PUBLICATION

U.S. Health Care Sector Should Take Immediate Mitigating Actions Due to Targeted Attacks by Pro-Russia Hacktivist Group

Authors: Layna S. Cook Rush
February 02, 2023

Health care providers of all sizes should be reviewing their Distributed Denial of Service (DDoS) mitigations and response plans immediately. On February 2, a pro-Russia hacktivist group, dubbed "Killnet," called upon all of its members to actively target named entities in the U.S. health sector. Earlier this week, Killnet actors targeted more than a dozen U.S. hospitals using DDoS attacks, crippling their forward-facing webpages, and reportedly exfiltrating protected health information.

Killnet emerged in the wake of last year's Russian invasion of Ukraine. The group, aligned with the Russian government, is composed of pro-Russia hackers from around the world who conduct DDoS attacks and misinformation campaigns against supporters of Ukraine. The most recent targeting of U.S. hospitals comes on the heels of the U.S. government announcement that it would be sending Abrams Main Battle Tanks to Ukraine.

Threat

In the early morning hours of February 2, Killnet posted to its followers on Telegram the following task:

"The largest DDoS attack on the US medical sector is announced. The list of targets included corporate networks of hospitals, hospitals, [and] providers of online medical services. May the bandwidth of the global network be with us! List of goals for all participants in the event: [provided separately] We are Russians, We are Killnet!"

DDoS Mitigations

A DDoS attack is a malicious attempt to negatively impact the availability of a webpage, system, or network by using bots to flood the target with thousands or hundreds of thousands of requests per second. Because the webpage, system, or network cannot handle that volume of traffic, it crashes, resulting in unavailability for hours or days.

To limit damage and downtime from DDoS attacks, network defenders of targeted health care providers should take immediate mitigation steps:

- Check firewall rules and rate-limiting rules, and reduce the traffic allowed to any public-facing website based on historic usage.
- Enable caching to limit the impact to servers.
- Enable DDoS alerting.
- If using Cloudflare, ensure all DDoS Managed Rules are set to default settings, and enable Adaptive DDoS Protection.

- Temporarily block traffic from foreign IP addresses.
- Consider leveraging managed IP lists in firewall rules.
- Consider taking sites down as traffic destabilizes the network to avoid a breach.

Summary

Killnet has a history of targeting organizations across U.S. critical infrastructure sectors, including health care, and will continue to do so. This is not an idle threat. Health care providers of all sizes should be reviewing their DDoS mitigations and response plans immediately.

For more information, see the Department of Health and Human Services Analyst Note detailing the threat Killnet poses to the health sector here.

For immediate assistance in the event of an attack, contact Baker Donelson's Data Incident Response Team on our 24-hour incident response hotline: 1-877-215-6115, or contact Layna Cook Rush or another member of Baker Donelson's Data Incident Response Team.