This week, Health-ISAC®'s Hacking Healthcare® checks in on the state of ransomware. In particular, we examine encouraging reports that suggest a significant drop off in ransomware payment resolution and total payment made to ransomware actors in the second half of 2024. In the action and analysis section, we examine how these findings may influence the discussion around ransom payment bans, increasing law enforcement collaboration, and a potential policy shift on offensive cyber operations.

Welcome back to Hacking Healthcare®.

The State of Ransomware and the Potential of "Offensive Cyber Operations"

From time to time, Hacking Healthcare likes to assess the ever-evolving state of ransomware, and an interesting new report from Chainalysis provides a good reason to do so. In addition to breaking down the highlights and trends found in the report, the Action & Analysis section takes an expanded look at how "offensive cyber operations" might augment the law enforcement portion of the report.

Chainalysis Report

On February 5, the blockchain analysis firm Chainalysis published a report[i] that made some interesting claims about the state of ransomware in 2024. Their report states that:[ii]

- "The total volume of ransom payments decreased year-over-year (YoY) by approximately 35%"—down to $813.55M from $1.25B last year.
- The payment decrease was allegedly "driven by increased law enforcement actions, improved international collaboration, and a growing refusal by victims to pay."
- Much of the decline comes as a result of significantly less payment activity in the last six months of the year.
- The disruption and collapse of major cybercriminal groups like LockBit and BlackCat/ALPHV, as well as the lack of a major player to fill the void that was created, have been major contributing factors.
- Blockchain and data leak site analysis suggested that more victims may be refusing to pay ransoms.

- "Thanks to improved cyber hygiene and overall resiliency, victims are increasingly able to resist demands and explore multiple options to recover from an attack."

The report's findings are roughly aligned with other reports on the ransomware landscape. Ransomware remediation firm Coveware's most recent quarterly report[iii] also credited the success of law enforcement actions as a critical driver of lowered total ransomware costs. Coveware also elaborates on ransomware payment resolution rates, finding a "drop in the percentage of companies paying ransoms to an all-time low of 25%."[iv]

Action & Analysis

Included with Health-ISAC Membership

[i] https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

[ii] https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

[iii] https://www.coveware.com/blog/2025/1/31/q4-report

[iv] https://www.coveware.com/blog/2025/1/31/q4-report

[v] https://health-isac.org/health-isac-hacking-healthcare-1-17-2025/

[vi] https://www.coveware.com/blog/2025/1/31/q4-report

[vii] https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

[viii] https://homeland.house.gov/hearing/unconstrained-actors-assessing-global-cyber-threats-to-the-homeland/

[ix] https://www.washingtontimes.com/news/2025/jan/22/washington-eyes-new-offensive-cyber-operations-pri/

[x] https://www.cbsnews.com/news/michael-waltz-trump-national-security-adviser-face-the-nation-transcript-12-15-2024/

[xi] https://www.cbsnews.com/news/michael-waltz-trump-national-security-adviser-face-the-nation-transcript-12-15-2024/

Report Source(s)

Health-ISAC

Release Date

Feb 11, 2025, 10:59 PM

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

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 Councils 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 Councils 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-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

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

Tim can be reached at tmcgiff@venable.com.

Turn off Categories:

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

Access the Health-ISAC Threat 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 Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org