Cyber Roundup – March 2022

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

Cyber criminals certainly rise to the occasion as you will see in this issue of *Cyber Roundup*. They take advantage of wars, the job market, the surging bitcoin phenomenon and matters of the heart. They increase the amenities available from them – like a 24/7 help center, ransomware payment negotiations and assistance with restoration of data.

Let the Cybersecurity team at PKF O'Connor Davies help you fight back on cyber criminality, keep your data safe and secure it from inside and outside bad actors.

Key Cyber Events

The following is a rundown of trends and what's been happening recently in the cyber world. We welcome your comments, insights and questions.

- **Chainalysis, a Singapore software company, through analysis of the block chain, reported an estimated $1.3 billion had been paid to ransomware gangs since 2020.** The analysis was conducted through identification of ransomware payment addresses. Separately, a joint advisory was issued by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Australia and the United Kingdom highlighting the increasing globalized threat of ransomware. A few key points of the report are as follows:

    - Phishing, password brute forcing of Windows Remote Desktop and vulnerability exploitation are the primary mechanisms of infiltration.

    - The cybercriminal services-for-hire business model became more mature and well-established. New tactics of the cyber threat actors were identified as that which "utilized independent services to negotiate payments, assist victims with making payments and arbitrate payment disputes between themselves and other cyber criminals." In addition, a concierge level of service was identified that offered the victims of the services of a 24/7 help center that could facilitate ransom payment and/or assist in the restoration of encrypted systems or data.

    - There was a shift away from "Big Game" U.S. targets. After the attention and retaliation received from the federal government from attacks like the Colonial Pipeline, the cyber threat actors have shifted their attention to smaller businesses to stay below the radar.

    - Ransomware gangs increased their impact by targeting business models that support multiple other businesses. Cloud providers, IT managed service providers and supply chain entities have become some favorites.

- **The Department of Justice seized approximately $3.6 billion in bitcoin stolen from a major exchange hack, Bitfinex, in 2016.** A young married couple in New York was charged with the crime. The original hack in 2016 resulted in approximately 2,000 transactions being executed across users' accounts to a single wallet address. At the time of the hack, the bitcoin was valued at only $76 million. With the extraordinary price increases in bitcoin over the years, its value topped $5 billion. Because of the transparency of bitcoin and the blockchain, investigators kept their sights on the movement of crypto from that wallet. While tactics were employed by the couple to launder the money and evade detection, eventually their identity was uncovered.

  Tom's Takeaway: The perception that bitcoin is anonymous is inaccurate. It is pseudonymous. Through investigation of the chain, the transactions and meta data associated with those transactions, over time, enough information can be accumulated to link those transactions to an identity.

- **The FTC reported that Americans lost an approximate $547 million in online romance scams in 2021, marking an 80% increase from 2020.** A total of $1.3 billion has been lost over a five-year period. The DOJ lists a site noting hundreds of romance scam cases, found here. Individuals 70 years and older had the highest average loss of $9,000.

- **The FBI issued an alert warning the public of an increase in SIM Swapping attacks.** In 2021, an estimated $68 million was lost. A SIM swap scam is when a cyber criminal manipulates a cell phone carrier to transferring control of the cell phone number to a device under the control of the criminal. While the report issues key tips, additional clarity and emphasis need to be placed on the following controls partially noted in the report:

    - Establish a PIN on your SIM card. If you lose your phone, this will prevent someone from taking that card, inserting it into a new device and taking control of your number.

    - Establish a PIN with your carrier. Many carriers allow you to establish a PIN that must be provided before a number can ever be ported by the carrier.

    - Don't provide your PIN to anyone that calls you claiming to be the carrier. Call back the known good number to ensure the conversation is in your control.

  Tom's Takeaway: Cybersecurity is so much more than a business issue. It is an issue that impacts each and every one of us on a very personal level. While we often focus on the businesses that are impacted, it is important that we don't forget the emotional and financial toll experienced by the people. The mission of *Cyber Roundup* is to not only help businesses defend against the cyber threat, but also you, the reader.

- **During the time known as the Great Resignation, the FBI issued an alert, warning the public of fake online job postings designed to steal information.** The FBI warned of the efforts that fraudsters will go through – the efforts of replicating legitimate job postings by copying logos, HR contact names and content; however, the fraudsters would change the contact information. They would then trick those who made contact into handing over very sensitive information. A key point in the alert is the reminder that for any legitimate business HR will not ask for sensitive information until **after** an offer for employment has been accepted. Further, HR will not ask you to send them money to process an application.

- **In response to the Russian invasion of Ukraine, the notorious hacking group, Anonymous, declared cyber war on Russia.** Attacks have been ongoing against various Russian state-run entities. Anonymous is a decentralized activist/hacktivist collective. The origins of the group date back to 2003 with the movement into hacking-based activities around 2008.

- **The following are some additional ransomware events in February**:

    - Morley Companies, a prominent business service provider to the Fortune 500 and Global 100 firms, disclosed a ransomware event that occurred in August and resulted in the theft of data. Approximately 521,000 individuals' information was impacted by the breach across employees, contractors and clients. The breach included highly sensitive data such as SSNs and medical information.

    - Ohlone Community College in California suffered a ransomware attack that resulted in the disclosure of staff, faculty, current and former student information. Highly sensitive information, such as SSN, driver license numbers, passport, medical and bank account information, were compromised.

    - The U.S. football team, the 49ers, reported a ransomware event that resulted in the theft and release of the team's financial information.

    - Car manufacturer, Toyota, suspended operations across 14 plants in Japan after a key supply chain provider was breached with ransomware. The reaction was designed to control and contain the incident as the supplier was one of the approximately 400 suppliers that are directly connected to Toyota's Just-In-Time production control system.

Contact Us

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Principal
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Nick DeLena, CISSP, CISA, CRISC, CDPSE
Partner
Cybersecurity and Privacy Advisory
ndelena@pkfod.com | 781.937.5191