Protecting your organization against denial of service attacks

CANADIAN CENTRE FOR CYBER SECURITY

July 2022 | ITSAP.80.100

Threat actors carry out denial of service (DoS) attacks to disrupt the availability of an organization’s services and data. If successful, a DoS attack prevents people from accessing online services (e.g. email, websites, online accounts), information, and other network resources. Threat actors carry out DoS attacks (and are sometimes hired to do so) for different reasons, such as attacking for fun or attempting to disrupt a competitor organization or another country’s democratic systems during elections. DoS attacks are also used by hacktivist groups to protest political or social issues.

DoS attacks can target specific infrastructure, network applications, and other systems such as industrial control systems (ICS). In a DoS attack, the threat actor floods the target (e.g. a server hosting a website or an organization’s network) with traffic. The target is then overloaded by this traffic and cannot respond to it or the system crashes. When this occurs, a user may receive an error message when trying to access a website. Threat actors use different methods to carry out DoS attacks:

- **Flooding attacks:** Flooding attacks are the most common attack method. The threat actor repeatedly sends requests to connect to the target server but does not complete the connections. These incomplete connections occupy and consume all available server resources. As a result, the server cannot respond to legitimate traffic and connection attempts.
- **Crash attacks:** Crash attacks are less common. The threat actor exploits system vulnerabilities to crash a system.

Distributed DoS attack

A distributed DoS (DDoS) attack has the same goal of disrupting and preventing access to services and information, as a DoS, but it looks a bit different. To carry out a DDoS, a threat actor uses multiple machines to attack one target. While a DDoS attack can be a coordinated effort between a group of threat actors, it can also be carried out by one person using a botnet. DDoS increases the attack power but also makes it harder to identify the true source of the attack.

Security Tip (ST04-015) published by the U.S Cybersecurity and Infrastructure Security Agency (CISA) indicates that DDoS attacks have increased with more usage of Internet of Things (IoT). Current IoT devices have a low degree of IT security control and weak encryption capabilities, leaving devices vulnerable to potential threats and exploitation.

Check out CISA’s DDoS Quick Guide for info on possible attack methods, potential impacts and applicable mitigation strategies.

A **botnet** is a group of hijacked Internet-connected devices. To create a botnet, a threat actor takes advantage of security vulnerabilities or device weaknesses to control numerous devices. To prevent systems and devices in your network from becoming part of a botnet, protect your devices by running updates and security patches.

Impact of a DoS attack

DoS attacks are designed to exhaust your network’s resources, such as its bandwidth, computing power, memory, and storage.

In addition to losing access to services and resources, a threat actor may also use a DoS attack to distract your organization while other malicious activities are carried out, such as attempting to steal data.

Your organization may also be impacted in the following ways:

- Costs associated with responding to a DoS attack
- Lost or limited functionality of the affected service
- Decreased productivity

Your organization does not have to be the target of a DoS attack to be impacted. If your service providers (e.g. Internet service provider, cloud service provider) is attacked, your organization may experience loss of service.

Protecting your organization against denial of service attacks

CANADIAN CENTRE FOR CYBER SECURITY

July 2022 | ITSAP.80.100

Recognizing a DoS attack

Look out for the following signs that may indicate that you're the victim of a DoS attack:

- Slow network performance, such as when opening files or accessing websites
- Unavailable or inaccessible websites
- Inability to retrieve sensor data, or control critical processes of your ICS

These signs can resemble non-malicious performance and availability issues (e.g. a surge of visitors to your website following a press release). Over an extended period, your organization should establish a baseline of what is considered normal network activity. You can use this baseline to understand large increases or decreases in network activity and indicate any attempts to flood the network. To distinguish a possible DoS attack from non-malicious issues, your organization should continuously monitor and analyze traffic and logging information, which you can use to identify crashing and restarting services.

Preventing a DoS attack

You can reduce the possibility and the impact of DoS attacks with the following actions:

- **Work with your cloud and Internet service providers to implement service level agreements that include DoS defence provisions.** Your service providers may use multiple tools and techniques to help your organization protect itself against DoS attacks.
- **Ensure your system administrators are familiar with DoS protection services.** Familiarity with these services can help them effectively rate limit or whitelist.
- **Monitor network and systems.** Configure monitoring tools to alert you when there is an increase in traffic (outside of your baseline) or any suspicious traffic overloading a site.
- **Install and configure firewalls and intrusion prevention systems.** You can use these tools to monitor traffic and block known-malicious and illegitimate traffic.
- **Install and maintain anti-virus and anti-malware software**. Securely configure anti-virus and anti-malware software on all connected devices. Enable anti-malware solutions that update and scan automatically.
- **Update and patch operating systems and applications.** Update and patch systems and applications, including your firewalls, to ensure that security issues are addressed and prevent threat actors from taking advantage of vulnerabilities.
- **Use a website hosting service that emphasizes security.** Before you choose a service to host your website, verify that the vendor has security measures in place its customers.
- **Defend your network perimeter.** To protect your network, use a layered approach to security by implementing multiple controls and techniques.
- **Plan for an attack.** Have a recovery plan that prioritizes systems and processes based on their tolerable downtime. You should also identify points of contact and an incident response team.
- **Back up your data.** Create backups of your information and critical applications. Regularly test restore of your backups.

Responding to a DoS attack

Below are examples of actions to take if your organization is the victim of a DoS attack:

1. **Identify.** Flag any DoS indicators, such as poor network performance, and reference them against your normal traffic baseline. Contact your network administrator and Internet service provider to confirm the cause of the outage or issue.
2. **Contain.** Identify your organization's network perimeter and any exposed assets. Use network security systems, such as firewalls, or consider using DoS protection services that may be available through your service provider. Contact your Internet or cloud service provider as soon as possible.
3. **Recover.** Check for signs of other malicious activity that may have taken place during the DoS attack. Re-establish connections and communicate that services are back online. Ensure you have a strategy to gradually reconnect customer sessions.
4. **Review lessons learned.** After you have recovered from the attack, review all the actions taken. Make improvements and document changes in your response plan.

If your organization is the victim of a DoS attack, notify the Canadian Centre for Cyber Security: **contact@cyber.gc.ca**

Learn more

To find additional guidance and resources, you may refer to the following publications on our website:

- *Tips for backing up your information (ITSAP.40.002)*
- *How updates secure your device (ITSAP.10.096)*
- *Protect your organization from malware (ITSAP.00.057)*
- *Security considerations for industrial control systems (ITSAP.00.050)*
- *Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)*
- *Developing your incident response plan (ITSAP.40.003)*
- *Secure your accounts and devices with multi-factor authentication (ITSAP 30.030)*

Communications Security Establishment | Centre de la sécurité des télécommunications