October 9, 2018

TLP White

We start with a look at how countries are using name and shame tactics to deter cyber criminals. We also discuss the recent Facebook breach and the concerns that it raises around third-party apps and authentication. We conclude by shedding some light on a new law in New Zealand permitting custom agents to search digital devices. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Playing the Name and Shame Game.*** The U.S. and other governments are playing the name and shame game, relying on this tactic to deter cybercriminals by attributing blame for attacks to specific nation states. Most recently, a U.S. government complaint alleges that a North Korean government-backed programmer executed the 2014 Sony hack and the "WannaCry" attacks.[1] In 2016, Special Counsel Robert Mueller unsealed an indictment that charged a dozen spies believed to have been backed by the Russian government for interfering with the 2016 elections.

   The UK is also pointing fingers, and recently blamed Russian military intelligence of several cyber attacks. The National Cyber Security Center takes the position that Russian's Main Intelligence Directorate was responsible for four attacks, including hacking the 2016 Democratic Committee, the World Anti-Doping Agency, and the BadRabbit ransomware, in addition to attacking a UK-based television station.[2]

   Regardless of the effectiveness of the name and shame approach, these types of actions, along with imposing sanctions and serving indictments, are a form of self-regulation that only governments can do, and they should keep doing it.

2. ***Third-Party Concerns Surround Latest Facebook Breach.*** Following Facebook's recent data breach, the company announced that it found no evidence that any of the 50 million user accounts impacted by the breach had been used to access apps using Facebook Login. Nonetheless, security experts caution that the breach could have

[1] https://www.law360.com/articles/1083212/north-korea-hits-back-at-sony-wannacry-hacking-charges
[2] https://www.zdnet.com/article/the-new-weapon-against-russian-cyber-attacks-naming-and-shaming/

permitted hackers to access third-party apps and websites by relying on the single Sign-On ("SSO") feature API.[3] This API lets users log in to websites using Facebook credentials and can be obtained using access tokens.

A professor commenting on Facebook's investigation noted that although the results are encouraging, i.e. that there is no indication that apps have been accessed, the report lacks important information such as how long Facebook's audit occurred and the implications for apps. There are continued risks for individuals that used Facebook SSO for other third-party apps.

Current SSO deployment practices are problematic for Facebook and other identity providers, exposing users to stealthy attacks. While SSO is appealing for developers focused on a seamless user experience, great risk comes with integrating applications with this API. The risks are especially high when integrating critical functions like authentication.

The Fast Identity Online ("FIDO") Alliance is one solution that has emerged to the authentication challenges highlighted by the Facebook breach. The FIDO specifications and certifications enable an interoperable ecosystem of hardware, mobile, and biometrics-based authenticators that allow enterprises and service providers to deploy strong authentication solutions that reduce reliance on passwords and protect against phishing, man-in-the-middle and replay attacks using stolen passwords.[4] Moving away from traditional password mechanisms can help limit large scale incidents whose impact is difficult to trace such as with the recent Facebook incident.

3. ***New Zealand Customs Officers Asking for What?*** A law recently took effect in New Zealand requiring travelers to unlock their phone or other digital devices if customs officials believe that there is "reasonable cause."[5] Specially, the law requires travelers to provide "access information", defined as "codes, passwords, and encryption keys, and any related information that enables access to an electronic device." The law is ambiguous as to what constitutes "reasonable cause," but is clear about the repercussions for travelers that fails to comply. Travelers who decline to unlock their devices may be fined up to $3,200.

   A spokeswoman for the New Zealand Customs Services asserts that the number of devices searched is very low, and that 99.98 percent of travelers do not have their device examined. She further explained that reasonable cause is a higher threshold

[3] https://threatpost.com/facebook-breach-sparks-concerns-around-third-party-app-website-security/137918/
[4] https://fidoalliance.org/about/what-is-fido/
[5] http://www.legislation.govt.nz/act/public/2018/0004/latest/whole.html#DLM7039503

than reasonable suspicion and means that in light of all the facts, and circumstances, the officer reasonably believes that the electronic device contains evidence.[6]

New Zealand's new law is unsettling but not unprecedented. Earlier this year, U.S. Customs and Border Patrol released a directive that permits advanced device searches where there is a "reasonable suspicion" of a national security concern.[7] This type of surveillance can be difficult to dispute as it is typically carried out under broad national security authority.

Congress –

Tuesday, October 9:
--No relevant hearings.

Wednesday, October 10:
--Hearing to examine consumer data privacy, focusing on lessons from the European Union's general data protection regulation and the California Consumer Privacy Act (Senate Committee on Commerce, Science, and Transportation).[8]

Thursday, October 11:
--Hearing to examine the cryptocurrency and blockchain ecosystem (Senate Committee on Banking, Housing, and Urban Affairs).[9]

International Hearings/Meetings –

EU –

Wednesday, October 10
--Meeting to discuss, "Enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society" (EU Parliament's Committee on the Environment, Public Health and Food Safety).[10]

Tuesday, November 13:
--Hearing entitled, "Assessing the impact of digital transformation of health services Related information" (EU Commission's Expert Panel on Health).[11]

---

[6] https://arstechnica.com/tech-policy/2018/10/new-zealand-customs-now-might-force-you-to-open-up-your-phone-or-pay-up/
[7] https://www.documentcloud.org/documents/4344208-CBP-directive-on-border-search-of-phones-laptops.html
[8] https://www.senate.gov/committees/hearings_meetings.htm
[9] https://www.senate.gov/committees/hearings_meetings.htm
[10] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bCOMPARL%2bENVI-OJ-20181010-1%2b01%2bDOC%2bXML%2bV0%2f%2fEN&language=EN
[11] https://ec.europa.eu/health/expert_panel/events_en

October 9, 2018

Conferences, Webinars, and Summits –

--HSCC Joint Cyber Working Group Meeting – Nashville, TN (10/9-11)
<https://nhisac.org/events/nhisac-events/hscc-joint-cyber-working-group-meeting/>
--Biotech/Pharma Security Workshop – Tokyo, Japan (10/17) <https://nhisac.org/events/nhisac-events/biotech-pharma-security-workshop-tokyo/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--CSS - "Table Stakes" in the Development and Deployment of Secure Medical Devices – Minneapolis, MN (10/22) <https://nhisac.org/events/nhisac-events/css-3/>
--Summit on Third-Party Risk – Leesburg, VA (10/24-26) <https://nhisac.org/events/nhisac-events/summit-on-third-party-risk/>
--2018 Heathcare CyberGard Conference – Charlotte, NC (10/25-26)
<https://nhisac.org/events/nhisac-events/2018-heathcare-cybergard-conference/>
--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/7-9)
<https://www.nist.gov/news-events/events/2018/11/nist-cybersecurity-risk-management-conference>
--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>
--NH-ISAC Blended Threats Exercise Series – So. CA (11/19) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29)
<https://www.destinationhotels.com/la-cantera-resort-and-spa>
--FIRST Symposium 2019 – London, UK (3/18/19)
<https://nhisac.org/events/nhisac-events/first-symposium-2019/>

Sundries –

--**Justice Department charges 7 Russian intelligence officers**
<https://www.cyberscoop.com/def-con-voting-village-report/>
--**Election security experts wonder what lies beyond 2018**
<https://www.cyberscoop.com/election-security-readiness-summit-eac-funding/>
--**DHS Warns of Cybersecurity Threats to Agriculture Industry**
<https://www.bleepingcomputer.com/news/security/cisco-releases-alerts-for-14-high-severity-bugs/>
-- **Apple, Amazon, among companies compromised in Chinese intelligence hack: report**
<https://thehill.com/policy/technology/409861-companies-including-apple-amazon-compromised-in-chinese-intelligence-hack>
--**Irish data watchdog opens investigation into Facebook breach**
<https://thehill.com/policy/technology/409848-irish-data-watchdog-opens-investigation-into-facebook-breach>

Contact us: follow @HealthISAC, and email at contact@h-isac.org

October 9, 2018