Cyber Roundup – October 2022

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

It is not uncommon, when we do client assessment and process reviews, that we find many great policies exist; however, they are not well-communicated to those who need to execute them nor are the details delineated. This goes back to awareness, training and communication. While many of you may have adopted online security awareness training that has generic content, it may not communicate specific actions. Your designated managers must take this on when projects arise and communicate the particulars to those who will be executing the assignment. Cybersecurity is just as much about process definition and communication as it is about technology.

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.

- **Security researchers at Proofpoint have identified an Iranian hacking group implementing a new phishing technique which Proofpoint has dubbed "multi-persona impersonation."** The technique works by leveraging multiple identities from various compromised accounts to entice the target into believing the legitimacy of the e-mail and thread. For example, you may receive an e-mail with multiple other individuals cc'd on that e-mail. Since the attackers also have control of those cc'd accounts, they will begin to respond from those accounts creating what appears to be a legitimate conversation. By utilizing multiple accounts with active conversation, it leverages the psychology principle of social truth to add elements of legitimacy to the e-mails. Eventually, the target will be sent either a link or attachment with the intent of compromising the machine.

  Tom's Takeaway: At its core, social engineering is the act of manipulation of a person's emotions to trigger a response. Our brains have learned to process various social cues and associate them with trust. In this case, the active dialogue makes the thread that much more real. As you evolve your training programing, part of what your end goal should be is to re-wire those learned behaviors through continued awareness of the tactics used. While it bothers me personally that I have to say *assume all communications are not trustworthy until proven so*, that is the unfortunate reality of the digital world in which we live.

- **The SEC has fined Morgan Stanley $35 million for its failure to protect personal information of their clients**. As far back as 2015, Morgan Stanley did not properly and securely dispose of devices that contained client information. The release provides an example of Morgan Stanley using a moving company with no prior experience or qualifications in secure data destruction to decommission thousands of hard drives that contained client information. The drives, which were unencrypted, were sold as is by the moving company on an internet auction site. Morgan Stanley has settled with the SEC and agreed to pay the fine without admitting or denying the findings. The full release by the SEC can be found here.

- **The FBI issued an alert that cybercriminals are actively targeting DeFi (decentralized finance) cryptocurrency platforms costing investors $1.3 billion in the past three months.** The alert notes that the theft is often the result of vulnerabilities in smart contracts. The FBI is actively calling on the DeFi community to adopt real time monitoring and response processes as well as increase the extent of software code security review and testing.

- **Cybercriminals are increasingly utilizing a tactic dubbed "MFA Fatigue" to bypass a company's MFA (Multi-Factor Authentication) implementation.** The attack works by continuously logging into a site or application with the correct username and password causing the user whose credentials have been compromised to continuously receive push (pop-up) notifications. These notifications can continue hours on end, effectively resulting in the targeted user accepting the push and granting the cyber criminal access. As you evaluate the effectiveness

of your MFA solutions, in addition to educating employees of this tactic and what to do if it occurs, ensure that you have monitoring controls to alert to continuous push attempts in a defined period.

- **The IRS reported a data leak that impacted 120,000 taxpayers.** The issue was tied to those that filed a 990T which is used to report unrelated business income to a tax-exempt entity, such as non-profits or retirement accounts (IRAs). For the tax-exempt entities, that information ultimately is made public; however, for individuals, that information is to remain confidential. When the IRS shared the data on the non-profit entities they also erroneously shared the data on taxpayer IRAs that were not intended to be publicly accessible. While the IRS states the data did not include sensitive information, such as a Social Security Number, it has started alerting those impacted individuals.

- **The country of Albania has become the first to sever ties with another county in response to a cyberattack.** Albania had suffered a cyberattack in the form of ransomware from Iran that ultimately destroyed government data, took down services and attempted to exfiltrate data. Albania responded by severing all diplomatic relations and expelling Iranian embassy staff from the country.

- **The following are key ransomware events in September**:

  - SetinelLabs reported that ransomware gangs are adopting a technique called “intermittent encryption” to significantly increase the speed at which the ransomware can encrypt files, reducing the chance of being identified or stopped. The technique works only on encryption portions of the file and not the whole file. The file is still rendered useless to the victim without the encryption key; however, the process is now significantly more efficient.

  - In last month’s **Cyber Roundup**, we noted that Suffolk County, LI, NY and Los Angeles, CA Unified School District, suffered ransomware attacks; however, they both claimed no such ransom had been demanded. As time passed, both eventually reported that the ransomware gang has demanded a ransom. Suffolk County and LAUSD have both had their stolen data published to the dark web by the ransomware gang for their refusal to pay since we published our **Cyber Roundup** last month.

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