Cyber Roundup – May 2021

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

As we finalize this issue of *Cyber Roundup*, the ransomware attack on Colonial Pipeline is fresh in the minds of the American public. It's especially distressing as it upsets the availability of gasoline along the east coast just as we are coming out of pandemic mode and ready to jump in our cars for spring travel.

Our readers are aware that ransomware threats are becoming more dominant and common. Extortion demands by threatening actors increased dramatically in 2020, with 61% of companies being attacked. Targets include businesses, government agencies, educational systems (K-12, colleges, and universities) and individuals. No one is exempt or safe from these bad actors. The average ransom paid in 2020 was $312,000 with an all-time high payment of $5 million in 2019. Coincidentally, Colonial Pipeline paid hackers $5 million in ransom to restore its systems and get gasoline flowing again; but will that only embolden these bad actors and invite more malware attacks? Perhaps the time has come to prohibit all ransomware payments.

Lack of training, lack of cybersecurity preparedness and not having a set plan in the event an attack does occur exacerbates the damage that can be done if attacked. Training, planning, and engaging with us to help identify problems, harden your cyber infrastructure and create solutions will help you **Know Greater Cybersecurity**.

Key Cyber Events

The following is a rundown of what happened during the month of April 2021. We welcome your comments, insights and questions.

- **Large-scale cyberattack presents greater risk than another financial crisis like that of 2008.** As the world evolves, cyber risk is the main concern shared by institutions and governments, especially those in the finance sector. What would happen if our financial institution payment systems were compromised? Federal Reserve Chairman Jerome Powell, supported by Janet Yellen's recent comments, both believe it is our obligation to consider the possibility of a United States digital currency. However, the U.S. is in no rush to be first in this space; getting it right and ensuring consumer protection must be the foundation of this effort.

- **Nation state attacks increase 100% in three years.** Direct intelligence shows an increase in sophisticated structures that transect with underground cybercrime. COVID-19 has created a hotbed of opportunity for attacks on both digital and physical assets. Acquiring IP data relating to COVID-19 is typical of how nation states are both the provider and the receiver in cybercrime economic activity. These types of attempts against software supply chains show how far nation states are willing to go to prey on their victims. "Atypical purchasers" account for 10% to 15% of dark net vendor sales.

- **Number of reported U.S. breach victims jumps 564% in Q1 2021 with over 51 million consumers affected.** The numbers show an alarming pattern of supply chain breaches which in the first quarter of 2021 saw a 42% increase over Q4 2020. Comparatively, while the volume of breaches only increased slightly, the disparity in numbers is a result of how a single breach may impact numerous organizations and victims.

- **Compromised emails cost businesses $1.8 billion to resolve in 2020.** Since 2019, studies have shown extortionware (a.k.a. ransomware) is dominating the cybersecurity arena. News cycles suggest a much lower rate of incidents perhaps due to under-reporting or payments being made by third parties. However, those payments pale in comparison to business email

compromise (BEC). A BEC attack is usually delivered electronically by creating a fraud via email addresses (spoofed or real), insertion into a real conversation or imitating an employee. These attacks are very adept at evading detection.

BEC attacks are brought against people, so it is imperative to include technology, training, and awareness campaigns as part of your defense. Email fraud prevention solutions should be broad-based and can help reduce the risk of being compromised. There are no silver bullets, so being aware of every type of threat you may be exposed to is key to your security.

Tom's Takeaway: When looking at the three prior bullet points, one thing is certain, the cyber risk is growing and evolving. As a business or an individual, the decision is yours to take action and defend against the cyber threat or roll the dice and hope luck is on your side. The core mission of the *Cyber Roundup* is not only to bring awareness of the issue, but to empower you on how to find the solution. Great battles are never won alone; let us partner with you should you decide to take on the cyber threat.

- **FBI arrested a man for allegedly planning a bomb attack against Amazon Web Services (AWS) to kill about 70% of the internet.** In late January, Seth Aaron Pendley began collaborating with another source to acquire C-4 plastic explosives to allegedly be used in an attack on a well- known tech company's data center, with the intent to "conduct a little experiment." An elaborate undercover FBI operation ensued and in April, after purchasing the "fake" explosives from an agent, Mr. Pendley was arrested. He chose the AWS center as he believed it housed the web servers for the FBI, CIA, and other federal agencies. His plan was to kill "the oligarchy" presently in power in the U.S.

- **Attackers target VPN vulnerabilities.** VPN access was one of the top three access points sold on cybercriminal sites. Attackers find VPN appliance vulnerabilities in a variety of places. Russian and Chinese actors have affected several organizations within the U.S. Currently there are 12 separate malware families targeting VPN vulnerabilities. Targeting Remote Code Execution (RCE) flaws is yet another vulnerable access point for cyber activity. RCE failings were **THE** most common flaws exploited. RCE abuses account for 23% of the attacks.

  Tom's Takeaway: Remote work and remote access is without question something that will persist in a much larger capacity in the post-pandemic world. Not all remote access is created equal, with each method having unique risks that need to be considered. As you look toward the future, now is a prudent time to reevaluate your remote access solutions and ensure that they will support both the operational and security factors necessary to sustain your future success.

- **European law enforcement automatically wipes Emotet malware from infected systems across the world as part of a mass sanitization operation.** Emotet is classified as a banking Trojan; a piece of software that once installed steals sensitive data and spies on the infected machine. Operation Ladybird, which disrupted the EMOTET botnet, was a coordinated effort by Europol and Eurojust. Authorities, once in control of the operation, issued commands to uninstall the malicious software on the compromised machines. The U.S. Department of Justice issued an affidavit confirming this sanitization. Recently, spam campaigns have used malicious messages or links in fake invoices, shipping documents, COVID-19 information, resumes, and financial or scanned documents.

  Between April 1, 2020 and January 17, 2021 foreign law agencies, together with the FBI, lawfully accessed international Emotet servers and identified the IP addresses of approximately 1.6 million computers – 45,000 of these computers are in the U.S. The FBI also released the e-mail addresses used by Emotet. To check if your address was included, click here.

- **According to the U.S. Department of Justice (DOJ), phishing attacks used vaccine surveys to steal personal information.** Vaccination surveys received via email or text are sent to victims for completion with the lure of prizes for their efforts. Victims supply credit card and personally identifiable information (PII) which leaves them totally exposed to scammers and potential identity theft. The DOJ suggests not clicking on any links received through email or text that come from unknown sources. Victims are urged to report any fraudulent activity to the National Center for Disaster Fraud (NCDF) via the NCDF Web Complaint Form or by calling 866-720-5721.

- **Lazarus hacking group now hides payloads in BMP image files.** The Lazarus group, one of the most sophisticated advanced persistent threats (APT) from North Korea, is responsible for global attacks. Lazarus employs a unique method targeting payloads in image files. A phishing document is launched, the victim is asked to enable macros (i.e., software) to view its content, which automatically deploys a malicious payload. Once activated, the software infiltrates with a Remote Access Trojan (RAT) that allows the cyber criminals to take control of the victim's machine.

  Tom's Takeaway: If you follow *Cyber Roundup* or have listened to me speak, you know I'm a big believer in the importance of cyber security awareness training for employees. The prior two bullets underscore the importance of training your employees to protect not only themselves but also to protect the business. Your employees are your greatest asset in this cyber security battle. In order to win this battle, you need to arm them with the necessary knowledge. If you need assistance in creating an effective cyber security awareness training program, please feel free to reach out to me.

- **Experian API exposed credit scores of most Americans.** A sophomore at Rochester Institute of Technology searching for student loan vendors discovered an Experian data vulnerability in an Experian partner's website. While viewing the code behind his lookup page, he noticed it cited an Application Programming Interface (API) that is related to FICO credit scores. The Experian API allowed this person to pull anyone's credit score without any authentication. Having a security freeze with the three major credit bureaus prevents this particular API from accessing information. Upon being contacted, Experian worked with the offending vendor and the API has been disabled; however, it is believed this solution does not address the systemic issue. In the hands of identity thieves unsecured APIs can be devastating.

- **Fraudsters steal GEICO customers' driver license numbers.** The breach, which occurred between January 21 and March 1, affected an unspecified number of GEICO clients. This breach could serve as a pathway for fraudsters to apply for unemployment benefits in another person's name in states where this information is required. Exploitation of weaknesses in auto insurance websites allows cybercriminals access to this information.

- **Former employees hack into water utility servers with harmful intent, potentially affecting residents' drinking water.** Luckily, these breaches were discovered before any resident was exposed to contaminated water. Lack of firewall protections, remote access to "supervisor control and data acquisition" (SCADA), as well as failing to cancel ex-employee credentials and access, are to blame.

- **Dutch Data Protection Authority (DPA) imposes huge fine on Booking.com for slow data breach reporting.** The fine imposed considered not only the breach itself but the delay in reporting this incident to the local authority. At the time of the breach, over 4,000 customer accounts were compromised. Criminals accessed booking details, names, addresses, phone numbers and CVV security codes. Booking.com became aware of this breach on January 13, 2019, however, did not report the incident until February 7, 2019. Legally, companies have 72 hours to notify authorities from the time they become informed of the breach. Losses can be mitigated by training employees to recognize social engineers, creating a place to report suspicious activity, and having a set plan in place to address a breach should one occur.

  Tom's Takeaway: For many businesses in the U.S., General Data Protection Regulation (GDPR) seems like a thing of the past. GDPR was the first of its kind privacy legislation implemented in Europe that requires any business that processes the personal information of a European resident provide transparency in how they handle that information and also empowers the individual to have greater control of their information. GDPR requires that any breach of personal information be reported to the authorities in 72 hours. The importance of having a privacy program cannot be understated. While the U.S. does not have any comprehensive federal law like GDPR, the states are actively creating similar GDPR-type legislation. If you are not certain of the privacy implications for your business and need assistance, please feel free to contact us.

Contact Us

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

PKF O'Connor Davies, LLP
665 Fifth Avenue, New York, NY, 10022
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, fourteen offices in New York, New Jersey, Florida, Connecticut, Maryland and Rhode Island, and more than 800 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 27th on *Accounting Today*'s 2020 "Top 100 Firms" list. It is also ranked among the top 20 best accounting employers to work for in North America by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.