October 15th, 2019

Hacking Healthcare

TLP White

In this edition of Hacking Healthcare, we begin by exploring major proposed changes to the Domain Name System—an Internet mainstay that maps IP addresses to website names. Next, we explore the possibility of the Department of Homeland Security gaining new subpoena powers. Finally, we wrap up with a quick briefing of the U.S. Food and Drug Administration's Cybersecurity Bill of Materials and its potential shortcomings. Welcome back to *Hacking Healthcare*.

Changes to Domain Name System Prompt Push Back. The Domain Name System (DNS), which acts as the address system for the Internet, has managed to remain relatively intact since its inception decades ago. However, a new push by several major companies, including Google and Mozilla, to encrypt DNS lookups would significantly alter the aging protocol. Not everyone is convinced the move is for the better.

Proponents for the change generally cite security and privacy concerns as the catalyst for altering the protocol. The current lack of encryption on DNS requests means that Internet service providers (ISPs), governments, and malicious actors can monitor your Internet activity or possibly even manipulate it through DNS hijack attacks. By implementing an encryption method, such as DNS over HTTPS (DoH) or DNS over TLS (DoT), unwanted surveillance and hijacking attacks become significantly more difficult to achieve. The requirement for using one of these encryption methods is that you need a DNS resolver that can see the unencrypted DNS requests before being processed.

So, what are the issues? First, there are relatively few such resolvers in the market today.[1] This lack of diversity inherently centralizes DNS requests to only a few companies, which would give those companies unique access to the type of information that ISPs currently also receive. Second, unlike end-to-end encryption, which is intended to keep information private between the sender and receiver, DNS encryption with either DoT or DoH doesn't so much keep information private as it changes who can see what sites you are visiting. In essence, these encryption protocols partially cut out ISPs and governments in favor of these resolvers, which to tend be large tech companies.[2]

The U.S. Department of Homeland Security Asks for Subpoena Powers. As all cybersecurity leaders know, time is the most valuable resource when attempting to find and patch vulnerabilities or when responding to incidents. In recognition of this fact, an effort is underway to streamline and quicken the process by which the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) can contact vulnerable critical infrastructure operators. DHS is asking Congress to grant it "administrative" subpoena authorities so it can compel an Internet service provider (ISP) to give it contact information for equipment owners who are deemed to be at risk.[3]

Why does DHS need this power? Currently, DHS has the ability to scour the Internet to find the IP addresses of vulnerable systems, most notably Industrial Control Systems (ICS), but it often does not have contact information for those addresses.[4] ISPs generally know which IP addresses belong to which organizations, as well as their contact information, but current laws prohibit the ISPs from sharing that information with DHS.[5] These laws have forced DHS to ask ISPs to make notifications to the vulnerable operators on their behalf. Currently, ISPs are not obligated to follow through, nor are they always staffed or trained to respond, and this workaround approach adds an additional communication layer that takes time to process.[6]

As things stand, members of the U.S. Senate Homeland Security and Governmental Affairs Committee have been briefed by members of the Trump Administration on DHS's need for capabilities to tackle this issue and have reviewed DHS's legislative proposal.[7] While Congress appears receptive to hearing DHS out on the matter, there are those who are staunchly opposed to it. Speaking to TechCrunch, Jake Williams, founder of Rendition Infosec and a former U.S. National Security Agency (NSA) hacker, exclaimed that this was a power grab and that "[he could not] fathom that this will not be used in a way that lawmakers who are drafting the legislation will not have intended."[8]

Without the ability to access the text of the proposed legislation, it is hard to judge the scope of the subpoena powers DHS is requesting and how justified opponents are in their concern for potential misuse. And it seems that we may be waiting a while before any such legislation has a chance to be considered. With Congress embroiled in several partisan battles leading into an election year, it may be difficult for such legislation to gain traction in the near term.

Shortcomings in the U.S. FDA's Bill of Materials. The U.S. Food and Drug Administration's (FDA) current draft of a proposed cybersecurity bill of materials (CBOM) will have far reaching impacts for the healthcare industry once implemented. However, at least a few cybersecurity professionals are warning that not all the proposed requirements may be as beneficial or easily implemented as hoped.

The CBOM, as currently outlined in the FDA's *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* from October 2018, requires medical device manufacturers to "include a list of software and hardware components which have vulnerabilities or are susceptible to vulnerabilities."[9] The intent is to help healthcare organizations better understand the devices they use and better assess the risk involved in using those devices. While the response to the CBOM has generally been positive, there are several concerns.

First, medical device manufactures are quick to point out just how complex these devices can be. Listing all hardware components and sub-components is not just resource intensive but may not actually be feasible in all circumstances. This has led some to push for a revision of the CBOM to only include software.[10] Second, there is some worry among device manufactures that having to disclose software partners prior to device approval may inadvertently out those partners to competitors.[11] Once known, competitors may attempt to use the same vendor or may even try and acquire that vendor. Lastly, not everyone is happy with the two-tiered approach the FDA has drafted for classifying medical devices for cyber risk. Responses have requested everything from dropping the tiered lists, adding a third tier, or completely revising the tier definitions to be broader.[12]

October 15th, 2019

Congress –

Tuesday, October 15th:
-No relevant hearings

Wednesday, October 16th:
Public-Private Initiatives to Secure the Supply Chain (House – Committee on Homeland Security)

Thursday, October 17th:
-No relevant hearings

International Hearings/Meetings –

EU –

Thursday, October 17th:
European Commission - EU Health Policy Platform annual meeting

Conferences, Webinars, and Summits –

--2019 H-ISAC European Summit – Zurich, Switzerland (10/16/2019-10/17/2019)
https://h-isac.org/summits/european_summit/
--Health IT Summit (Midwest) – Minneapolis, MN (10/17/2019-10/18/2019)
https://endeavor.swoogo.com/2019-Minneapolis-Health-IT-Summit
--Healthcare Cybersecurity Forum (Midwest) – Minneapolis, MN (10/18/2019)
https://endeavor.swoogo.com/2019_Midwest_Cybersecurity_Forum
--H-ISAC / MITSF Healthcare Cybersecurity Workshop – Tokyo, Japan (10/24/2019)
http://www.cvent.com/events/h-isac-mitsf-healthcare-cybersecurity-workshop/event-summary-21a9794745bf41c4bb55ba9dd29dc256.aspx
--Key Steps to Building a Threat Intelligence Strategy – Webinar (10/24/2019)
https://h-isac.org/hisacevents/trustar-webinar/
H-ISAC Security Workshop – Titusville, FL (11/4/2019)
https://h-isac.org/hisacevents/h-isac-security-workshop/
--CHIME Healthcare CIO Boot Camp – Phoenix, AZ (11/6/2019-11/9/2019)
https://h-isac.org/hisacevents/chime-healthcare-cio-boot-camp/
--Health IT Summit (Southwest) – Houston, TX (11/14/2019-11/15/2019)
https://endeavor.swoogo.com/2019-Dallas-Health-IT-Summit
--Southwest Healthcare Cybersecurity Forum – Dallas, TX(11/15/2019)
https://endeavor.swoogo.com/2019_Southwest_Cybersecurity_Forum
--Health IT Summit (Northwest) – Seattle, WA (11/19/2019-11/20/2019)
https://endeavor.swoogo.com/2019-PacificNorthwest-HITSummit
--Pacific Northwest Healthcare Cybersecurity Forum – Seattle, WA (11/20/2019)
https://endeavor.swoogo.com/2019_Pacific_Northwest_Cybersecurity_Forum
--2019 H-ISAC Fall Summit – San Diego, CA (12/2/19-12/6/2019)
https://h-isac.org/summits/fall-summit-2019/
--H-ISAC Security Workshop – London, UK (2/5/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-2/

Sundries –

--Phishing Incident Exposes Medical, Personal Info of 60K Patients
https://www.bleepingcomputer.com/news/security/phishing-incident-exposes-medical-personal-info-of-60k-patients/
--No-deal Brexit data - should firms worry?
https://www.bbc.com/news/technology-49980327?intlink_from_url=https://www.bbc.com/news/technology&link_location=live-reporting-story
--Bug Bounty: Who Wants to Hack the Army Again?
https://www.nextgov.com/cybersecurity/2019/10/who-wants-hack-army-again/160518/
--Planting Tiny Spy Chips in Hardware Can Cost as Little as $200
https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/
--AIG says its cyber insurance plans don't cover criminal acts; wants lawsuit tossed
https://www.cyberscoop.com/aig-cyber-insurance-lawsuit-bec/

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

[1] https://www.wired.com/story/dns-over-https-encrypted-web/
[2] https://www.wired.com/story/dns-over-https-encrypted-web/
[3] https://techcrunch.com/2019/10/09/cisa-subpoena-powers-isp-vulnerable-systems/
[4] https://www.cyberscoop.com/dhs-cisa-subpoena-authority-vulnerable-asset-owners/
[5] https://www.cyberscoop.com/dhs-cisa-subpoena-authority-vulnerable-asset-owners/
[6] https://www.cyberscoop.com/dhs-cisa-subpoena-authority-vulnerable-asset-owners/
[7] https://www.cyberscoop.com/dhs-cisa-subpoena-authority-vulnerable-asset-owners/
[8] https://techcrunch.com/2019/10/09/cisa-subpoena-powers-isp-vulnerable-systems/
[9] https://www.hipaajournal.com/concerns-raised-with-fda-over-medical-device-security-guidance/
[10] https://www.hipaajournal.com/concerns-raised-with-fda-over-medical-device-security-guidance/
[11] https://www.healthcareitnews.com/news/fda-s-bill-materials-crates-cybersecurity-blind-spot-medical-devices
[12] https://www.hipaajournal.com/concerns-raised-with-fda-over-medical-device-security-guidance/