PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – April 2023

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

It is clear that cybercrime will continue to increase, losses will mount and the tactics used by cyber criminals will rotate and evolve. What remains consistent, however, is the need for awareness and vigilance in defending against the cyber threat.

One of the objectives of our monthly **Cyber Roundup** – celebrating the sixth year of its launch this month – is to continue to remind you that you are not alone in the fight to keep your business systems and data safe. As AI (Artificial Intelligence) is used more and more in our businesses, **Cyber Roundup** will make you aware of news items requiring your attention. Resources exist to help and with PKF O'Connor Davies you will ***know better service***.

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.

- **The FBI released their annual Internet Crime Report** that depicts the top threats reported to the Internet Crime Complaint Center (IC3). The key points for 2022 are as follows:
  - **Internet crime losses** over the past five years total $27.6 billion. 2022 and 2021 accounted for $10.3 billion and $6.9 billion, respectively, of that total.
  - **Investment scams** topped the charts for 2022, resulting in $3.3 billion in total losses, more than doubling from the prior year's $1.45 billion. Cryptocurrency related scams accounted for the majority of those losses.
  - **Business e-mail compromise losses** increased to $2.7 billion, compared to 2021's $2.4 billion.
  - **Ransomware losses** ticked down to $34.3 million, compared to $49.2 million in 2021.
  - **The IC3's Recovery Asset Team (RAT)** had a 73% success rate for asset recovery. The RAT was established in 2018 for the sole purpose of streamlining communications between field offices and financial institutions to freeze funds of victims.
- **Authorities had a few wins in the past month successfully taking down two popular and damaging darknet marketplaces, the Genesis Market and ChipMixer.** ChipMixer was a darknet cryptocurrency mixer used by cybercriminals to launder in excess of $3 billion in cryptocurrency. The Genesis Market specialized in the sale of stolen data related to credentials, bank account information, computer and mobile identifiers (aka fingerprints) and other identity-related information.
- **Orlando Family Physicians, a Florida medical practice group of 10 clinics, settled a class action lawsuit from a data breach that occurred in 2021.** Under the settlement, impacted patients can receive $225 or $7,500 in restitution. The amount awarded depends on the level of severity. $225 can be awarded for documented expenses related to freezing credit, paying for identity monitoring and anything related to the communication, e.g. postage; $7,500 is reserved for those that had documented identity theft related to the incident.

Tom's Takeaway: The reality is that $7,500 for a person who suffered true identity theft is really only a fraction of the true dollar amount they should be awarded; however, it sends a clear message to those who handle sensitive personal information. Protect it, or pay up. It is a proven and well-documented fact that the cost of cybersecurity prevention is far less than the cost of dealing with the incident when it happens.

- **In a report released by Google security researchers, China-backed hackers have developed increasingly sophisticated techniques and toolsets that allow them to successfully penetrate government and corporate networks and remain undetected** while they steal information over the course of years. Leading cybersecurity breach response firm, Mandiant, notes that the tactics are so stealthy, even with their sophisticated hunting techniques, the intrusions are very hard to find.
- **Russian-speaking darknet marketplace, BidenCash, offered a promotional giveaway of 2 million stolen payment card information.** While it was identified that most of these numbers were already known to be breached and already circulating, the value of the numbers goes beyond just being able to make a purchase. Armed with these numbers, targeted spear phishing campaigns can be used to further compromise individuals.
- **Microsoft issued an alert on the large-scale use of phishing kits in the distribution of millions of malicious e-mails daily.** The kit being readily made available through Telegram and accessible with a $100 monthly licensing fee, facilitates an Adversary in the Middle Attack. Such an attack is designed to not only steal credentials, but also bypass Multi-Factor-Authentication to gain access to the target site.

The following are key ransomware events in March:

- **Minneapolis Public Schools**, which suffered a ransomware event early this year, has now reported that the threat actors have released the stolen information to the dark web. Data published consists of payroll information, union grievances, health information, civil rights investigations and other sensitive records. The data dates back as far as 1995. The cyber criminals were demanding $1 million to prevent the posting of the data.

- **Washington State Public Bus System** suffered a ransomware attack disrupting some of their systems. The threat actors are also currently claiming to have stolen data.

- **The City of Oakland**, which suffered a ransomware event in February, has reported that the ransomware gang has started to publish the stolen information. A first batch consisting of 10GB of compressed data consisting of highly sensitive information such as IDs, passports, financial information, etc. has been published.

- **Oak Ridge, a city in Tennessee**, suffered a ransomware attack impacting many of their government systems. This comes on the heels of Tennessee State University suffering a ransomware event two weeks prior.

- **Dish Networks**, which suffered a ransomware event late February this year, currently faces multiple class action lawsuits stemming from the event on the grounds of making materially false and misleading statements. The lawsuit claims that Dish Networks overstated their operational efficiency and cybersecurity infrastructure resulting in financial losses to investors when the ransomware event occurred.

Contact Us

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
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

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.