Understanding DoS and DDoS Attacks: Their Impact, Trends, and Mitigation Strategies
Understanding DoS and DDoS Attacks: Their Impact, Trends, and Mitigation Strategies

 Bernard Sfez - 2024-02-06 10:00

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are among the most disruptive cybersecurity threats faced by businesses and governments alike. These attacks involve overwhelming a system with excessive traffic to render it inaccessible, thereby causing significant service disruptions. While DoS attacks are typically launched from a single source, DDoS attacks leverage a multitude of sources, making them much more difficult to mitigate.

Recent trends indicate a surge in such attacks, with a notable example being the 2023 HTTP/2 protocol exploit that saw major tech giants like Google and Amazon fend off record-breaking levels of traffic.

This article explores these threats and outlines key strategies for mitigating risks, such as the use of DDoS protection services, network security protocols, secure authentication methods, proactive monitoring, and more. By implementing these strategies, businesses can significantly reduce their vulnerability to such attacks and safeguard critical infrastructure.

Understanding DoS and DDoS Attacks: Their Impact and Potential Risks

To clarify, a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. In simple terms, DoS attacks aim to flood a target server with overwhelming traffic, rendering it inaccessible or slow to legitimate users. A DDoS attack differs slightly in that it leverages multiple sources—either people or bots—to carry out the assault, exponentially increasing its impact.

Source: wikipedia
In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests .../...

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. More sophisticated strategies are required to mitigate this type of attack; simply attempting to block a single source is insufficient as there are multiple sources...

DoS and DDoS attacks trend (updated 2023)

Based on CVE (cataloging cybersecurity vulnerabilities and attacks), total incidents declared DDoS attacks have more than doubled over 2023, exploding from just over 1,000 in 2022 to more than 2,100 a year later.

One common method of attack involves saturating the target mechanism with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

One of the most significant DDoS attacks of 2023 involved the exploitation of a new vulnerability in the HTTP/2 protocol, which was exploited by a technique called the "Rapid Reset" attack. Major tech companies, including Google, Amazon, and Cloudflare, observed record-breaking levels of traffic during these attacks in August 2023. Google mitigated an attack peaking at an unprecedented 398 million requests per second (RPS), while Amazon and Cloudflare saw similarly massive attacks with peaks of 155 million and 201 million RPS, respectively. World Economic Forum

Although specific financial figures for this attack aren't fully disclosed, industry experts estimate potential costs in the millions for affected companies, covering lost revenue, mitigation efforts, and damage to infrastructure. Costs also stemmed from downtime and emergency fixes, which required collaborative updates and protocol adjustments by numerous service providers to control the attack.

Common Tactics of DoS Attacks

One of the most popular methods is saturating a target server with external requests, ultimately overwhelming its capacity and preventing legitimate access. In general, DoS attacks can be performed by:

- Consuming Resources: Overloading the server's capacity, causing it to crash or slow down.
- Resetting Targeted Computers: Forcing a targeted machine to reset, interrupting services.
- Obstructing Communication: Blocking communication channels between users and the target, effectively cutting off access.
- In more advanced scenarios, large-scale attacks can involve malicious code sent to a subhost, which then uses a botnet—a network of automated bots—to flood the target with

millions of requests per second. This type of attack can be aimed at either a single IP (for business motivations) or an IP range (for political or military motivations).

Uncovering Data Through DoS Attacks: Indirectly Exploiting Vulnerabilities

While a DoS attack typically doesn't provide direct access to data, there are scenarios where information could unintentionally be exposed:

- Network Mapping: When backing systems go offline, load balancers may expose internal network details, such as subnet information or internal machine names, which attackers can use to map the target infrastructure.
- Error Message Data: If a DoS attack shuts down a database, error messages may expose critical information like database engine type, connection usernames, or internal IP addresses.
- API and Web Software Vulnerabilities: Poorly designed APIs or web applications may have a "fail-open" setting, allowing unauthorized access if the Single Sign-On (SSO) server fails due to a DoS attack.
- Advanced Persistent Threat (APT) Operations: In sophisticated APT scenarios, attackers might DoS detection systems to evade security alerts while they gather data from the network.
- Firewall Admin Interface: A DoS on firewall admin interfaces can slow down response efforts by the network administration team.
- Key Revocation Attacks: Targeting key-revocation services could allow attackers to continue using compromised credentials without being flagged.

Beyond Overloading: The Secondary Purpose of DoS Attacks

DoS attacks may not only be about crashing a service. Often, they're used as a "smoke screen" to distract IT teams while other, more invasive breaches are attempted. This two-pronged attack approach can prepare the ground for later, more impactful phases of an attack.

Mitigating DoS Risks: Key Strategies

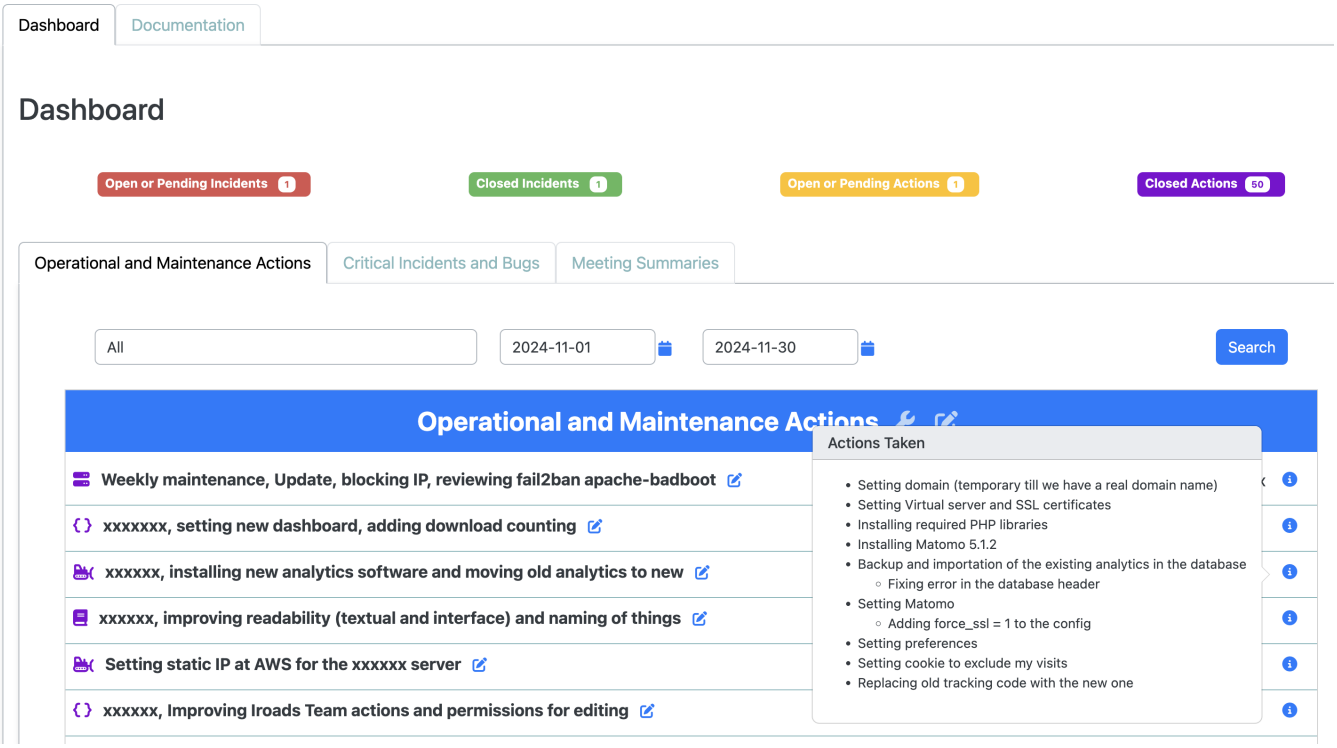
To reduce the likelihood and impact of a DoS attack, implement precise monitoring, consistent documentation, and proactive measures.

At OpenSource Solutions, we've implemented a comprehensive protocol that encompasses all aspects of proactive monitoring and maintenance. For enterprise-grade projects, we use active monitoring tools, alongside a structured weekly maintenance protocol. Additionally, our approach includes a monthly-reviewed maintenance protocol with a focus on the following key elements:

- DDoS Protection Services: Utilizing DDoS protection systems to provide Out-of-Band Detection, High Traffic Volume Management, Attack Identification and Response.

- Networking Protection: We configure and adjust firewalls and banning rules to provide a critical layer of defense against DoS attacks. By implementing strict access controls, we filter out malicious traffic and prevent unauthorized access to services. This access control strategy includes blocking redundant attempts to access non-existent resources, applying Geo-Blocking, rate-limiting, all measures tailored based on a detailed analysis of the project's specific security needs and constraints.
- Updating and Upgrading Components: We keep track of all software, libraries, and third-party components that enable a project to fulfill its intended purpose, ensuring that they are updated regularly. This includes monitoring updates from cybersecurity and governmental agencies, as well as private security organizations, to take immediate action in response to emerging threats.
- Secure Authentication and Permissions: 2FA (Two-Factor Authentication), strong passwords, unique usernames, clear group names, and well-defined permissions.
- Content Access: Through regularly audit of the page access we identify and secure forbidden pages or area (administrative, test pages, etc.) ensuring they are either removed or set to private. Additionally, we actively manage crawler and search bot access, allowing or blocking them as needed to prevent unnecessary resource usage and enhance security.
- Review of Web-based Applications: APIs and web software should be reviewed and secured before becoming accessible online.
- Proactive Monitoring and Alerts: We utilize advanced monitoring and alerting tools that notify IT administrators of potential issues in real-time. These tools also enable the analysis of more subtle, insidious behaviors that could indicate security vulnerabilities or performance degradation.

We track and log all issues and actions taken, ensuring that this information is discussed and reviewed with our customers and partners during our weekly or monthly meetings. This approach keeps everyone informed about progress, challenges, and resolutions, fostering transparent communication and collaboration.


Dashboard
Documentation
Dashboard
Open or Pending Incidents 1
Closed Incidents 1
Open or Pending Actions 1
Closed Actions 50
Operational and Maintenance Actions
Critical Incidents and Bugs
Meeting Summaries
All
2024-11-01
2024-11-30
Search
Operational and Maintenance Actions
Weekly maintenance, Update, blocking IP, reviewing fail2ban apache-badboot
xxxxxxx, setting new dashboard, adding download counting
xxxxxx, installing new analytics software and moving old analytics to new
xxxxxx, improving readability (textual and interface) and naming of things
Setting static IP at AWS for the xxxxxx server
xxxxxx, Improving Iroads Team actions and permissions for editing
Actions Taken
Setting domain (temporary till we have a real domain name)
Setting Virtual server and SSL certificates
Installing required PHP libraries
Installing Matomo 5.1.2
Backup and importation of the existing analytics in the database
Fixing error in the database header
Setting Matomo
Adding force_ssl = 1 to the config
Setting preferences
Setting cookie to exclude my visits
Replacing old tracking code with the new one