Cyber Roundup – April 2022

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

As we read about the victims of cybercrime each month, it is important to bear in mind that many of these breaches were preventable. Often, the failures we see are a result of cybersecurity programs and controls that were not matured and monitored effectively. An effective cybersecurity program is one that is continually assessed and tested. While no business will ever be 100% secure, it should always be in a demonstrable position that it exercised due care in the design and implementation of its cybersecurity program. When failures do occur and breaches result, timely transparency and ownership of the issue will be key.

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 the Internet Crime Report of 2021 that summarizes and compares key cybersecurity crime related statistics over time.** The highlights of the 2021 report are as follows:

  - Business e-mail compromise (BEC) remains the greatest source of financial loss. The 2021 total loss from BEC was $2.4 billion, up an estimated $1.8 billion compared to 2020.

  - In 2021, $6.9 billion in total victim losses were incurred across the various crime types, inclusive of ransomware, BEC, romance scams, etc. In 2020, the total victim losses were $4.2 billion.

  - The top five infrastructure sectors victimized consisted of: Healthcare, Financial Services, Information Technology, Manufacturing and Government.

  - The top five states by victim total loss are: California, Texas, New York, Florida and Pennsylvania.

- **JDC Healthcare Management LLC, a Dallas-based dental care provider, suffered a data breach that may have impacted the sensitive personal information of approximately one million individuals.** The breach was the result of malware being introduced into the environment which gave unauthorized parties access.

- **Morgan Stanley Wealth Management alerted that some of its customers were the victim of account compromises stemming from social engineering attacks.** The attackers impersonated Morgan Stanley utilizing both phone and e-mail social engineering tactics to obtain access to the customer accounts. Once access was obtained, fund transfers were executed utilizing the Zelle payment system.

  Tom's Takeaway: Company impersonation tactics utilizing phone phishing have been on the rise. I also have noticed an increase in fraudulent calls to my personal telephone number from spoofed financial institutions. What is concerning is that many times the caller ID displays the correct company name and number – making the calls all the more convincing. To protect yourself, we offer the following guidance:

  1. Make yourself familiar with your financial institutions' guidelines on how they will communicate with you on matters that require attention.
  2. Don't trust the caller ID. It can be spoofed.

3. In the event you believe the call to be real, but are not certain, disconnect and call the number back. By initiating the call back, you can have a higher degree of certainty you will be speaking with the correct company and not a fraud.

- **In a report issued by Unit 42, the average ransomware payment was $540,000 in 2021.** That represented a 78% increase from the prior year. The average ransom demand increased 144%, reaching an average of $2.2 million.

- **Ransomware was the dominant headline in March.** The following are the key ransomware events in March.

  - The FBI released a notification alerting that ransomware attacks are straining local U.S. government and public services. The attacks have resulted in disrupted operational services, risks to public safety and financial losses

  - Security software vendor Splunk released the results of an analysis on the speed in which 10 different ransomware variants encrypted data. Utilizing 100,000 files, or approximately 53 GBs of data to encrypt, the fastest ransomware encrypted all the data in four minutes. The slowest ransomware variant took 43 minutes.

  - Shutterfly, the major online photography printing service, issued a notification of a ransomware event in December 2021 that impacted the personal information of some of its employees. The information appeared to be HR related and consisted of such information as salary, payroll and employment offer letters. The information that was exfiltrated has been posted to the dark web and is available for download.

  - Partnership HealthPlan of California suffered a ransomware attack that resulted in the theft of personal information relating to 850,000 individuals. The organization was targeted by the HIVE ransomware group which is known to target healthcare entities.

  - TransUnion South Africa, the credit reporting agency, suffered a ransomware attack with the attackers demanding $15 million. The attackers obtained approximately four terabytes of data. The attackers claim they gained access through a user account that had a password of “password.” The Company has been working to validate the claims made by the hacker regarding the legitimacy of the data they claim to have. The Company has made it clear they will not pay the ransom.

- **Software consultancy firm Globant suffered a breach from the notorious Lapsus$ group.** The group released approximately 70 GBs of data to their victim site, appearing to include data on some high-profile companies, such as Facebook, Apple and C-Span. In addition to the data posted, it included information on the less than complex administrative passwords used to secure the DevOps platforms. Globant wasn’t alone in March suffering a breach attributed to Lapsus$. Samsung, Microsoft and Okta also disclosed they were victims of the group.

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