PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – August 2023

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

As summer is coming to an end, there's no let-up to cyber-criminal activity. As a matter of fact, with the school year starting soon (in some states schools are already open) and with boundless internet access, we need to be ever more cautious both personally and businesswise. We will advise our readers throughout the year on what's happening and what they can do to mitigate danger. With Labor Day approaching, stay with us and don't hesitate to reach out to us if we can help.

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.

- **A new Artificial Intelligence (AI) tool, called FraudGPT, has been developed and made available by cybercriminals for malicious purposes.** The cost is $200 per month or a discounted yearly rate of $1,700. Not limited to the following, the tool offers these capabilities:

    - Write malware.
    - Make the malware undetectable by anti-malware solutions.
    - Create phishing landing pages.
    - Write phishing and scam emails.

    Tom's Takeaway: Since this tool has been launched, the general feedback by security researchers is that it is not that effective when it comes to certain of its claimed capabilities, such as writing undetectable malicious code; however, as it learns – no different from any other AI engine – that could change over time. As we move into the future, the cybersecurity landscape will inevitably become a battle of AI, good versus bad.

- **Microsoft reported that it was the target of a China-based threat actor that resulted in the theft of emails of approximately 25 U.S. organizations, inclusive of government agencies.** The motive of the attack was espionage. The attack, now dubbed Storm-0558, leveraged a vulnerability that resulted in unauthorized access to email accounts belonging to the victim organizations.

- **HCA Healthcare reported a breach impacting approximately 11 million patients across 170 of its hospitals.** The breach was first discovered when the stolen data was posted to an online forum. The data is believed to have been taken from an external storage location utilized by the Company. HCA claims that no highly sensitive information has been impacted. The data stolen consisted of information such as name, address, email, phone number, gender, service date, zip code, etc. Patient clinical information was <u>not</u> impacted.

- **In a study, the UK-based Royal United Services Institute identified no material correlation between ransomware victims that ultimately pay the ransom that have cyber insurance as opposed to those who don't.** They identified that those targeted that had their cyber insurance policy details exfiltrated as part of the attack did result in leverage from the cyber criminals in setting their ransom demands.

    Tom's Takeaway: This topic of cyber insurance fueling the ransomware landscape has been a long debated one. Logical reasoning tends to side with the conclusion that cyber insurance has allowed – and often accelerated – payment by those that otherwise may not have been able to pay or pay anywhere near as much. While it may not be the primary fuel source of the fire, it certainly has stoked the flames in my opinion.

- **The U.S. Health Department was the victim of a cyberattack that may have resulted in the breach of personal data of 100,000 individuals.** The attack is attributed to Russian cybercriminals and the now notorious MOVEit vulnerability.

  Tom's Takeaway: The impact of the MOVEit vulnerability, utilized in a massive number of attacks during May and July, continues to unravel. This will likely continue over the coming months as other organizations come forward. To date, 701 organizations, many of which are well known large organizations, have been confirmed as victims. In total, approximately 48 million individuals have been impacted and countless other types of confidential data. An active listing of impacted companies can be found here.

- **The Community College of Hawaii suffered a ransomware attack and ultimately paid the negotiated ransom of $100,000.** While the College was able to restore the impacted systems, it ultimately paid the ransom in an effort to prevent the leakage of approximately 65GB of data stolen during the attack. The exposure would have impacted approximately 28,000 individuals.

- **Google launched a new pilot program that will restrict select employees to internet-free desktops.** Google is running the program in an effort to reduce the risk of a cyber breach. By limiting internet exposure, they are in effect limiting a primary vector of compromise.

  Tom's Takeaway: While it sounds almost unthinkable to remove internet access in this day and age, the reality is, in certain cases, it makes perfect sense. Not every employee and every role requires internet access to perform their functions. While it is unlikely that any company can restrict every employee, by restricting a subset you are reducing the likelihood. It is very easy to get caught up in thinking that a control needs to be all or none to be effective. That is not accurate. While a company cannot always eliminate risk, they can manage it. Applying a control such as this to only a subset by no means eliminates the risk, but certainly allows Google to better manage the risk.

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.