# Cyber Roundup – August 2018

By Thomas J. DeMayo, Principal, Cyber Risk Management

No doubt you have noticed some of the interesting "lingo" associated with the cyber world whether reported in *Cyber Roundup* or otherwise. Below are general meanings of some of the more noteworthy terms. Always amazing to see how common English words can be morphed into such descriptive cyber terminology.

**Cloud storage**: a backup and storage service on the internet. Providers generally let users upload any size and type of computer file. Many providers offer this service for free (aka "freemium") for limited storage; higher capacities are available for monthly fees.

**Keylogger**: is a computer program (often deemed "spyware") that records every keystroke made by a computer user generally to gain fraudulent access to passwords and other confidential data. The log may be saved to a file or sent to another device over a network.

**Remote Desktop Protocol (RDP):** provides remote access to individual computer devices for network administrators so they can diagnose and resolve cyber problems.

**Spear phishing**: customized email attacks with the target's name, position, company, work phone number and other specific personal information to trick the recipient into thinking they have a connection to the sender.

**Sandbox**: a security mechanism for separating and isolating running programs in an effort to mitigate system failures or software vulnerabilities from spreading. Generally, programs running in the "sandbox" have limited access to your files and system.

**Key Cyber Events**

The following is a rundown of what happened during the month of July 2018. We welcome your comments, insights and questions.

- **Research conducted by Positive Technologies identified that the demand for dark web cybercrime services outpaced supply threefold.** The assessment included the analysis of approximately 10,000 hack-for-hire and malware postings in dark web marketplaces. The following interesting findings were noted in the research:

  - The overall cost of cybercrime as a service is decreasing. The following service price tags were as follows:

    - ATM logic attacks: $1,500+
    - Targeted business attack: $4,500+
    - Web application hack and takeover: $150+

  - Cryptomining malware accounted for 20% of the malware for sale, trailed (in order) by hacking utilities, botnet malware, remote access Trojans and ransomware. As noted over the past couple of months, the decrease of ransomware across the board has become the general trend as cybercriminals favor crypto malware.

  - Hack-for-hire requests involved finding vulnerabilities at 36%, trailed by stealing email passwords and hacking social network accounts.

- **In separate news related to dark web sales, McAfee researchers identified credentials for sale to Windows-based servers using the Remote Desktop Protocol (RDP) for as little as $10.** Included in the listing were credentials that would provide access to the security system of a major international airport. This research is a sobering reminder that we must stay vigilant in our cyber defenses.

- **The Boys Town National Research Center reported the largest breach to date affecting a pediatric or children's hospital.** Sensitive data on 105,000 individuals is believed to be part of the breach. The issue was first identified when unusual activity was spotted with an employee's email account. While no activity has been identified with the information being used, it was only a few months back that we included in our *Cyber Roundup* a report that the personal information on children is some of the most valuable. The value is driven by the extended period of time the information may be used before it is noticed. If you have assessed your cyber risk and have not factored in the exposure through email, you have overlooked a large piece of the cybersecurity puzzle.

- **ComplyRight, a cloud-based human resources company, announced that it may have been the victim of a breach through its website that exposed a treasure trove of client/employee sensitive personal information.** This breach comes on the heels of the FBI releasing private industry notification alerting that cyber criminals have been increasingly utilizing social engineering techniques to obtain access to employee HR self-service portals in an attempt to divert payroll. Human resources departments and services are some of the highest risk areas of any business. As such, this is one of the areas where cyber defenses need to be the highest. If you would like a copy of the alert, please contact me directly.

- **Macy's, New York-based B&B Hospitality Group, Adidas, and LifeLock all reported breaches of customer data.** ***Macy's*** has not disclosed the number affected, but noted the incident was the result of breached employee credentials used to access customer data associated with Macys.com and Bloomingdales.com. ***B&B Hospitality Group***, operators of nine New York restaurants (Del Posto, Babbo, Casa Mono, Becco, Otto Enoteca e Pizzeria, Esca, Lupa, Tarry and Felidia) was subject to the known classic, point-of-sale breach, exposing customer payment information. The ***Adidas*** website was breached with the attackers gaining access to the back-end servers and millions of customer details inclusive of their encrypted passwords. ***LifeLock***, a company routed in the protection of personal identities, fixed a vulnerability on their website that allowed anyone to identify the email accounts associated with their customers. While the vulnerability doesn't directly cause harm, this type of information can be used for phishing attacks against those customers.

- **A sophisticated and highly targeted mobile malware campaign was identified targeting iPhones.** It is believed the attack has been operating since August 2015. The attack tricks users into downloading an open source mobile device management software. Once installed, given the nature of the mobile device management package, the attackers can take complete control of the device performing such functions as tracking the user's location, enabling the microphone and camera, and stealing contacts, photos, text, and messages for messaging and chat apps. It is not yet known who is behind the attack; however, the attackers have tried to make it look like it was Russian-based.

- **Medical testing giant LabCorp and Chinese shipping giant COSCO suffered Ransomware attacks.** ***LabCorp*** has not disclosed the extent of the damage but has noted the attack affected only the diagnostic network, slowing down test processing and delaying customer access to test results, but has not affected the development component of its operations. The hackers demanded a ransom of $6,000 in bitcoin for each infected machine or $52,500 to unlock all the machines. The company has opted to replace the machines and will not pay the ransom. The attack against ***COSCO*** was only successful in taking down the email and phone network and did not impact the operations of their shipping fleet.

- **In the wake of GDPR (General Data Protection Regulation) going into effect on May 25, 2018, the EU parliament is pushing for the U.S. Privacy Shield to be revoked until the U.S. program complies with necessary data protection mechanisms.** While it may be hard to believe, the U.S. — in the eyes of Europe — is not considered as having adequate safeguards universally to allow for the legal transfer of EU personal data to U.S. companies. The Privacy Shield is an elective program that a U.S.-based company can participate in and certifies that the company has the necessary privacy practices in place to protect EU personal data, thus allowing

for the transfer of EU personal data. The Commission is calling for the U.S. to be fully compliant by September 1 or recognition of the Privacy Shield may be suspended.

- **A sextortion scam has been making its rounds sending people into a panic.** The scam involves an email that is sent to the individual with the cyber criminals claiming to have compromising information on them — including explicit pictures and websites accessed (or made a recording of the individual while they were watching those websites) — that they will share with all the victim's friends and family unless a ransom is paid. To make the scam seem legitimate, the email will include a known password associated with the email account. If the victim doesn't pay the ransom, the cyber criminals threaten they will send that compromising information to all of their contacts. What makes this attack very real and scary is that the password contained in the email is a real password of the user; however, that information was not obtained directly from the victim's computer device(s). Rather, the attackers pulled the information from the dark web. So while the credential is real and the hackers have it, they did not obtain it from the victim's computer device and they do not have the information that they claim. We have witnessed this scam first hand as we assisted a number of our clients. We have extensive dark web monitoring capabilities and, for the clients who contacted us, we were able to identify that the credentials were in fact located in the dark web for sale in ID theft forums.

## 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, nine offices in New York, New Jersey, Connecticut and Maryland, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 29th on *Accounting Today's* 2018 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today.* In 2018, PKF O'Connor Davies was named one of the 50 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.