HC3: Analyst Note
February 13, 2023 TLP:CLEAR Report: 202302131500

Healthcare Sector DDoS Guide

Executive Summary

Distributed Denial of Service (DDoS) attacks have the potential to deny healthcare organizations and providers access to vital resources that can have detrimental impact on the ability to provide care. In healthcare, disruptions due to a cyber-attack may interrupt business continuity by keeping patients or healthcare personnel from accessing critical healthcare assets such as electronic health records, software-based medical equipment, and websites to coordinate critical tasks. (See HC3 Analyst Note titled: Pro-Russian Hacktivist Group 'Killnet' Threat to HPH Sector). Link can be found here.

Threat actors utilize DDoS attacks due to the cost effectiveness, and relatively low resources and technical skills needed to deploy this type of attack as a hacker doesn't have to install any code on a victim's server. Moreover, DDoS attacks are getting more sophisticated and complex while getting easier and cheaper to perpetrate as cyber criminals take advantage of the sheer number of insecure internet-connected devices. (**Analyst Comment:** It is strongly recommended by cybersecurity institutions like the National Institute of Standards and Technology, that organizations effectively manage the cybersecurity and privacy risks associated with Internet-of-Things (IoT)). (See NIST Report (NISTIR) – 8228). Link can be found here.

Report

What is DDoS?

Distributed-Denial-of-Service (DDoS) attacks can be classified as a logic and resource exhaustion flooding attack. Logic attacks exploit security vulnerabilities to cause a server or service to crash or significantly reduce performance. Resource exhaustion flooding attacks cause the server's or network's resources to be consumed to the point where the service is no longer responding, or the response is significantly reduced.

DDoS Killchain

A threat actor can use DDoS at various stages of an attack. In the early reconnaissance stage, threat actors use it to test an organization's preparedness to respond to an initial attack and to cover up activities such as port scanning. Threat actors may then use it to produce extraneous forensic logs and data files at the weaponization or malware delivery stage, and then to make identification and eradication of planted malware challenging. At the data extraction stage, it will be used as a diversionary tactic to conceal exfiltration of confidential data.

Web Applications

DDoS attacks can be a precursor to a much larger nefarious plot of a threat actor. Often, DDoS attacks are used as smokescreens to divert a target victim's attention and resources while threat actors deploy potentially more malicious attacks. Application layer DDoS attacks, specifically ransom DDoS attacks, are on an uptick. Reports claim ransom DDoS attacks increased by 67 percent year-on-year and 24 percent quarter-on-quarter.

Web applications are essential to the healthcare sector, allowing patients and healthcare professionals to submit and retrieve data to/from a database over the internet using a preferred web browser. Common web applications in the healthcare sector include patient portals, telehealth services, electronic health

record systems, webmail for hospitals and clinics, and patient monitoring applications with IoT devices, etc. Adversaries will use web application attacks, such as DDoS attacks, to target an organization's most exposed infrastructure, such as web servers to exploit a weakness in an internet facing computer or software.

There are a variety of processes, technologies, and methods to protect against DDoS and other web application attacks. Web applications, like all software, may inevitably contain defects. First and foremost, web application security and sourcing, which is a collection of security controls engineered into a web application, must be a security priority to defend healthcare assets from cyber criminals. Specifically, to help secure and mitigate DDoS Attacks, healthcare organizations should sanitize, increase resource availability, implement cross-site scripting (XSS) and cross-site request forgery (XSRF) protections, implement Content Security Policy (CSP), audit third party code. Additional steps include running static and dynamic security scans against the website code and system, deploying web application firewalls, leveraging content delivery networks to protect against malicious web traffic, and providing load balancing and resilience against high amounts of traffic.

UDP, SYN, and TCP DDoS Attacks

Healthcare sector defenders should prioritize User Data Protocol (UDP), SYN (synchronize), and Transmission Control Protocol (TCP) as likely vectors that threat actors will use to perpetuate DDoS attacks. According to security researchers, as of Q2 of 2022, UDP attacks accounted for 62.53 percent of all DDoS attacks. SYN accounted for 20.25 percent and TCP 11.4 percent of all DDoS attacks respectfully.

DDoS Mitigation Quick Guide

The healthcare sector can more effectively defend against the potential impact of a DDoS attack by taking methodical inventory of critical assets, and to prepare contingency plans for a variety of circumstances in which those assets may come under attack from a determined threat actor. Healthcare organizations should prioritize identifying services and devices that may be exposed to the public internet, vulnerabilities, and how a user base connects to networks. Moreover, it is recommended that healthcare organizations engage service providers such as internet service providers (ISP) and cloud service providers, etc., to understand dedicated edge network defenses and develop a DDoS contingency plan.

Quick DDoS reference guide:

- General considerations:
  - Most DDoS attacks will focus on overwhelming resources for a specific system or application.
  - Identify specialized equipment and software to defend against DDoS attacks for your specific assets and networks. Also, understand your equipment capabilities in preventing and mitigating a DDoS.
  - Identify key IT professionals that will participate during incident response; try to limit the number of people on a team for efficient workflow.
- Preparing for an attack:

  - Document internet-facing (IoT, servers, applications) and IT infrastructure assets by preparing a network topology diagram and an asset inventory.
  - Contact services providers to understand what DDoS capabilities are and can be provided, i.e., Service Level Agreement (SLA).
  - Understand business implications.
  - Create a whitelist of prioritized source IPs and protocols you must allow during an attack.
  - Identify, confirm, and appropriately configure DNS time-to-live settings for systems that might be targeted.
  - Develop a SOP for coordinating with your internal and service provider legal teams.
  - Consider implementing or changing defense strategies one at a time, so that you can efficiently analyze cause and effect of a change.

- Assessing the attack:
  - Understand the tactical and strategic flow of a DDoS attack and identify infrastructure components at risk.
  - Coordinate with services providers to identify their visibility into an attack and mitigation assistance, such as specific traffic you would like to control (blackhole network blocks, source IP rate limits, etc.).
  - Review logs of servers, routers, firewalls, applications for patterns, anomalies, discrepancies, and what aspects of the DDoS traffic differentiate from benign traffic such as TCP flags, specific source IPs, destination ports, etc.
  - Utilize a network analyzer to review traffic (e.g., tcpdump, MRTG, etc.).
  - Coordinate with your internal and third-party legal teams.

- Mitigating Effects of a DDoS Attack:
  - Use a load balancer, router, or specialized device to throttle or block specific traffic.
  - Terminate suspicious connections or processes on servers and routers. Also, tune their TCP/IP settings.

- Blackhole DDoS traffic targeting the original IPs.
- Configure egress filters to block traffic that your IT infrastructure may send in response to a DDoS attack.
- If possible, add additional server and network bandwidth to curb the DDoS load.

- Incident conclusion:
  - Thoroughly document lessons learned, specifically what worked and what didn't and why. Consider what preparation steps can be taken next time for better incident response.
  - Assess the effectiveness of your organization's DDoS preparedness, especially people and communication.
  - Evaluate relationships, internal and external, to your organization that could assist with the planning and incident response of future attacks.
- Additional DDoS Resources:
  - Understanding Denial-of-Service Attacks | CISA
  - Advanced DDoS Mitigation Techniques | NIST
  - Distributed Denial of Service DDoS Attacks | H-ISAC

References

A Summary of Dos/DDOS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment
1212.pdf (egnyte.com)

DDoS Attack Used As Smokescreen
DDoS Attack Used As Smokescreen (netscout.com)

Cloudflare DDoS Threat Report 2022 Q3
Cloudflare DDoS threat report 2022 Q3

CISA Security Tip (ST18-006) Website Security
Website Security | CISA

DDoS Attacks in Q2 2022
DDoS attacks in Q2 2022 | Securelist

HC3: Analyst Note
February 13, 2023 TLP:CLEAR Report: 202302131500

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback