THREAT BULLETINS

Pro-Russian Hacktivist DDoS Campaign Targeting Healthcare

TLP:WHITE

Feb 06, 2023

On January 27, pro-Russian hacktivists operating on cybercriminal forums threatened to demolish attack the networks of medical institutions in the United States, United Kingdom, and abroad. The threats were purported to be a response to new aid packages providing security assistance for Ukraine.

On January 28, hacktivist threat actors shared screenshots from a list of hospitals and medical organizations on Twitter. Health-ISAC acquired the complete list of hospitals and medical organizations intended to be targeted and began alerting the potential victims.

Health-ISAC and the Department of Health & Human Services Health Sector Cybersecurity Coordination Center (HC3) delivered targeted alerts to organizations the hacktivists aggregated targeted for orchestrating the DDoS attacks. The targeted alerts included the

domains shared by the hacktivists believed to be the intended DDoS targets. Health-ISAC delivered the alerts in a timely manner to a dedicated cyber threat intelligence point-of-contact within those member organizations with established intelligence point-of-contacts.

On January 28, in addition to delivering the targeted alerts, Health-ISAC published a TLP:GREEN Threat Bulletin to provide members of the community and partners with additional context to support the targeted alerts delivered. This also ensured that unlisted organizations could enable proactive DDoS mitigation measures considering the healthcare sector being targeted.

Organizations leveraged the information in the alerts to ensure DDoS mitigation services were adequately configured and load balancers were aligned appropriately given the intended domain to be targeted.

On January 30, Health-ISAC aggregated the initial feedback provided by members who received targeted alerts and members who shared reports of a DDoS campaign impacting operations. The updated alert included a Health-ISAC White Paper on DDoS Strategies.

On January 31, Health-ISAC shared 48 additional healthcare organizations were added to the target list of threat actors orchestrated DDoS attacks. The alert also shared indicators of compromise (IOCs) observed by members within the healthcare community shared for the sector to leverage for defense measures.

On February 3, Health-ISAC provided additional mitigation guidance and web application firewall configuration settings shared by members that proved effective within their environments. The updated alert also included guidance from Health-ISAC encouraging member organizations not to make any public statements about DDoS attack impacts. The media coverage of DDoS campaigns only encourages the threat actors to continue the attacks against hospitals.

Health-ISAC would like to thank the community for sharing insights from their environments and helping bolster the security posture of the healthcare sector during this recent campaign.

Reference(s)	Health-ISAC DDoS Whitepaper
Report Source(s)	HC3, Health-ISAC

Recommendations
Health-ISAC recommends organizations:

- Enable a DDoS mitigation or system or service - Health-ISAC White Paper on DDoS Strategies.
- Enable web application firewalls to mitigate application-level DDoS attacks.
- Implement a multi-content delivery network (CDN) solution to distribute and balance web traffic.
- Enabling blocking of Anonymous Proxies - attacks were observed moving through Anonymous Proxies. Many of the XDR technologies support the blocking of anonymous proxies.
- Organizations are encouraged to geo-block web requests according to the geography of their business operations.
    - Healthcare organizations have also observed the majority of denial-of-service requests originating outside their business operations geography.
    - For organizations that can geo-block web requests, consider filtering out requests originating outside of your business operations geography. For example, if you are located in "Country A" and have customers and business partners only in "Country A," then you could geo-block IP addresses outside "Country A."

Alert ID 5db8ed44

View Alert

Tags Health-ISAC, HC3, DDoS, Healthcare

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

Conferences, Webinars, and Summits

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

Turn off Categories For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

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

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**