June 12, 2018

TLP White

We have another big week for you, folks. We start with a big decision coming out of the Eleventh Circuit which raises some doubt about the FTC's data security authority and then discuss some highlights from Apple's WWDC. We also address a recently announced multi-stakeholder effort on software transparency and then shed some light on VPNFilter. We conclude with addressing some drama on Capitol Hill regarding the Healthcare Cybersecurity and Communications Integration Center. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***A Jab to The FTC's Authority.*** The Eleventh Circuit vacated a Federal Trade Commission ("FTC" or "Commission") order that required LabMD, a medical testing company, to improve its data security practices. The court reasoned that the FTC's order "does not enjoin a specific act or practice…[but instead] mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished."[1]

   The FTC has broad authority under Section 5 of the FTC Act to bring actions against companies that participate in "unfair…acts or practices" – i.e., a practice that is "likely to cause [consumers] substantial injury…"[2] In 2013, under this authority, the Commission asserted that LabMD's security practices in 2008 were inadequate and exposed sensitive personal and health information of about 9,300 consumers onto LimeWire, a peer-to-peer network.[3]

   According to the FTC, the exposure – which included names, dates of birth, social security numbers, lab test codes, and health insurance information – caused consumers substantial injury. LabMD challenged the FTC's authority, however, claiming that the order was "unenforceable because it does not direct LabMD to cease committing an

[1] https://www.reuters.com/article/us-ftc-datasecurity-labmd/u-s-agency-loses-appeal-over-alleged-labmd-data-security-lapses-idUSKCN1J22XD
[2] https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority
[3] https://www.reuters.com/article/us-ftc-datasecurity-labmd/u-s-agency-loses-appeal-over-alleged-labmd-data-security-lapses-idUSKCN1J22XD

unfair act or practice…"[4] The Eleventh Circuit agreed. A spokeswoman from the FTC, responding to the ruling, said that "[a]lthough we are disappointed by the appeals court's ruling, we will continue to do everything we can to protect consumer privacy… [and] are evaluating our next steps in response to this decision."

2. ***Apple's WWDC.*** Apple recently held the Worldwide Developers Conference ("WWDC"),[5] where it announced fitness updates to the Apple Watch, and privacy updates to its web browser, Safari, and mobile operating system, iOS.[6] WWDC provides technology enthusiasts and industry leaders an opportunity to connect and learn about Apple's developments.

   The multinational technology company announced upgrades to its popular smartwatch, Apple Watch, which can be used for fitness and health tracking.[7] The device offers new health and fitness features including, (1) allowing users to challenge one another to exercise competitions and communicate with one another over Walkie Talkie; (2) offering new workouts like yoga and hiking; (3) improving heart rate tracking and Siri's monitoring capabilities; and (4) recording users' rolling-mile pace – i.e., the user's last mile ran.

   Fitness trackers like Apple Watch promote health and fitness and with features like these, they only become more attractive. However, more features means more data. Therefore, organizations who offer fitness and health tracking should remain cognizant of the appropriate data laws and remind their customers of important data security practices – e.g., keeping devices up-to-date – to ensure their customers' health and fitness data remains secure.

   Apple's web browser, Safari, and mobile operating system, iOS, will be getting a privacy upgrade. Most notably, the updated web browser will (1) block tracking associated with comment fields as well as "like" or "share" buttons; (2) alert users when a website wants to access cookies or data and permit users to prohibit access; (3) reduce "fingerprinting" – i.e., when marketers assign an individual, trackable ID to a device based on publicly accessible device information – by exposing only generic information; and (4) monitor password usage to deter users from assigning the same password to multiple accounts.[8] Apple also announced that iOS apps will need explicit permission from users before accessing the device's camera, microphone, location, mail, and messages. Indeed, Apple has always prided itself on its attitude towards privacy and according to Craig Federighi, Apple's senior VP of software engineering, "One of the reasons that people choose Apple products is because of our commitment to privacy."

---

[4] https://www.bna.com/bellwether-data-security-n73014476288/
[5] https://developer.apple.com/wwdc/
[6] https://www.wired.com/gallery/everything-apple-announced-wwdc-2018/
[7] https://arstechnica.com/gadgets/2018/06/watch-os-5-announced-for-the-apple-watch/
[8] https://www.wired.com/story/apple-safari-privacy-wwdc

It is an exciting time for technology and if Apple's WWDC indicates anything, it's that the company has a new approach to health, fitness, and privacy. Let's see if other organizations follow suit.

3. ***Multi-Stakeholder Effort on Software Transparency.*** The U.S. Department of Commerce's National Telecommunications and Information Administration ("NTIA"), the agency tasked with counseling the president on telecommunication and information policy issues,[9] recently launched a multi-stakeholder initiative to improve software component transparency.[10]

   According to the NTIA, a complete account of software components is not always accessible, which can make it difficult for entities to protect against security risks – especially given "the growth in Internet of Things ["IoT"] devices, as companies add 'smart' features or connectivity without clear visibility into a product's underlying software components."

   The initiative builds on existing IoT cybersecurity best practices and its goal, through a transparent and multi-stakeholder approach, is to (1) identify how to share component data, (2) determine what voluntary practices stakeholders should adopt, and (3) decide which market challenges the broader community should address. Ultimately, NTIA states that the "process aims to create a market offering greater transparency to organizations for risk management."

   The initiative is also the NTIA's first move towards implementing the joint US Departments of Homeland Security and Commerce *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*,[11] which we covered in last week's edition of *Hacking Healthcare.*

4. ***VPNFilter: Worse Than We Thought.*** For at least two weeks, researchers from Cisco's Talos security team have been tracking VPNFilter, a malware which has allowed hackers working for the Russian government to infect more than 500,000 consumer-grade routers in 54 countries.[12] This week the Talos team revealed that the threat presented by VPNFilter is worse than we thought, targeting a broader base of devices than was originally reported two weeks ago.

   According to the Talos Team's analysis, VPNFilter performs a man-in-the-middle attack on a router's incoming web traffic, allowing attackers to use the "ssler" module to inject

[9] https://www.ntia.doc.gov/about
[10] https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency
[11] https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets
[12] https://arstechnica.com/information-technology/2018/06/vpnfilter-malware-infecting-50000-devices-is-worse-than-we-thought/

malicious payloads into traffic as it passes through an infected router. The ssler module is designed to steal sensitive data passed between connected end-points and the outside Internet, actively inspecting URLs for indications that they are transmitting passwords or other sensitive data. This information is then copied and transmitted to servers that are under the control of the attackers. The ssler module is capable of bypassing TLS encryption, downgrading HTTPS connections to plaintext traffic.

Originally, Cisco took the position that the goal of the VPNFilter was to use home and small-office routers, switches, and network-attached storage devices as a platform for launching attacks on primary targets. The Talos Team's discovery of the ssler module indicates that router owners themselves are the key target for the malware. As described by Craig Williams, a senior technology leader and global outreach manager at Talos, the attackers can manipulate everything that passes through a compromised device. "They can modify your bank account balance so that it looks normal while at the time they're siphoning off money and potentially PGP keys and things like that. They can manipulate everything going in and out of the device."[13]

The multi-layered nature of the malware makes disinfecting devices rather challenging, and the steps for fully disinfecting devices varies from model to model. For some models, pressing a button to reset the device to factory settings will eliminate at least part of the malware. For other models, device owners must reboot the device and then immediately install the latest available firmware from the manufacturer.

5. ***HHS: Healthcare in the Hot Seat.*** This week leadership from two congressional committees sent a letter to Health and Human Services ("HHS") asking for a status update on some of HHS's to-do items provided in the Cybersecurity Information Sharing Act ("CISA").[14] Lawmakers explained that industry is confused by the lack of direction for the Healthcare Cybersecurity and Communications Integration Center ("HCCIC"), lack of clarity about HHS's plans, and asked for a status update on HHS's report on cybersecurity best practices – pursuant to CISA's requirements.[15]

   In addition to the letter, HCCIC was also in the spotlight during this week's House Energy and Commerce health subcommittee hearing on the reauthorization of the Pandemic and All-Hazards Act (S.2852). The reauthorization bill includes a provision designating HCCIC as the lead entity in HHS for cybersecurity incidents. The bill restructures HCCIC, placing it in the Office of the Assistant Secretary for Preparedness and Response ("ASPR") instead of in HHS's Office of the Chief Information Officer. Historically, ASPR has primarily focused on public health emergencies, raising concerns that ASPR may lack the technical expertise necessary to manage a cybersecurity initiative.

---

[13] https://arstechnica.com/information-technology/2018/06/vpnfilter-malware-infecting-50000-devices-is-worse-than-we-thought/

[14] https://energycommerce.house.gov/wp-content/uploads/2018/06/20180605HHS.pdf

[15] https://www.politico.com/newsletters/morning-ehealth/2018/06/06/cyber-drama-on-hill-today-243470 headline

The highly anticipated HHS report is incomplete, but scheduled for released at the end of 2018. We will keep you posted as this saga continues.

Congress –

Tuesday, June 12:
--No relevant hearings

Wednesday, June 13:
--Hearing to examine the National Telecommunications and Information Administration (Senate Committee on Commerce, Science, and Transportation)[16]

Thursday, June 14:
--No relevant hearings

Friday, June 15:
--Hearing titled, "The State of U.S. Public Health Biopreparedness: Responding to Biological Attacks, Pandemics, and Emerging Infectious Disease Outbreaks" (House Subcommittee on Oversight and Investigations)[17]

Conferences and Webinars –

--Health IT Summit – Minneapolis, MN (6/13) <https://vendome.swoogo.com/2018-Minneapolis-Health-IT-Summit>
--Biotech / Pharmaceutical Security Workshop - Dublin, Ireland (6/21) <https://nhisac.org/events/nhisac-events/medical-device-and-pharmaceutical-security-workshop-dublin/>
--Health IT Summit – Nashville, TN (6/28) <https://vendome.swoogo.com/2018-Nasvhille-HITSummit>
--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>
--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--Biotech/Pharma Security Workshop at Gilead Sciences, Foster City, CA (8/29) <https://nhisac.org/events/nhisac-events/biopharma-workshop-at-gilead-sciences-foster-city-ca/>

[16] https://www.senate.gov/committees/committee_hearings.htm
[17] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108422

--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/4-6)
<https://www.nist.gov/cyberframework>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29)
<https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

-- **The Fifth Anniversary of the Snowden Disclosures**
<https://www.lawfareblog.com/fifth-anniversary-snowden-disclosures>
-- **Feds Ramp Up Investigations Into Online Harassment, Cyberstalking & Threats**
<https://www.bleepingcomputer.com/news/government/feds-ramp-up-investigations-into-online-harassment-cyberstalking-and-threats/>
-- **Windows 10 April 2018 Update Already Installed on 50% of Windows 10 PCs**
<https://www.bleepingcomputer.com/news/microsoft/windows-10-april-2018-update-already-installed-on-50-percent-of-windows-10-pcs/>
-- **GitLab Sees Huge Traffic Spike After News of Microsoft Buying GitHub**
<https://www.bleepingcomputer.com/news/technology/gitlab-sees-huge-traffic-spike-after-news-of-microsoft-buying-github/>
-- **Fortinet Completes Bradford Networks Purchase**
<https://www.darkreading.com/operations/identity-and-access-management/fortinet-completes-bradford-networks-purchase/d/d-id/1331955>
-- **Q&A with FBI cyber chief**
<https://www.politico.com/newsletters/morning-cybersecurity/2018/06/04/q-a-with-fbi-cyber-chief-240483>
-- **An Encryption Upgrade Could Upend Online Payments**
<https://www.wired.com/story/tls-encryption-upgrade-credit-card-online-payments>
-- **Windows 10 Insider Build 17686 Released. Here's Whats New!**
<https://www.bleepingcomputer.com/news/microsoft/windows-10-insider-build-17686-released-heres-whats-new/>
-- **Chinese, Russian hacking groups spy on South Korea amid U.S.-North Korea peace talks**
<https://www.cyberscoop.com/chinese-russian-hacking-groups-spy-south-korea-amid-u-s-north-korea-peace-talks/>
-- **Phishing Scams Target FIFA World Cup Attendees: Kaspersky Lab**
<https://www.darkreading.com/threat-intelligence/phishing-scams-target-fifa-world-cup-attendees-kaspersky-lab/d/d-id/1331959>