# Cyber Roundup – September 2022

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

Cybercriminals predictively continue to outdo their tricks in enticing us to fall for their money-making ploys. This month you will see that call-back phishing – which evades computer security filters – has become popular. You will also note how USB drives are used to allow for hacking into computers to install malware with the intent of a payoff. Scamming the elderly hit a new high with cybercriminals sending an Uber car to enable the victim to get to the bank conveniently to wire money.

There are lessons to be learned to avoid various cyber tricks just by reading *Cyber Roundup* and incorporating some of the incidents into your cybersecurity awareness training. Or, you can call on us for assistance.

## 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.

- **The FBI, CISA and MS-ISAC issued a joint advisory alert noting that they have observed cyber actors "disproportionately targeting" the k-12 education sector with ransomware attacks**. The alert came on the heels of the Los Angeles Unified School District, one of the largest districts in the U.S., notifying that they had been targeted with ransomware. While the disruption appeared to be limited and the ransomware gang allegedly did not request a ransom, the district's School Board approved an emergency declaration removing the need for competitive bidding as it relates to cybersecurity contracts to expediate enhancements.

- **Elmbrook School District in Wisconsin suffered an attack that resulted in student records and employee data publicly posted on the Dark Web.** Vice Society is the ransomware organization that has claimed responsibility for Elmbrook and Los Angeles School District attacks. As with Los Angeles, the attack did not result in a ransom demand.

  ***Tom's Takeaway:*** $3.56 billion was lost by U.S. schools to ransomware attacks in 2021. The education sector, public or private, has been and will likely remain a very active target for cyber criminals. Many schools unfortunately don't have and have not been afforded the resources to have a fighting chance. We commend the Los Angeles school district for eliminating competitive bidding for a period to hasten the response and to shore up their defenses; however, like most, the response is reactionary. We have actively worked with many k-12 public school districts and private schools to understand and manage their cyber risk. If you need assistance in taking a proactive stance against the cyber threat, we stand ready to help.

- **In a report issued by the DOJ, titled *Comprehensive Cyber Review*, the DOJ warns of the "blended threat."** The blended threat is that of nation states and criminal actors forming alliances of "convenience, alliances of opportunity and sometimes alliances by design." These alliances operate such that some nation states will ultimately function as a safe harbor for the cyber criminals allowing the illegal activity without consequence.

- **In a report issued by Agari, call-back phishing attacks have increased 625% since Q1 of 2021.** A call-back phishing attack is a hybrid form of a social engineering attack that combines an initial email and a follow-up phone call. The emails will be designed as such to entice the victim to call a number. Once the call has been performed, the cyber criminals will manipulate the victim over the phone to perform additional actions such as giving them access to the victim's machine to perform some type of malicious function.

***Tom's Takeaway***: One of the common traits we have noticed with these hybrid attacks is the initial email does not include any clickable links or attachments. The primary motive is the call-back. By eliminating links and attachments, not only does the email have a better chance of bypassing the security filters, but it also avoids the heavy emphasis placed on the suspicion and avoidance of links and attachments during cybersecurity awareness training. As with any training, it is only as good as yesterday's knowledge. Take this opportunity to ensure your trainings also factor in voice phishing and other phone related tricks such as caller id spoofing.

- **The FBI issued an alert of cyber criminals utilizing compromised home machines and networks to commit large scale credential stuffing attacks.** Credential stuffing is a tactic in which a list of compromised usernames and passwords is utilized against various other sites to gain access. Access is obtained because users have a tendency to employ the same credentials across many sites. By leveraging home networks, the attacks are harder to block increasing the likelihood of success for the cybercriminal.

  ***Tom's Takeaway:*** The prior bullet should serve as a reminder that cybersecurity is an issue that can have very serious implications personally and professionally. In an ever increasing digital and connected world, we all need to work together to protect each other. That protection can start by simply reading this newsletter and adopting the lessons learned from all those that have been victimized.

- **Scammers in the UK have been spotted sending Microsoft branded USB drives to random addresses in an effort to compromise the machines with malware.** The USB drives are delivered with a note that the individual has received a free Office Professional Plus install. Once connected and the installation started, the victims are prompted to call a fake support line. Once connected with the support line, they will be enticed to allow the fake support representative access to their machine. The ultimate goal is to eventually persuade the victim into sending money.

- **Hanesbrands Inc. disclosed that the ransomware attack it suffered in May cost it about $100 million in sales for the second quarter.** The attack resulted in the inability to fulfill orders for approximately three weeks. In addition to the $100 million in lost sales, a $35 million reduction in adjusted operating profit was incurred.

- **Baker & Taylor, one of the largest distributors of books to libraries worldwide, suffered a ransomware attack.** The attack impacted the company's phone systems, service centers and offices. The Company has stated it will not pay the ransom.

- **In an article released by KrebsOnSecurity, email scammers went as far as sending an Uber to the personal residence of an 80-year old woman to help her get to the bank and wire money to them.** The woman initially responded to an email regarding an appliance installation. The timing of the email was beneficial to the fraudsters as the woman's dishwasher had recently failed and had purchased a new one and was awaiting delivery and installation. Fortunately, no money was transferred. If you are interested in the full story, it can be found here.

## 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