Potential Threats to Healthcare Executives Are Circulating On-Line

Threat Bulletins	TLP:WHITE	Alert Id: da2c7f6d	2024-12-09 16:18:40

Health-ISAC has received reports of multiple on-line postings threatening executives within the health sector. Forums have been identified as a source of threats targeting CEOs in the healthcare industry, particularly those leading major health insurance companies and pharmaceutical firms.

These threats, which range from general intimidation to specific calls for violence, have emerged in the wake of the recent killing of a UnitedHealthcare CEO. It is important to note that the perpetrator of this recent assassination has not yet been apprehended, and the investigation into the possible motives is still ongoing.

While these circulating threats have not been verified, Health-ISAC recommends heightened security awareness among healthcare executives and more stringent security measures to ensure safety.

Calls for violence may extend to the cyber domain, leading hacktivists to carry out DDoS and other disruptive attacks on the health sector. Health-ISAC recommends that members remain vigilant about safeguarding all infrastructure and that organizations share any specifics they can about threats to executives so we can keep the community informed.

Sourcing of the post on 4chan threatening several healthcare industry CEOs.
hxxps://i[.]4cdn[.]org/pol/1733459214350069.jpg

hxxps[:/]/newmitbbs[.]com/viewtopic[.]php?t=656257

Recommendations:

- Remove personally identifiable information (PII) regarding executives from the company's website, and third-party public data aggregators.
- Conduct open-source intelligence (OSINT) investigations against senior leadership and C-suite personnel to identify what information is publicly available.
- Provide additional security measures for ongoing and upcoming public events, including conferences and summits where they may be speaking.
- Bolster executive protection measures for C-suite personnel by assigning protective details, recurring personalized threat assessments, and physical penetration tests on primary residences to shore up security gaps.
- Inform CEOs and executives about the potential threats and encourage them to be vigilant.
- Establish clear communication channels for reporting suspicious activity or threats.
- Conduct regular security awareness training for all employees.
- Maintain close contact with law enforcement agencies to share information and coordinate efforts.
- Report any credible threats or suspicious activity to the appropriate authorities.
- Increase intelligence-gathering efforts by monitoring forums and other online spaces for emerging threats to healthcare executives and leveraging OSINT tools to gather information that directly mentions the company.
- Share reports of threats to executives and/or organization infrastructure to Health-ISAC.

Incident Date: Dec 09, 2024 (UTC)

Tags: Healthcare Industry Threats
TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
Share Threat Intel:
For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.
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