Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ TLP:WHITE Alert ID : dabc58a3 Feb 10, 2024, 07:59 AM

This week, *Hacking Healthcare*™ examines the recent news of a widespread state-sponsored cyber campaign targeting American critical infrastructure. We dig into what happened, how the U.S. and its allies have responded, and what Health-ISAC members can learn from it.

Welcome back to *Hacking Healthcare*™.

U.S. Government Agencies Highlight State Actor Threat to Critical Infrastructure

Last week, it came to light that the U.S. government had taken action to combat an apparently widespread Chinese cyber operation carried out by the Volt Typhoon group that had compromised "thousands of internet-connected devices," and had thoroughly targeted multiple critical infrastructure sectors.[i] [ii]The seriousness of the effort was increasingly made clear through congressional testimony, warnings from the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), and even a joint cybersecurity advisory from the Five Eyes intelligence alliance, which includes the U.S., U.K., Australia, New Zealand, and Canada. With the picture made a bit clearer after a week of follow-up reporting and explanation from government sources, let's examine what happened and how it impacts the healthcare and public health (HPH) sector.

What Happened?

At the end of January, it was reported that the U.S. government "in recent months launched an operation to fight a pervasive Chinese hacking operation."[iii] The report stated that the U.S. Department of Justice (DOJ) and the FBI had even "received legal authorization to remotely disable aspects of the Chinese hacking campaign." While this kind of action has precedent, the seriousness of the operation became clear in the following days.

A congressional hearing in the House of Representatives included CISA Director Jen Easterly, FBI Director Christopher Wray, and General Paul Nakasone, wearing two hats as both the head of U.S. Cyber Command and Director of the National Security Agency (NSA). They provided some sobering details about the Chinese state-sponsored operation.

In testimony to Congress, Director Easterly noted that CISA has "observed a deeply concerning evolution in Chinese targeting of US infrastructure," and that the Chinese are "burrowing deep into our critical infrastructure to be ready to launch destructive cyber-attacks in the event of a major crisis or conflict with the United States."[iv] Her testimony continued by outlining that CISA had been busy finding and removing Chinese-linked "intrusions" across multiple critical infrastructure sectors, "including aviation, energy, water, and telecommunications."[v]

Director Wray's testimony elaborated, stating that the U.S. Intelligence Community (USIC) had "assessed that China is attempting to pre-position on U.S. critical infrastructure—setting up back doors to cripple vital assets and systems in the event China invades Taiwan and, therefore, limiting our ability to assist Taiwan." He continued by saying that "we have observed the [Chinese Communist Party] target multiple critical infrastructure entities, attacks which could potentially jeopardize the physical safety of Americans."[vi]

General Nakasone added to these remarks with the concerning testimony that the decision to target these kinds of critical infrastructure entities represented "a decision by an actor to actually focus on civilian targets."[vii]

Response: New Joint Cybersecurity Advisory

Roughly a week after the concerning testimony and reports of U.S. government action to dismantle the Chinese cyber operation, a joint cybersecurity advisory was posted urging critical infrastructure entities to take action in regard to the Chinese threat actor Volt Typhoon.[viii]

The joint cybersecurity advisory was signed off on by a multitude of government agencies from the U.S. and its allies in the Five Eyes intelligence alliance, including CISA, NSA, FBI, the Department of Energy (DOE), the Environmental Protection Agency (EPA), the Transportation Security Administration (TSA), the Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Canada's Centre for Cyber Security (CCCS), a part of the Communications Security Establishment (CSE), the United Kingdom National Cyber Security Centre (NCSC-UK), and New Zealand's National Cyber Security Centre (NCSC-NZ).

Reiterating the testimony of Directors Easterly and Wray and General Nakasone, the advisory warns that the threat actors' "choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable the disruption of OT functions across multiple critical infrastructure sectors."[ix]

The 37-page advisory goes on to outline technical details, detection recommendations, and mitigations, including a plea for potential targets to apply patches to internet-facing systems, implement phishing-resistant multi-factor authentication (MFA), and "ensure logging is turned on for application, access, and security logs."[x]

Action & Analysis
****Available with Health-ISAC Membership****

Congress

Tuesday, February 6

No relevant hearings

Wednesday, February 7

No relevant meetings

Thursday, February 8

No relevant meetings

International Hearings/Meetings

No relevant meetings

EU

[i] https://www.reuters.com/world/us/us-disabled-chinese-hacking-network-targeting-critical-infrastructure-sources-2024-01-29/

[ii] https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly

[iii] https://www.reuters.com/world/us/us-disabled-chinese-hacking-network-targeting-critical-infrastructure-sources-2024-01-29/

[iv] https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly

[v] https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly

[vi] https://www.fbi.gov/news/testimony/the-ccp-cyber-threats-to-the-american-homeland-and-national-security

[vii] https://cyberscoop.com/chinese-cyber-threats-fbi-operation-botnet/

[viii] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[ix] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[x] https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf

[xi] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[xii] https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly

[xiii] https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly

[xiv] https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly

[xv] https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/ncd-coker-written-testimony.pdf

[xvi] https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/ncd-coker-written-testimony.pdf

Report Source(s)

Health-ISAC

Reference | References

house
FBI
CISA
CISA
Cyberscoop
Reuters
CISA

Tags

Cybersecurity Advisory, Volt Typhoon, secure-by-design, Hacking Healthcare, Geopolitics, International Collaboration, China

---

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC's annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC's monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-

isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org