Cyber Roundup – January 2022

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

In terms of cybersecurity (or lack thereof), the year 2022 starts out pretty much as it ended in 2021: cyber criminals of all stripes are actively pursuing information from your computer system so they can leverage it on their behalf. Not only do you need to be aware, you need to be prepared. Contact us to see if we can help 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.

- **As disclosed in December 2021, a major zero day software vulnerability named Log4j was impacting organizations of all sizes across the globe.** The vulnerability allows an attacker to take control of an impacted system. To date, the vulnerability has been leveraged to distribute ransomware, install cryptominers, steal credentials, and infiltrate deep within a company's network. The Federal Trade Commission (FTC) has made it clear that organizations need to respond to this vulnerability and remediate it, or face penalties. The Cybersecurity and Infrastructure Security Agency has released guidance in addition to tools to help manage the vulnerability. The guidance can be found here.

  Tom's Takeaway: The Log4J vulnerability, while sounding technical and easy to glance over, is something that should not be ignored. There is a high probability your business is using a piece of software that is vulnerable to this issue. As senior management or the Board, the individuals or third parties responsible for the management of your IT operations should be providing to you a clear plan to identify and remediate the vulnerability. If you need assistance in understanding the cyber risk to your business and how to manage that risk, we can assist.

- **A leading University in Japan, Kyoto University, lost approximately 77TB of data as a result of a backup software error.** The issue occurred from a flaw in a software update applied to their backup software, resulting in the deletion of data. The vendor, HPE, has accepted responsibility for the issue.

- **Colorado energy company, Delta-Montrose Electric Association, suffered a cyberattack that resulted in approximately 90% of their internal systems being taken offline and the loss of historical data spanning 25 years.** The attack did not impact the power grid; however, all support systems, billing operations, and customer-facing systems were impacted.

  Tom's Takeaway: After reading the prior two bullets, two key words pop into my head, *Preparation* and *Resiliency.* Issues will happen that will impact your operations, be it a cyberattack, unintentional software malfunction, or a global pandemic. Regardless of the issue, the questions you need to reflect on are how resilient is your company's operations and do you have the plans in place, procedurally and technically, to recover. Tackling issues like the ones above, will come down to three key plans: Business Continuity, Disaster Recovery, and Incident Response. Like everything in life, something is not an issue, until it is an issue. These plans will help ensure you have a fighting chance for survival regardless of the event. If you need assistance, designing, evaluating, or testing these plans, we can help.

- **Car maker, Volvo, suffered a breach that resulted in the theft of sensitive research and development information.** Volvo has confirmed the attack was not a ransomware event and that they remained in control of their systems. In addition, it noted that the attack did not impact the security of their customers' data or car safety.

- **In a study released by Stony Brook University and Palo Alto Networks, they note the proliferation of malicious toolkits being created and sold to allow cyber criminals to defeat Multi-Factor Authentication.** The tools are used to phish users and gain access to websites they use, regardless of multi-factor authentication being enabled. In their search of the DarkWeb, they identified approximately 1200 different toolkits designed for the task.

  Tom's Takeaway: While this sounds discouraging, it doesn't have to be. Multi-Factor Authentication still is fundamentally one of the best protections you can implement to secure your accounts. For these attacks to be successful, the attackers will need to phish or trick their victims first into interacting with them. This further reinforces the need for effective cybersecurity awareness training and the understanding that technology alone cannot and will not defeat the cyber threat.

- **Ransomware attacks remained consistent during the month of December. The following is a summary of key ransomware related events:**

  - Kronos, a major provider of payroll and timekeeping systems, suffered a major ransomware attack that impacted businesses across the U.S. The attack resulted in Kronos advising the users of their software to activate their business continuity plans as it relates to payroll processing as their system will be offline for an extended period.

  - Ransomware gang, AvosLocker, provided a decryption key free of charge when it learned it had impacted the systems of a U.S. police department. A member of the AvosLocker organization noted that they typically avoid government agencies and hospitals; however, affiliates that utilize their ransomware software may do so without notifying them first. The gang refused to provide a listing of files that they may have taken and also provide information on how they gained access to the network.

  - The FBI issued a flash alert, found here, that they have identified that a Cuba ransomware gang has successfully compromised 49 critical infrastructure companies over the past year. The companies ranged across the sectors of government, healthcare, information technology, manufacturing, and financial. The gang obtained $43 million in ransom payments out of the $74 million total requested.

  - Shutterfly, a photo service provider, suffered a ransomware attack impacting components of their internal network related to manufacturing and support systems. Shutterfly noted that the attack did not impact any sensitive customer data. The incident remains under investigation.

  - Virginia's Legislative Information Technology Agency suffered a ransomware attack. The attack impacted systems supporting the Division of Legislative Services, Division of Capital Police and other internal systems that support the drafting and modification of bills. The attack remains under investigation.

Contact Us

Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory
CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE

PKF O'Connor Davies, LLP
212.867.8000 or 646.449.6353 (direct)
tdemayo@pkfod.com

www.pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, the Firm has 16 offices in New York, New Jersey, Connecticut, Maryland, Massachusetts, Florida and Rhode Island and more than 1,200 professionals providing a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is led by over 135 partners who are closely involved in the day-to-day management of engagements, ensuring a high degree of client service and cost effectiveness.

The Firm is a top-ranked firm, according to *Accounting Today's* 2021 "Top 100 Firms" list and was recently recognized as one of "America's Best Tax Firms" by *Forbes*. PKF O'Connor Davies was named one of *Vault's* 2022 Accounting 50, a ranking of the 50 best accounting employers to work for in North America and ranked among the top 50 most prestigious accounting firms in America in a complementary *Vault* survey.

PKF O'Connor Davies is the lead North American representative of the international association of PKF member firms. PKF International is a network of legally independent member firms providing accounting, tax and business advisory services in over 400 locations in 150 countries around the world. With its tradition, experience and focus on the future, PKF O'Connor Davies is ready to help clients meet today's ever-changing economic conditions and manage the growing complexities of the regulatory environment. For more information, visit www.PKFOD.com.