The concern is that the device is connected to the internet and has the necessary components to facilitate spying on the President should it be hacked.

  Tom's Takeaway: As we have said in many *Cyber Roundups* and at cyber training sessions, **with connectivity comes risk.** What is important is that you understand that risk and make the appropriate decisions on whether you want to accept it, manage it, or walk away from it. The Peloton and the President truly reinforce the issue and the personal decisions to be made. As always, one of the primary goals of *Cyber Roundup* is to keep you informed and also empowered to make the decision that is best for you as it relates to cybersecurity.

- **A misconfigured online database consisting of 320,000 court records has been discovered by a security researcher.** The database appears to have come from an internal court system and contained personal information such as name, address, case numbers and case notes. It is not known who the owner of the database is; however, it appears to have since been corrected.

- **Dating website, MeetMindful.com, suffered a breach of member personal data**. A cybercriminal breached the site and posted approximately 2.28 million member records for download. The data includes name, e-mail address, body details, dating preferences, geo-location, and other sensitive information.

- **Shopify, a popular online shopping app, suffered a breach that disclosed member details, inclusive of their payment information.** Approximately 100,000 purchase details were compromised across 17,000 stores.

- **UScellular, a U.S.-based wireless carrier, reported a breach that resulted in the compromise of personal information and the porting over of cellular numbers.** The cybercriminals targeted employees in the retail stores and tricked them into installing malicious software that gave the cybercriminals remote access to the terminals and the connected CRM system. UScellular has contained the incident and is attempting to retrieve the stolen numbers.

Contact Us

Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory
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, fourteen offices in New York, New Jersey, Florida, 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.