Cyber Roundup – May 2022

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

As you read through the cyber incidents recently occurring, you will note a real-world example of how much damage ransomware can inflict. A college in Illinois survived two World Wars, the Spanish Flu, the Great Depression and other significantly challenging events over its 157-year history but, sadly, could not recover from the damage of ransomware and financial distress.

Make a commitment today to put your IT infrastructure under scrutiny. Call or e-mail us and we will offer some potential cyber services we can provide.

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 leak of internal documents of the Conti ransomware group provided unique insight into the internal operations of the organization.** Interestingly, the ransomware gang operates no different than a legitimate corporate business. They maintain salaried employees who are provided bonuses, performance reviews, employee referral incentives and the coveted spot of "Employee of the Month." The employee of the month receives a bonus equal to half their salary.

- **In a report by Checkpoint that studied ransomware trends, the following interesting insights were noted:**

  - The "threat actor" will typically request 0.7 to 5% of the compromised company's revenue.
  - The weekly average of organizations impacted by ransomware increased by 24% year-over- year.
  - Select ransomware groups may offer discounts of up to 25% for quick payment.
  - The average total cost of a ransomware attack is more than seven times higher than the average ransom paid. The ransom paid is dwarfed by the total fees incurred for response, investigation, remediation, legal fees, operational down time and other factors.

- **Lincoln College, an Illinois liberal arts college, will be forced to shut down as a result of a ransomware attack, ending 157 years in operation.** Lincoln College (which was already under financial distress) suffered the attack in December 2021 resulting in all key systems required for recruitment, retention and fundraising efforts inaccessible. The systems were down for an extended period of time, during which the College could not recover. Schools remain a common target for cyber criminals. Lincoln College was just one of 1,000 schools that were impacted in 2021 by ransomware.

  Tom's Takeaway: All too often, cybersecurity isn't an issue until it is an issue. As budgets are planned and approved, it's easy to shift funds away from cybersecurity when no tangible benefits can be directly observed. This type of traditional mentality will be a key differentiator in the coming years of the businesses that survive vs those that don't. Cybersecurity isn't a cost of your business, it is your business.

- **Mail Chimp was the victim of a very targeted attack designed to try and steal funds from cryptocurrency wallets**. The attackers gained access to an internal system and stole data on approximately 100 clients. The clients targeted were those in the cryptocurrency and finance sectors. The data harvested was used to conduct phishing campaigns alerting the users of a breach and instructing them to download an updated version of Trezor (hardware wallet) software. Once installed, the software is designed to take over the wallet and steal the seed phrase. The seed phrase is the grouping of words that is used to construct the private key which is stored in the hardware wallet. The private key is what is needed to control and transact with the wallet. With the

seed, the attackers could move the money out of the wallet. The impacted users were notified and no known users are believed to have been victimized.

- **A spear phishing campaign was identified in April targeting hiring managers with malicious malware under the guise of resumes.** The e-mails would include a response to an open position and guide the recipient to download a file. The file would contain the malware. Once executed, the malware is designed to steal credentials to gain further access to other accounts and systems.

  Tom's Takeaway: Human Resources is a high value target from a cyber-criminal perspective. In assessing your cyber and information security risk, Human Resources needs to be a separate and distinct focus area. Scenarios such as receiving malicious resumes need to be accounted for and controls designed to mitigate that risk.

- **Security researchers have identified during the first quarter of 2022 six strains of malware – a significant increase from the prior year – specifically designed to erase data.** The malware has been identified as being used extensively against Ukraine's infrastructure and organizations. While Ukraine has been the primary target, the U.S. Government warns that such attacks could be directed in the future toward Western governments and companies.

- **308,000 databases were identified by security researchers as being directly exposed to the internet, allowing anyone access to the data.** From Q1 2021 to Q1 2022, the number of exposed databases identified over the period increased approximately 25%. The growth is attributed to companies continuing to expand their accessibility to account for the continuance of remote work.

  Tom's Takeaway: An incorrectly exposed database is a prime example of a preventable problem. As businesses further embrace remote work as the model that will be sustained going forward, risks continue to need to be assessed. The risk assessment has to not only factor in the user, but the infrastructure used in the support of the user. Exercises such as penetration tests against the exposed infrastructure are key in identifying misconfigurations before issues arise that ultimately result in a breach. If you are in need of a penetration test, we have a team of skilled professionals who can assist.

- **The hacktivist group, Anonymous, has leaked approximately 5.8 TB of Russian data since declaring a cyber war on Russia in response to its invasion of Ukraine.** The data belonged to various Russian-based businesses and government entities, inclusive of a commercial bank.

- **Kansas-based hospital, Newman Regional Health, reported a data breach that impacted more than 52,000 individuals.** The breach was the result of an external party gaining access to e-mail accounts between January 2021 and November 2021. The e-mail accounts compromised were identified as containing extensive personal data, inclusive of protected health information.

  Tom's Takeaway: Businesses often underestimate the extent and sensitivity of the data that resides in e-mail, often resulting in breach notifications when an account is compromised. All e-mail accounts should be multi-factor authentication enabled. In addition, retention requirements should exist on e-mail. We identify a large number of businesses that have no defined e-mail retention requirements and mailboxes that contain years of data. An e-mail system should not be used as a document storage system. When it is used as a document storage system, the impact caused by a breach of the e-mail account often becomes significantly greater.

- **T-Mobile has again been a victim of a breach, this time resulting in the theft of approximately 30,000 source code repositories.** The attack, which has been attributed to the Lapsus$ hacking group, is believed to have occurred as the result of the group purchasing stolen credentials belonging to T-Mobile employees. The stolen credentials were used to gain access to key T-Mobile systems. The accounts were identified as trying to access mobile accounts belonging to the FBI and Department of Defense; however, additional authentication procedures for those accounts prevented the access.

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