Cyber Roundup – June 2020

By Thomas J. DeMayo, Principal, Cyber Risk Management

While putting together this issue of *Cyber Roundup* compiling cybersecurity incidents occurring in May 2020, I was brought back to my first personal encounter with a computer virus. I can even give you the date – May 5, 2000 – 20 years ago. As a kid, I was always fascinated by computers, with the Commodore 64 being an early favorite of mine.

I was in college on May 5, 2000 when the ILoveYou Virus hit infecting 50 million machines and causing upwards of $15 billion in damages. At that time, this was one of the very first highly destructive social engineering attacks. I remember staring at my screen incredibly frustrated at what just happened to my computer, but at the same time, amazed at the damage caused by this little text file that made me believe someone had a crush on me.

Twenty years later, the ecosystem of computer security remains foundationally the same – poorly coded systems and the manipulation of human emotions to gain entry. This has been, and continues to be, my objective over all these years: help businesses and individuals secure their systems, tell them what's out there in the way of danger, and turn the tide on the current wave of cyber threats.

Key Cyber Events

The following is a rundown of what happened during the month of May 2020. We welcome your comments, insights and questions.

- **The Department of Homeland Security and the FBI published a report on the 10 most commonly exploited software vulnerabilities over the past four years.** The DHS and FBI are urging all businesses to review the listing and ensure that the necessary software fixes have been applied. The details of the report can be found here.

Tom's Takeaway: This report serves as a reminder that a strong process of consistently identifying and applying software patches is a key component of your cybersecurity program. I encourage you to take this listing provided by DHS and the FBI and ensure your IT Department or IT Managed Service Provider has installed these fixes.

- **The law firm of Grubman Shire Meiselas reported a ransomware attack.** The law firm services many famous celebrities and high profile individuals. The cybercriminals threatened to expose approximately 1 Terabyte of celebrity data obtained in the attack unless the ransom is paid. Data obtained consisted of contracts, telephone numbers, e-mails, personal correspondence, etc. The cybercriminal group believed to be behind the attack is known as the REvil Ransomware Group or Sodinokibi [say that three times].

- **The same cybercriminal group, REvil Ransomware Group, that targeted the law firm to the stars, also targeted President Trump.** REvil demanded $42 million in cryptocurrency to avoid the distribution of information on the President. Later in the month, the group claimed to have sold the information to an "interested party."

Tom's Takeaway: Law firms are key targets for cybercriminals because of the extent of sensitive information they possess. If your law firm needs assistance in understanding and managing its cyber risk, please feel free to contact us.

- **A grandmother was ordered by an EU court to delete Facebook photos of her grandchildren in accordance with the General Data Protection Regulation (GDPR).** After a breakdown in relations between mother and daughter, the daughter requested that the grandmother delete the photos of the children from the grandmother's social media. The courts sided with the daughter and instructed the grandmother to remove the pictures or pay a fine.

Tom's Takeaway: When we think about privacy regulations, we naturally associate them with big corporations and their conduct and don't think of it in terms of our own personal actions. Albeit that the bulleted item may be an extreme example, I believe this ruling is significant because it emphasizes that we – as individuals – have a responsibility (no different than a business) to value, protect, and handle the personal information we obtain with care and consideration.

- **An international group of criminals was identified as having targeted state unemployment systems stealing hundreds of millions of dollars.** The state of Washington was the hardest hit; however, multiple other states have also reported being targeted. The criminals, leveraging stolen identity data from previous breaches, submitted unemployment claims. In an effort to quickly respond to the tidal wave of unemployment claims, the states initially emphasized speed of processing over fraud detection when providing funds to those in need. The states began to realize the issue when those who had not filed for unemployment received postal mail indicating they had. These states have since added measures to prevent any further fraud; however, such measures come at the expense of delayed payments to those in need.

- **In a report released by the Federal Trade Commission, U.S. victims suffered $13 million in losses from COVID-19 scams.** The top 5 products or service scams by number of reported cases are as follows:

Product or Service	Reported Cases	Dollar Loss
Travel/Vacations	2,853	$4.8 Million
Online Shopping	1,804	$1.45 Million
Mobile: Text Messages	1,039	$78 Thousand
Internet Information Services	390	$171 Thousand
Imposter: Business	384	$1.2 Million

In a separate and unrelated study, fraud prevention company, Bolster, reported that it detected 250,000 websites devoted to COVID-19 scams.

Tom's Takeway: Whenever looking at articles regarding published losses, always keep mind, this is what has **been reported** and **is known**. The reality is, the true losses and the extent of the scams are more than likely far greater.

- **Duncannon, a borough of Perry County in Pennsylvania, suffered a ransomware attack that resulted in the municipality paying $35,000 to regain access to their data.** The cybercriminals initially set the ransom at $50K; however, it was negotiated down to $35K. The municipality was left with no option but to pay as a result of their backups also being encrypted by the ransomware.

- **Duncannon was not alone in ransomware attacks in May.** The following entities also experienced ransomware incidents:

  - **The Texas Court system** was forced to disable its website and shutdown servers in response to a ransomware attack that affected a portion of its network. It is not believed any sensitive information was compromised in the attack.
  - **Alleghany Intermediate Unit, Homestead, PA,** suffered a ransomware attack that affected their operations.
  - **Bernard's Township, NJ**, suffered a ransomware attack on their network operations.

Tom's Takeaway: While many large corporations have embraced the need to ensure adequate funds on developing a cybersecurity program, many small to medium businesses, especially municipalities, have yet to make the necessary investments. While no system will ever be 100% secure, the extent of companies and other organizations that fall prey to cybercriminals as a result of easily preventable measures (such as a safe backup) remains disappointingly high. If you have not already done so, I encourage you to shift your view of cybersecurity as a business expense to that of an investment – an investment in the future sustainability and profitability of your business. If you need assistance in how to best manage that cybersecurity investment in the future of your business, please contact us.

- **Supercomputers across the EU were breached and infected with cryptocurrency mining malware.** Infections were reported in the UK, Switzerland, Germany and Spain. The infections led to the supercomputers being shutdown to investigate the issue. It is believed that the breach was the result of compromised credentials which were then subsequently used to install the malware.

- **The FBI and the Department of Homeland Security released an alert that the Chinese government may be targeting organizations that are performing research related to COVID-19.** The Chinese threat actors have been observed trying to identify and obtain intellectual property pertaining to vaccines and treatments for COVID-19. The FBI and DHS encouraged those organizations performing the research to maintain and enhance their cybersecurity and insider threat programs to protect their valuable information.

- **Home Chef, a meal delivery service, reported a breach that impacted approximately 8 million customer records.** Information consisted of name, address, phone, last 4 digits of the payment card, encrypted passwords, and other account information. The cause of the breach has not been reported and is being investigated.

Contact Us

Thomas J. DeMayo, Principal, Cyber Risk Management
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, twelve offices in New York, New Jersey, 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.