Cyber Roundup – November 2017

By Thomas J. DeMayo, Principal, Cyber Risk Management

Seem like cyber villains are "equal opportunity" predators. Whether you're an adult or an adolescent, affluent or average — or your business is for-profit, non-profit, publicly-listed or government-related — you personally, or as a member of a group, can be impacted by cyber misdeeds. Complacency is not an option. Just being aware of what's going on may help you recognize red flags and possibly avert or mitigate negative consequences. Realizing that you may have to enlist the help of IT consultants, we hope that at that time you will consider PKF O'Connor Davies.

Key Cyber Events

The following is a rundown of what happened during the month of October. We welcome your comments, insights and questions. Please contact Tom DeMayo, Principal, Cyber Risk Management, to explore how we may help you safeguard the security of your organization, business, clients and constituency.

- **Hackers set their sights on K-12 schools prompting the U.S. Department of Education to issue a warning.** The alert, found here, advises teachers, parents and education staff of the cyber attacks targeting school districts across the country. It is reported that these cyber criminals seek to extort money from school districts and other educational institutions on the threat of releasing sensitive data from student records and also includes threats of violence, shaming, or bullying the children unless payment is received. The advisory gives key steps schools should take immediately. Schools need to acknowledge that they can and will be targeted by cyber criminals and, therefore, need to establish a reasonable and sound cyber security program.

- **Researchers identified significant security concerns on children's smartwatches.** These devices could easily be targeted to take control of the device and spy on children by eavesdropping or tracking their location. The FBI issued an alert in July speaking to this concern. As a parent or guardian, you need to be cautious of any internet-connected device used or worn by your children. Rule of thumb: if you can access the device remotely, someone else who is not authorized could also potentially access that same device remotely.

- **Accenture, a global consulting firm, exposed a treasure trove of sensitive information in an unsecured Amazon S3 storage area.** The data exposed consisted of authentication credentials, certificates, decryption keys and customer data. If accessed by malicious individuals, they would have a lot of valuable information to target both Accenture and their clients. Over the past six months, we have reported on a number of instances where Amazon services have been configured incorrectly placing sensitive information at risk. While the cloud has some inherent security benefits, it still needs to be properly designed, secured and assessed to protect the data it holds.

- **Another major ransomware campaign — dubbed Bad Rabbit — swept the globe in late October.** Similar to other major ransomware attacks, WannaCry and NotPetya, the cyber criminals used the NSA exploits exposed by the hacking group, the Shadow Brokers, in April. The malware was being spread by a fake Adobe Flash update installer. Once a machine is infected, it will try to spread across the network, infecting additional machines. Unlike WannaCry and NotPetya, it will also try to steal credentials from the infected machine. Microsoft released a patch

back in March that would protect against the spread of these ransomware variants using the released NSA exploits. If you have not done so, ensure all your machines are patched with MS17-010.

- **Dark web vendors have been identified selling remote access to corporate systems for as low as $3.** The sale includes credentials to compromised remote desktop protocol ("RDP") accounts around the globe. RDP is a popular choice for companies when establishing a remote access solution. While remote access to company resources is common, it needs to be properly secured to manage the risk of the exposure it creates.

- **Hyatt Hotels and Pizza Hut announced they suffered a credit card data breach.** For Hyatt, this is the second credit card breach in the past two years. The breach affected Hyatt-managed locations between March 18, 2017 and July 2, 2017 and affected payment card information either entered manually or swiped at the front desk of certain locations. A listing of affected locations can be found here. For Pizza Hut, the breach occurred as result of a vulnerability in its website. It is believed the breach occurred between October 1, 2017 and October 2, 2017 and resulted in approximately 60,000 customer credit card records stolen.

- **A major wireless vulnerability was identified placing Wi-Fi networks and devices around the world at risk.** The Wi-Fi vulnerability — dubbed KRACK — takes advantage of a flaw in the now standard WPA2 cryptographic protocol. If leveraged, the attacker could potentially read or modify data on the network that would otherwise be protected. This could expose sensitive information such as passwords and financial data or allow the attacker to manipulate data in transit potentially resulting in the unauthorized transfer of funds. Patches are being released to correct the vulnerability. It is important that you inventory the wireless devices on your network and apply the patch as soon as possible. In the interim, manage the risk by not connecting to public wireless networks and using a trusted VPN to secure the traffic across any wireless network.

- **The Equifax credit assistance website was identified as distributing malware.** Upon visiting the website, users were prompted to download a fake and malicious update for Adobe Flash Player. It was determined that the malware was not being distributed directly by Equifax, but by the code provided by a third party vendor Equifax was using to collect website performance data. Prior to the incident, Equifax had been awarded a $7.2 million contract by the IRS to help verify taxpayer identities and prevent fraud. As a result of the recent data breach and this incident with malware distribution soon after, the IRS dropped its contract with Equifax.

- **Researchers identified a flaw in LG's smart home software that could allow attackers to remotely control the smart devices and spy on homeowners.** The flaw— being dubbed HomeHack — targets the app that is used to control the devices remotely. One of the appliances affected is a vacuum cleaner that also serves as a security monitoring system. A security camera mounted on the vacuum cleaner will detect movement in the home and alert the homeowner who can then switch-on the camera to see what is happening. Leveraging the flaw, the attackers can turn on the camera at will and spy on the homeowners. LG has released an update to the SmartThinQ app to correct the issue.

Contact Us

Thomas J. DeMayo, Principal, Cyber Risk Management
CISSP, CISA, CIPP/US CPT CEH CHFI MCSE

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 28th on *Accounting Today's* 2017 "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 2017, 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 440 locations, in 150 countries around the world.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind