PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – May 2023

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

As I was preparing this ***Cyber Roundup***, my iPhone rang with a text from Bizarro World (just joking) stating that my shipment could not be delivered due to an unpaid duty fee (not joking). As I did not order anything nor, sadly, did I expect a gift package, I deemed it a scam. Even if I had a pending order, I would not click on the link provided, but, rather, telephone the vendor.

If our readers recall, five years ago when we started this publication, we reported on email scams, then text scams, then personal identity incursions, ransomware incidences and on other cyber infiltrations – both personal and corporate – et al. Now, artificial intelligence (AI) incidents are being reported. There is no slowdown to cyber criminality, including selling scams online. ***Cyber Roundup*** is published monthly to keep our readers updated. We are here to answer your questions, cyber train your staff and help you develop cyber defenses.

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.

- **Palo Alto released their Unit 42 Cloud Threat Report.** It provided the following interesting insights:
  - It takes on average approximately six days to resolve a security alert.
  - 63% of the software code deployed into production is susceptible to known and unpatched high or critical risk vulnerabilities.
  - 76% of organizations don't enforce Multi-Factor Authentication (MFA) for users, while 58% of organizations don't enforce MFA for their privileged administrative users.
  - Insecure configurations are a primary source of the security risk, driven by the use of vendor default configurations and templates that are not adjusted.

  Tom's Takeaway: The Cloud, through successful marketing tactics, has adopted a long-running misconception that it is inherently more secure. Going back to some of my first talks on the Cloud in 2010, that was a notion that even then had to be challenged. The Cloud is only as secure as the controller of the Cloud designs and maintains it. The act of going to the Cloud is not going to remove your security obligations nor reduce your risk; to a great extent, it simply shifts the risk. Even if the Cloud is configured with optimal security, your users remain the conduit to the Cloud. The attackers will always have a path. What remains consistent is the need for any organization, Cloud-based or not, to understand and manage their risks. Should you need help with that understanding, we are always here to help.

- **FBI Director Christopher Wray, in a report to Congress, noted that the scale of the Chinese hacker program compared to the U.S. would outnumber FBI cyber personnel 50 to 1.** He further noted that the Chinese government has the largest hacking program than every major nation combined and has successfully stolen more data from corporations of all sizes than any other nation. To help combat the issue, the Director is requesting $63 million to add another 192 cybersecurity positions.

- **As summer vacation travel season begins to roll in, the FBI sent out a public advisory reminding people to avoid using free charging stations at hotels, airports, etc.** By using the free charging station and connecting directly into the USB port, malware can be loaded onto your device. To be safe, carry your own physical charger and cord and connect directly into a traditional power outlet.
- **A new dark web marketplace, STYX, is rapidly gaining traction for transacting various types of illegal services.** This comes on the heels of law enforcement's recent wins in taking down other similar long running marketplaces, such as Genesis, which we reported on in last month's ***Cyber Roundup***. The STYX marketplace offers the following services:
  - Tools to bypass anti-fraud filters such as fingerprint emulators and spoofers, or services such as Multi-Factor Authentication.
  - Stolen personal information such as SSNs, credit card and other personal data for sale.
  - Lookup services that extract information about individuals or organizations.
  - Fake ID services for over 65 countries.
  - Telephone, Short Message Service (SMS) and email flooding services at a cost of $4 to $150 per day.
  - Money laundering services.
  - Renting malware.
  - Manuals and tutorials on hacking and cybercrime operations.

  Tom's Takeaway: While the listing above is, for the most part, nothing new, we do want to highlight the Multi-Factor Authentication bypass. Over the past few months, we have witnessed many clients and friends fall subject to this attack. In order for this attack to be successful, in almost all cases it starts with the manipulation of the user through social engineering. As you update your awareness training programs, be sure to mention and include this tactic.
- **For the first half of the year, ransomware attacks were relatively low**. Over the past month, the attackers certainly made up for lost time. The following are some major ransomware events that occurred during the month of April:
  - **Voice cloning using artificial intelligence is starting to take the headlines.** Last month, news broke that kidnappers utilized the technology to emulate the voice of a 15-year old girl to her parents. The voice of the 15-year old claimed being held captive and would only be released if a ransom were paid. This is likely only the tip of the iceberg when it comes to this technology being used for malicious purposes. In my opinion, we will begin to see this being used to facilitate the movement of money.
  - **A Minneapolis school district suffered a ransomware attack.** The cyber criminals released a large amount of highly sensitive information consisting of teacher SSNs and student psychological reports and allegations of abuse. While cyber criminals will typically only post to their forums on the dark web, this particular group also posted to twitter and facebook.

  Tom's Takeaway: Many schools have moved away from storing student SSNs. What is often overlooked is the other forms of sensitive data that may exist. As schools evaluate their cybersecurity programs, tracing the movement of such information through the school is a critical component to ensure it is protected adequately.
- **Camden County Police Department in New Jersey suffered a ransomware attack.** It resulted in the encryption of case files and disruption of administration tasks. The 911 system was not impacted.

- **Jefferson County School District in Alabama suffered a ransomware attack shutting down all key systems.** Teachers reverted to traditional teaching and grading with non-electronic technologies. It has been claimed that the cyber criminals did not steal any school information as part of the attack.
- **Illinois-based hospital, Sarah D. Culbertson Memorial Hospital, suffered a ransomware attack that resulted in the shutdown of their Electronic Medical Record system.** The investigation is ongoing and patients will be notified if their information was determined to be compromised because of the breach.
- **The ransomware gang that infiltrated Western Digital is now requesting a minimum eight figure payout to stop the release of data stolen during the attack.** The hackers claim to have taken 10TB of information consisting of both customer and sensitive company data. The cyber criminals have not encrypted the systems to date but are warning they will do so, in addition to leaking the data, if they are not paid. The cyber criminals have been actively reaching out to the Company's executives.
- **One Brooklyn health system which experienced a ransomware attack in November 2022 is now facing a class action lawsuit on behalf of the patients whose sensitive personal data was impacted during the breach.** Approximately 235,000 patients had their information compromised.
- **NCR, the parent company of the Aloha Point of Sale System and back-office app used by over 100,000 restaurants and bars, experienced an outage as it suffered a ransomware attack.** The outage significantly impacted its customers' ability to manage their operations. Payments could not be processed and access to staffing schedules, inventory and payroll systems was disrupted.

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