SHARING SINCE 2010
Health-ISAC™
Collaborating for Resilience in Healthcare

Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare™ ○ TLP:WHITE Alert ID : 461a3151 Aug 11, 2023, 04:06 PM

This week, *Hacking Healthcare*^{TM} examines the possibility of the Biden administration pursuing a general ban on ransomware payments as a means to disincentivize ransomware actors. We provide a brief background on the United States government's policy towards ransomware, including the recent remarks that have brought the issue back to light, and then analyze why we think fears of a near term policy change to ban payments feels unlikely.

Biden Administration Considering Banning Ransom Payments?

Whispers that the Biden administration may have an interest in pursuing a broad ban on ransomware payments has raised some eyebrows over the past few months. The private sector, especially critical infrastructure entities, are right to be concerned about what that may mean. However, after presenting some background on the issue, we will explain why we are skeptical that this approach will be pursued and why it may not be as impactful as feared for healthcare organizations.

Background: Ransomware Policy

For context, while ransomware has been around for quite some time, the explosion of ransomware attacks that continuously stole headlines only really got going around 2017. While roughly six years probably feels like an age to healthcare's network defenders, in the policy sphere, things move much less quickly. Over this time period, government policy has been to heavily discourage ransomware payments and selectively ban them where such payments may involve sanctioned actors, but never to blanket ban such payments.[i]

Between changeovers in Presidential administrations, the growth of the Cybersecurity and Infrastructure Security Agency (CISA), the creation of the Office of the National Cyber Director (ONCD), and the Department of Health and Human Services (HHS) attaining a better understanding of the issue, a federal strategy to counter ransomware has been largely uneven and uncoordinated until relatively recently. Some of the more notable actions to be taken include the Biden administration launching an international ransomware initiative in 2021, the public-private Ransomware Task Force Report in 2021, and the 2022 National Cyber Strategy.[ii], [iii], [iv] 2021 was the previous time this issue appeared to be gaining significant traction. At that time, the White House decided against pursuing such a ban, with CISA Director Anne Neuberger stating that while she “initially… thought [a ban] was a good approach,” discussions with the private sector convinced them it would only harm victims and drive payment activity underground.[v] Even the FBI came out against the idea, with a senior official telling the Senate Judiciary committee that “it would be our opinion that if we ban ransom payments, now you are putting U.S. companies in a position to face yet another extortion, which is being blackmailed for paying the ransom and not sharing that with authorities.”[vi]

Recent Comments

Talk of a possible ban on ransomware payments returned this past May due to comments made by Neuberger during an event hosted by the Ransomware Task Force. Noting that the only way to systemically cure the ill of ransomware is cutting off its profitability, Neuberger is quoted as saying that “for an individual entity, it may be they make a decision to pay, but for the larger problem of ransomware, that is the wrong decision.”[vii]

Action & Analysis

Included with Health-ISAC Membership

Congress

Tuesday, August 8

No relevant hearings

Wednesday, August 9

No relevant meetings

Thursday, August 10

No relevant meetings

International Hearings/Meetings

No relevant meetings

EU

No relevant meetings

About the Author

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

[i] https://ofac.treasury.gov/media/912981/download?inline
[ii] https://securityandtechnology.org/ransomwaretaskforce/
[iii] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/
[iv] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[v] https://cyberscoop.com/anne-neuberger-ransomware-cryptocurrency/
[vi] https://thehill.com/policy/cybersecurity/565110-top-fbi-official-advises-congress-against-banning-ransomware-payments/
[vii] https://www.politico.com/newsletters/future-pulse/2023/05/10/a-tb-fighter-sees-reason-for-hope-00096140
[viii] https://www.cybersecuritydive.com/news/white-house-considers-ransom-payment-ban/649673/
[ix] https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments
[x] https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments

Report Source(s)

Health-ISAC

Reference | References

Cyberscoop
treasury
cybersecuritydive
Politico
Health-ISAC
Whitehouse
The Hill
Whitehouse
securityandtechnology
Coveware

Tags

Biden, Regulation, Hacking Healthcare, Ransomware Payment, law, Ransomware

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

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

Hacking Healthcare:

Written by John Banghart, who 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.

John can be reached at jbanghart@h-isac.org and jfbanghart@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