August 11th, 2020

TLP White

This week, Hacking Healthcare begins by exploring just how significant the Trump Administration's recent Executive Order targeting WeChat may be for those in the healthcare sector. We then conclude this issue by breaking down the recent news that China has started to block HTTPS traffic that used TLS 1.3 and ESNI, including why, how, and what it means for healthcare organizations.

***Note**: On the subject of TLS 1.3, we point you to a NIST workshop taking place this Thursday (August 13th) where you can learn more.*

https://www.nccoe.nist.gov/events/virtual-workshop-challenges-compliance-operations-and-security-encrypted-protocols-particular

Welcome back to *Hacking Healthcare*.

Presidential Executive Order Targets WeChat. On August 6th, 2020, President Trump signed an Executive Order "Addressing the Threat Posed by WeChat."[1] Citing authority granted by the International Emergency Economic Powers Act, the National Emergencies Act, and Section 301 of Title 3 to the United States Code, President Trump expanded upon his earlier Executive Orders that looked to curb the influence of Chinese technology products and services within the United States.

The President expressed the threat posed by mobile applications such as TikTok and WeChat in stark terms, claiming they threaten US national security, foreign policy interests, and the economy. In describing WeChat, the Executive Order condemns the application of "automatically [capturing] vast swaths of information from… users," in ways that "allow the Chinese Communist Party access to Americans' personal and proprietary information."[2] Additionally, the Executive Order posits that WeChat "censors content that the Chinese Communist Party deems politically sensitive and may also be used for disinformation campaigns" to benefit the Chinese government.[3]

The Executive Order goes on to detail the scope and content of the prohibited actions, which include "[a]ny transaction that is related to WeChat by any person, or with respect to any property, subject to the jurisdiction of the United States, with Tencent Holdings Ltd. Shenzhen, China, or any subsidiary of that entity, as identified by the Secretary of Commerce."[4] The

broadly worded Executive Order leaves a good deal of uncertainty as to exactly how it will be enforced if it is deemed to be legal.

Chinese tech companies are aware of the hostility and suspicion centered on them in foreign markets, and the US will not be the last country to raise potential security and privacy concerns surrounding their offerings. Tencent, WeChat's parent company, is said to be "reviewing the executive order to get a full understanding."[5]

Action & Analysis
H-ISAC Membership Required

China Updates Great FireWall to Block TLS 1.3 and ESNI. Since sometime around the end of July, the Great Firewall ("GFW"), the Chinese state's national Internet censorship apparatus, has been updated to block encrypted HTTPS traffic making use of TLS 1.3 and Encrypted Server Name Indication ("ESNI"). HTTPS traffic making use of older protocols has been unaffected, and it is speculated that the change has everything to do with how TLS 1.3 and ESNI conflict with the Chinese government's insistence on strict control over the data coming into China and what information Chinese citizens can access.

Recent reports state that "the Chinese government is currently dropping all HTTPS traffic where TLS 1.3 and ESNI are used, and temporarily banning the IP addresses involved in the connection."[6] As of last week, a number of workarounds had been reported on both the client side and server side, however, how long these will remain viable is anyone's guess.[7]

A team from the University of Maryland submitted a blog post last week that detailed their primary findings related to the GFW update. These findings include:[8]

- The GFW blocks ESNI connections by dropping packets from client to server.
- The blocking can be triggered bidirectionally.
- The 0xffce extension is necessary to trigger the blocking.
- The blocking can happen on all ports from 1 to 65535.
- Once the GFW blocks a connection, it will continue blocking all traffic associated with the 3-tuples of (srcIP, dstIP, dstPort) for 120 or 180 seconds.

Action & Analysis
H-ISAC Membership Required

August 11th, 2020

Congress –

Tuesday, August 11th:
- No relevant hearings

Wednesday, August 12th:
- No relevant hearings

Thursday, August 13th:
- No relevant hearings

International Hearings/Meetings –

EU – No relevant hearings

Conferences, Webinars, and Summits –

-- H-ISAC European Council Webinar Series – Webinar (8/14/2020)
https://h-isac.org/hisacevents/h-isac-european-council-webinar-series/
-- Securing Hospitals – How Compliance and Cybersecurity Align by IntSights – Webinar (8/19/2020)
https://h-isac.org/hisacevents/securing-hospitals-how-compliance-and-cybersecurity-align-by-intsights/
-- H-ISAC Monthly Member Threat Briefing – Webinar (8/25/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-11/
-- STOP HEMORRHAGING DATA: MINIMIZE THIRD-PARTY RISK IN HEALTHCARE BY RISKRECON – Webinar (9/1/2020)
https://h-isac.org/hisacevents/stop-hemorrhaging-data-minimize-third-party-risk-in-healthcare-by-riskrecon/
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
-- ENISA Trust Services Forum - CA Day 2020 - Schloßplatz Berlin, Germany (9/22/2020)
https://h-isac.org/hisacevents/enisa-trust-services-forum-ca-day-2020/
--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126
--H-ISAC Cyber Threat Intel Training - Titusville, FL (9/22/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-titusville-fl/
--H-ISAC Security Workshop – Forcheim, Germany - Virtual (9/23/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/
--H-ISAC Monthly Member Threat Briefing – Webinar (9/29/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-12/
-- The MedTech Conference – Virtual (10/5/2020)
https://h-isac.org/hisacevents/the-medtech-conference-toronto/
-- Healthcare Cybersecurity Forum – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
-- NCHICA AMC Security & Privacy Conference - Durham, North Carolina (10/21/2020-10/22/2020)
https://h-isac.org/hisacevents/nchica-amc-security-privacy-conference/
-- 2020 H-ISAC European Summit - Santpoort-Noord, Netherlands (10/20/2020-10/22/2020)

https://h-isac.org/summits/european-2020-summit/
--CYSEC 2020 – Dubrovnik, Croatia (10/27/2020 – 10/28/2020)
https://h-isac.org/hisacevents/cysec-2020-croatia/
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/
--H-ISAC Security Workshop - Paris, France (11/18/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-paris-france/
--H-ISAC Fall Summit - Phoenix, AZ (11/30/2020-12/4/2020)
https://h-isac.org/summits/fall-summit-2020/
-- H-ISAC Security Workshop - Prague, Czech Republic (12/8/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-prague/
-- 2021 APAC Summit – Singapore (3/23/2021-3/25/2021)

Sundries –

Flaws in Qualcomm chips could allow snooping, Check Point finds

> https://www.cyberscoop.com/400-vulnerabilities-qualcomm-snapdragon-chips-check-point-def-con-2020

Interpol Report: COVID-19 Impact on Ransomware, Threats, Healthcare Cybersecurity

> https://healthitsecurity.com/news/covid-19-impact-on-ransomware-threats-healthcare-cybersecurity

Researchers Create New Framework to Evaluate User Security Awareness

> https://www.darkreading.com/endpoint/researchers-create-new-framework-to-evaluate-user-security-awareness/d/d-id/1338603

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

---

[1] https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/
[2] https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/
[3] https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/

[4] https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/
[5] https://www.nytimes.com/2020/08/07/business/economy/trump-executive-order-tiktok-wechat.html
[6] https://www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/
[7] https://www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/
[8] https://geneva.cs.umd.edu/posts/china-censors-esni/esni/