Cyber Roundup – February 2022

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

So it continues. There is no end to the nefarious tricks created by cybercriminals. Gone are the days of emails from princes from other countries. We now have to be concerned that bad actors can wipe out our computer hard drives, steal credentials and funds using QR codes, take over our keyboard by means of malicious USB drives, create malware that can steal credentials stored in browsers, offer employees money to introduce ransomware into company networks … and the beat goes on.

Please reach out to us for assistance. We are here for you.

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.

- **With U.S. and Russian tensions rising, the Cybersecurity and Infrastructure Agency issued an advisory to protect against critical cyber threats to U.S. companies.** The alert is directed not only to government agencies, but every company of every size as well. Of concern is the identification of a newly-created attack designed to completely wipe the computer hard drive. The alert – in addition to actions to take – can be found here.

  Tom's Takeaway: Gone are the days of just worrying about a country's military power and nuclear capabilities. In a globally connected world, borders fade away and the attackers lurk in the shadows of the connectivity on which we depend. It is scary to think how much damage can be done without a single shot fired. The burden of the battle the government faces in the cyber realm does not solely lie with it. Every company – big and small – plays a role. In this world, the weakness of one can very easily translate into the weakness of all. If you need assistance in developing and strengthening your cyber strategy and upholding your role in this cyber battle, we are, and will remain, here on call and ready to assist.

- **The FBI issued an alert noting that cyber criminals are leveraging QR codes to infect users, steal credentials, or steal funds.** A QR code is similar to a barcode; however, it is intended to be scanned by a smartphone. Upon scanning, the code is translated into a website link to which the user is redirected. QR codes have become increasingly popular during the course of the pandemic.

  Tom's Takeaway: QR codes have now become common place for many situations, such as restaurants, school pickup, doctor's office check-in, and product registration. Ultimately, the code serves as a means to easily transfer you to the correct web site. Part of the problem is that in almost all circumstances, the QR code link displayed will also leverage a URL shortener, further obfuscating where the link will take you. In situations like this, don't forget***: Pause, Inspect, and Think*** before proceeding. You may have no choice but to scan; however, you do have the opportunity to make sure the website you land on is what you expect and consistent with the intent of the service. For example, if you scan a menu and are being prompted to log into an account, something is not right. For additional tips, read the FBI alert here.

- **The FBI issued an alert that a notorious ransomware gang, FIN7, has been identified as mailing malicious USB drives to U.S. businesses**. The malicious drives, once plugged in, will emulate a keyboard and begin executing commands on the machine. The speed at which the commands are executed could be very difficult for the end user to notice. While many companies may block USB storage devices, because this device emulates a keyboard, the device will

connect regardless of the company's controls. Training end users not to insert any USB drive into their computer is key in defending against this threat.

- **Researchers are cautioning users not to store passwords in their browsers.** As workers continue to work from home and potentially use personal machines, the convenience of storing passwords in the browser is commonplace. Malware is designed to steal those credentials that are stored in the browser and has been responsible for companies being breached. The current known malware strain is dubbed "RedLine." The malware is effective and can be easily obtained in the dark web for as little as $150 dollars.

  Tom's Takeaway: Remote work, in some capacity, will persist for the foreseeable future. Ensuring your remote access security controls are appropriate has been and will remain key. An effective remote access strategy needs to consist of not only technical controls but well-communicated policies to drive employee behavior. If you need assistance in evaluating or enhancing your remote access security strategy, we can help.

- **QRS, a vendor that provides an electronic health record portal for providers, is facing a class action lawsuit for a breach that impacted approximately 320,000 individuals.** QRS originally reported the breach in November after it determined that a single provider's portal had been accessed by an unauthorized individual in August and data may have been exfiltrated. The data included highly sensitive data such as SSNs and medical information. The suit claims that QRS failed to implement appropriate controls to prevent or detect the attack.

  Tom's Takeaway: Overall, we are seeing a general trend in private lawsuits being filed in the wake of a breach. HIPAA, which QRS is subject to, does not allow a private right of action (i.e., individuals can't sue the company for a breach of HIPAA); however, HIPAA does not override state laws that may be more restrictive and allow for such lawsuits to occur. Over the past two years since the start of the pandemic, we witnessed an intense uptick of identity fraud. This trend of lawsuits I personally believe is the response of people tired of being victimized from the digital negligence of others. Cybersecurity isn't optional for your business; it is and will remain a necessary component.

- **The International Committee of the Red Cross suffered a sophisticated cyberattack that resulted in the compromise of highly sensitive data on approximately 500,000 individuals.** The individuals impacted are considered highly vulnerable. They are people who have been separated from their families due to conflict, migration and disaster, detention, etc. It is not known who is responsible for the attack. The Committee has issued a public appeal to the attackers not to release the information.

  Tom's Takeaway: All too often I think we equate cyberattacks with monetary or commercial losses. This breach of a very prominent social service agency reminds us of the potential human and emotional impact that a breach can have. Every business, be it for-profit or not-for-profit, is at risk.

- **The following are some of the significant ransomware events in January:**

  - Bernalillo County, New Mexico suffered a ransomware attack that took down all major systems and resulted in the closure of most of the town's buildings. Emergency systems remained operational; however, contingency plans had to be deployed to resume operations.

  - The Maryland Department of Health suffered a ransomware attack; however, it quickly detected and responded to the incident, ultimately resulting in no significant impact or loss of data.

  - A survey conducted by HITACHI ID identified a 17% increase since November 2021 of employees being offered payment by bad actors to introduce ransomware into their company networks. In most cases, social media and email was the preferred method to contact the employees; however, 27% received a direct phone call.

  - McMenamins, an Oregon-based hospitality company, suffered a ransomware attack that resulted in the breach of 23 years of sensitive employee information. It does not believe

that customer information has been impacted. A class action lawsuit has been filed by the victims as a result of the breach.

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, IT Risk Assurance & Advisory
ndelena@pkfod.com | 781.937.5191

www.pkfod.com