October 16, 2018

TLP White

We start with a breach impacting a Maryland library system. We also discuss a new law in California banning weak passwords. We conclude by shedding some light on global supply chain risks, including the ones that you did not see coming.

Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Virus Hits Maryland Library System.*** Awareness around vulnerabilities and proper cyber hygiene are important to organizations of all shapes and sizes, including your local library. Those operating the library system in Anne Arundel County, Maryland are working to get it back online after a self-propagating Emotet banking Trojan infected around 600 staff and public library computers.[1] Officials in Anne Arundel County have informed thousands of library customers who used the public computers that their data may have been compromised, and urged them to monitor their personal information for fraudulent activity. This is particularly important for those who used the library computers to access banking or social security information.

   The library discovered the malware following reports from library staff that they were receiving an abnormal volume of spam to library accounts. Other symptoms included spontaneous computer reboots which spread to public computers. Once it was determined that the unusual activity was caused by malware, the computers were pulled from service. In response to the events, the library has since updated its malware scanning capabilities and is providing staff with training so that they can better recognize the warning signs of a digital threat.

   The implications of an attack like this one on public computers quickly becomes personal. Individuals that used compromised devices must be cautious of potentially infecting their home networks and must monitor their credentials across a number of accounts. Library systems have to be particularly careful about monitoring systems,

[1] http://www.capitalgazette.com/news/government/ac-cn-library-virus-1007-story.html

employing appropriate access controls, and keeping employees appropriately trained in order to limit system disruptions.

2. ***California Bans Weak Passwords.*** From our "Hey, at least it's something" department, we report on California recently passing a law that bans weak passwords in connected devices. The law demonstrates an attempt to bolster the security of Internet of Things ("IoT") devices by strengthening authentication requirements.

   The law provides that if a connected device can be authenticated outside of a local area network, it will be deemed to have reasonable security features if either: (1) the preprogrammed device password is unique to each device manufactured; or (2) if the device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.[2]

   When it comes to improving security outcomes, it is unclear whether using legislation to impose specific security requirements leads to more secure networks, or whether it is better to provide organizations with incentives in the way of tax breaks or other advantages to lure people into compliance.

   Either way, weak authentication continues to be a major vulnerability, and by extension, stronger authentication mechanisms will continue to be an important component of improving the security of connected devices. Other states may also jump on the strong password bandwagon as the proliferation of IoT devices continues to grow.

3. ***Tiny Spy Chip (maybe?). Big Supply Chain Problem (yes).*** This week it may have been difficult to miss headlines about the grain-of-rice-sized, data-stealing hardware believed to have been installed into Supermicro motherboards before the servers employing them were shipped off to several major US companies, including Apple, Amazon, and a telecommunications provider.[3] The elaborate attack was reported to have been the result of individuals gaining access to multiple factories in China and manipulating factory employees to permit the installation of malicious hardware that gave attackers undetectable access to computer network data.

   Bloomberg published a few articles breaking the story, explaining the compromise in greater detail.[4] However, Apple, Amazon and others have all flatly denied that any of this actually happened and it doesn't appear any physical evidence has actually been produced so far. Some may remember a few years ago when it was reported the National Security Agency was planting

[2] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

[3] https://arstechnica.com/information-technology/2018/10/supermicro-boards-were-so-bug-ridden-why-would-hackers-ever-need-implants/

[4] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies; https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom/.

spy tools on Cisco routers[5]. Even more recently, the US Government has been warning its own agencies and private sector companies about compromised software and hardware from China, Russia and elsewhere. So whether or not the Bloomberg story about Supermicro proves to be true or not, there is little question that the global technology supply-chain is rife with risks.

Congress –

Tuesday, October 16:
--No relevant hearings.

Wednesday, October 17:
--No relevant hearings.

Thursday, October 18:
--No relevant hearings.

International Hearings/Meetings –

EU –

Tuesday, November 13:
--Hearing entitled, "Assessing the impact of digital transformation of health services Related information" (EU Commission's Expert Panel on Health).[6]

Conferences, Webinars, and Summits –

--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>

[5] https://www.infoworld.com/article/2608141/internet-privacy/snowden--the-nsa-planted-backdoors-in-cisco-products.html
[6] https://ec.europa.eu/health/expert_panel/events_en

--H-ISAC Blended Threats Exercise Series – So. CA (11/19) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--2018 H-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 –

--**Magecart group compromises customer ratings tool, affecting 'hundreds' of online stores**
<https://www.cyberscoop.com/magecart-shopper-approved-skimmer-riskiq/>
--**Symantec reveals state-sponsored group that doesn't care for malware**
<https://www.cyberscoop.com/malware-less-cyber-espionage-hacking-group-symantec-research/>
--**Facial Recognition Tech: EFF Engaged in Battle Against "Expanding Proliferation of Surveillance"**
<https://www.bleepingcomputer.com/news/security/facial-recognition-tech-eff-engaged-in-battle-against-expanding-proliferation-of-surveillance/>
-- **New Android Trojan Gplayed Adapts to Attacker's Needs**
<https://www.bleepingcomputer.com/news/security/new-android-trojan-gplayed-adapts-to-attackers-needs/>
--**Hackers loot digital wallets using stolen Apple IDs**
<https://thehill.com/policy/technology/410984-hackers-steal-from-digital-wallets-in-china-with-stolen-apple-ids>

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