PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

DGC
ACCOUNTING • TAX • ADVISORY
A DIVISION OF PKF O'CONNOR DAVIES, LLP

Cyber Roundup – June 2022

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

You will see below a variety of cyber-criminal pursuits that occurred in a short period – including business e-mail compromises, ransomware activity demanding payoffs and malware attacks – along with others. These criminal pursuits affected diverse businesses – from professional associations to educational institutions to equipment manufacturers – to name a few. The attackers were domiciled in various geographical locations, including diverse localities, such as North Korea, Texas and Central America – among others.

In the "takeaways," we provide some actions that can be used to avert the incident, but if your business is being targeted or if you want to avoid such targeting, your best bet is to reach out to us so we can assist you hands-on.

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.

- **Business e-mail compromise (BEC) has resulted in $43 billion in losses since 2016, according to an updated FBI Public Service Announcement (PSA).** A large portion of the $43 billion in losses were incurred between July 2019 and December 2021, representing a 65% increase during that period. The report attributes some of the increase to the challenges faced during the period with many companies working remotely.

  Tom's Takeaway: As a Firm, as much as we try to educate our clients and other readers on how to avoid becoming a victim of BEC, losses are still incurred. What we have personally noticed is that many of our clients have implemented the correct procedures on paper to limit the risk; however, the procedures are not consistently followed resulting in funds being diverted. As a reminder, the PSA (linked above) provides key controls when it comes to limiting your risk to BEC. It is imperative that you not only adopt the controls by policy, but also by actions as well as consistently educate your employees on the process and make it clear: **no exceptions**.

- **Security Researchers from the NCC Group, demonstrated a proof of concept that a Tesla can be unlocked and stolen by taking advantage of the Bluetooth authentication process.** This attack can be applied to not only Tesla's but also other smart devices that utilize the technology. The attack works by relaying the signal from an already paired device that grants access to the car when in close proximity. The full technical advisory can be found here.

- **Zola, a wedding website registry, suffered an attack that resulted in customer accounts being breached.** The attackers ran up fraudulent charges on the customer stored credit cards and transferred gifted funds to unauthorized bank accounts. The attack utilized a credential stuffing technique in which customer passwords obtained from other company breaches are used in an attempt to gain access to other websites. Zola has addressed the issue and has committed to correcting any transactions not taken by the customers.

  Tom's Takeaway: A rule of thumb is to avoid using the same password across multiple websites. This type of attack on Zola specifically targeted those that did not follow that guidance. Over the past two years, this type of attack has become increasingly common. Password managers are an effective way to help ensure each website has a unique password and minimize the burden to the user of having to remember an endless number of passwords. An additional measure is to monitor the dark web for exposed credentials. We offer such a service for many of our clients. Additional information can be found here on the service.

- **Interpol Secretary, General Jurgen Stock, issued a warning that nation state malware will make its way into circulation on the dark web in the coming years.** This warning comes on the heels of the ongoing Russia-Ukraine military conflict and the respective nation state developed malware potentially utilized by both sides in the conflict. Once the malware is utilized and identified, it can be reverse engineered to generate unique and very powerful malware variants.

  Tom's Takeaway: As we have noted throughout the conflict, this is the first highly publicized military conflict that we are witnessing directly that utilizes cyber warfare. Once the malware is deployed against the enemy and identified, it is akin to a physical conflict which deployed top secret equipment and the equipment made its way into the hands of the other side. Once they have it, they will try to take it apart to understand the technology and how it works. Once they reverse engineer it, they can harness the knowledge gained and utilize it for their own attacks. Unfortunately, malware strains are much easier to obtain, duplicate and redistribute to multiple parties when compared to a large piece of military equipment, making it that much easier for it to make its way into the wrong hands.

- **In Netskope's most recent Cloud Threat Report, they note that most of the malware attacks are now coming from the same region as the victim.** Specific to North America, 84% of the malware downloaded can be attributed to a location hosted within North America. The trend is likely in response to the attackers attempting to bypass geographical restrictions that many companies have implemented. Interestingly, the report also notes the increase of attackers leveraging and enhancing their use of search engine optimization (SEO) to distribute malware by way of the search engines.

- **The FBI released an advisory alerting to North Korea's attempts to have their citizens obtain IT employment outside of North Korea.** The North Koreans will attempt to hide their citizenship as they look to obtain freelance jobs in the IT sector. These clandestine IT workers are a significant source of revenue for the regime and support the various sanctioned activities of the regime related to weapons of mass destruction and ballistic missiles. For more details on the operation and red flags to identify, the advisory can be found here.

- **A Texas man was arrested for procuring 38,000 stolen PayPal credentials with the intent and action of stealing funds**. The accounts were identified to have been used in one million fraudulent transactions. In addition to receiving a five-year sentence, the individual has been ordered to pay $1.4 million in restitution.

- **Ransomware continues to be a dominant threat. The following are the key ransomware events for May.**

  - The Chicago public school system issued an alert that a vendor used by the district suffered a ransomware attack which resulted in the exposure of the personal information of approximately 500,000 students. The breach impacted any student that attended a school in the school system between 2015 and 2019. Highly sensitive information such as SSN, financial information and grades were not impacted. Credit monitoring is being offered for all those impacted.

  - The American Dental Association suffered a ransomware attack that disrupted operations and resulted in the exposure of sensitive information. Approximately 2.8 terabytes (TB) of information that was taken from the ADA has been leaked by the Ransomware gang. The threat actor claims the 2.8 TB represents only 30% of the total data that was stolen. The published data that has been leaked appears to obtain highly sensitive information such as W2s in addition to other operational data, such as accounting schedules and NDAs.

  - AGCO, an agricultural equipment manufacturer, suffered a ransomware attack that resulted in a shutdown of operations at some of its facilities. For the impacted facilities, AGCO was forced to send their staff home until operations could resume. At the time of the notification, AGCO was anticipating being down several days – if not longer – as they attempted to repair the systems.

- Kellogg Community College in Michigan suffered a ransomware attack that resulted in the suspension of classes for their approximately 7,000 students. The College was attacked over the weekend and was able to resume operations by that coming Wednesday.

- The President of Costa Rico declared a state of emergency as a result of a ransomware attack that significantly disrupted government operations. The ransomware group that facilitated the attack claims to have gained access to 900 servers and extracted approximately 1 TB of data. The group is demanding $10 million. The Government has refused to pay the ransom. The gang has begun to publish the data that was stolen.

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