Cyber Roundup – July 2022

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

The speed and accuracy delivered by all forms of cyber machinations is undeniable. However, although cyber risk cannot be totally eliminated – at least at this stage of development and as evidenced by this issue of Cyber Roundup – it can be mitigated. The Cybersecurity and Privacy Advisory team at PKF O'Connor Davies can assist you at various levels in helping lessen your exposure to cybercrime.

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.

- **Russian law firm, Rustam Kurmaev and Partners, was successfully targeted by the Anonymous hacking collective, resulting in 1TB of stolen data leaked to the public.** The data consisted of client and internal e-mails, files and backups. This leak came on the heels of another successful Russian breach by Anonymous against one of Russia's largest media companies, Vyberi Radio, resulting in the release of hundreds of GBs of company data. Anonymous declared a cyberwar against Russia earlier this year in response to the Russian invasion of Ukraine.

- **The Department of Justice (DOJ) and FBI successfully seized three internet domains that hosted and offered access to stolen information and was utilized to perform cyberattacks**. The seized domains consisted of WeLeakInfo.to, ipress.in and ovh-booter.com. The sites contained information collected through more than 10,000 different data breaches. Once on the sites, users could search across 7 billion records to obtain stolen names, e-mail addresses, credentials, phone numbers, etc.

- **In another successful take down by the DOJ and FBI, with assistance of the Cyprus police, a marketplace on the dark web was seized.** The marketplace listed approximately 24 million SSNs belonging to U.S. citizens and generated upwards of $20 million in revenue.

  ***Tom's Takeaway**:* It is important that we don't lose sight of the continued efforts of law enforcement to combat the cyber threat. While it may seem easy to say, "why don't they just stop it," or "how can they let this happen," the reality is in the vastness of the internet. In addition, the various techniques used to stay anonymous, coupled with jurisdictions that will not cooperate with U.S. law enforcement, it is an incredibly difficult task. Small wins like those above are significant and need to be appreciated for what they are.

- **1.2 million patients of San Antonio-based Baptist Medical Center had their information breached and exfiltrated as a result of a malware incident.** The breach is the fourth largest medical records breach to date according to the Department of Health and Human Services. The information contained highly sensitive data such as medical information and SSNs.

- **In a statement made by Microsoft, 10,000 organizations were targeted by an advanced phishing campaign that effectively bypassed multi-factor authentication.** Once access was obtained to the victim mailboxes, the compromised accounts were further leveraged to commit business e-mail compromise (also known as BEC), an attack method used to siphon funds away from target companies.

  ***Tom's Takeaway**:* Multi-factor authentication (MFA) is by far one of the best and important controls every company should implement. However, it is important to keep in mind that it is not fool proof. Attacks can be designed to bypass the control. As a Firm that performs numerous penetration tests for our clients, it is an attack method that we also often use to demonstrate the

potential risks and weaknesses of MFA. While technical controls can be implemented – such a YubiKey – employee security awareness training remains one of the best tools in your arsenal. These attacks will often leverage a spoofed login page that intercepts your authentication and relays it to the real website and vice versa, effectively becoming the man-in-the-middle. In those situations, the website address will be slightly manipulated and not the real website.

- **Health care provider, Kaiser Permanente, suffered a data breach impacting approximately 70,000 patients as a result of unauthorized access to an employee's e-mail account.** The provider did not release how the incident occurred; however, it notes that while they have no indication that information was accessed by the unauthorized party, it cannot definitely conclude otherwise to rule out the possibility. The information that may have been breached contained patient information such as medical records, lab results and dates of service. SSNs and credit card numbers were not impacted.

  Tom's Takeaway: Logging and monitoring of account activity is one of the most important controls you will need in the event of a breach. Should an account be compromised, the onus will be on you to conclusively determine what the compromised account did and did not view, or actions performed. Without such logging to tell the full story and define the facts, you will likely be instructed by legal counsel that you need to assume it was compromised, potentially drastically increasing your reporting obligations and costs associated with the breach.

- **Michigan-based Flagstar Bank suffered a breach that resulted in the compromise of 1.5 million customer records.** The data impacted consisted of highly sensitive and financial information. Of greater concern, upon investigation of the breach, it was identified that the threat actor had compromised and had access to the Bank since December 2022.

- **The following is a summary of ransomware activity during the month of June:**

  - A new ransomware strain was identified by researchers and has been dubbed "GoodWill." Unlike typical ransomware which extorts their victims for cash, this particular group requires its victims to perform and prove the performance of, three socially driven and beneficial activities to obtain the decryption key. Once the activities are completed, the victims must post to social media how they transformed themselves into becoming a kind human being as a result of the GoodWill ransomware.

  - Hanesbrands suffered a ransomware attack toward the end of May. The Company has not released much information but has noted they obtained legal, forensic and other professional assistance. The Company stated that they cannot yet determine if this attack will have a material impact on their business. As a publicly registered company, Hanesbrands would be required to report to the public and shareholders any material impact.

  - The BlackCat ransomware gang has introduced a new tactic to their arsenal to help ensure payment by their victims. In addition to notifying the victim company directly that they have locked their data or exfiltrated it, the company is now also contacting individuals that had their information contained in the breach and notifying them of a public website they can use to search what has been stolen for their information. The goal is to have the victims reach out to the breached company and encourage them to pay.

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