

Preparation

1

Objective: Establish contacts, define procedures, and gather information to save time during an attack.

Internet Service Provider support

- Contact your ISP to understand the DDoS mitigation services it offers (free and paid) and what process you should follow.
- If possible, subscribe to a redundant Internet connection.
- If possible, subscribe to an Anti-DDoS service provider.
- Establish contacts with your ISP and law enforcement entities. Make sure that you have the possibility to use an out-of-band communication channel (e.g.: phone).

Inventory

- Create a whitelist of the IP addresses and protocols you must allow if prioritizing traffic during an attack. Do not forget to include your critical customers, key partners, etc.
- Document your IT infrastructure details, including business owners, IP addresses and circuit IDs, routing settings (AS, etc); prepare a network topology diagram and an asset inventory.

Network infrastructure

- Design a good network infrastructure without Single Point of Failure or bottleneck.
- Distribute your DNS servers and other critical services (SMTP, etc) through different AS.
- Harden the configuration of network, OS, and application components that may be targeted by DDoS.
- Baseline your current infrastructure's performance, so you can identify the attack faster and more accurately.
- If your business is Internet dependent, consider purchasing specialized DDoS mitigation products or services.
- Confirm DNS time-to-live (TTL) settings for the systems that might be attacked. Lower the TTLs, if necessary, to facilitate DNS redirection if the original IP addresses get attacked. 600 is a good TTL value.
- Depending on the criticality of services, consider setting- up a backup that you can switch on in case of issue.

Internal contacts

- Involve the NTT security team to check the firewall, F5, and network teams in case of issue.
- Collaborate with the business lines to understand business implications (e.g., money loss) of likely DDoS attack scenarios.

The "preparation" phase is to be considered as the most important element of a successful DDoS incident response.

Identification

2

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Analyze the attack

- Understand the logical flow of the DDoS attack and identify the infrastructure components affected by it.
- Understand if the client is the target of the attack or a collateral victim
- Review the load and log files of servers, routers, firewalls, applications, and other affected infrastructure.
- Identify what aspects of the DDoS traffic differentiate it from safe traffic
 - Source IP addresses, AS, etc
 - Destination ports
 - URLs
 - Protocols flags

Network analysis tools can be used to review the traffic behavior:
➔ Tcpcdump, Wireshark, Snort, MRTG, monitoring tools...

Involve internal and external actors

- Contact your internal teams to learn about their visibility into the attack.
- Contact the ISP to ask for help. Be specific about the traffic you would like to control:
 - Network blocks involved
 - Source IP addresses
 - Protocols
- Notify the NTT-BE's management team and legal teams.

Check the background

- Find out whether the customer received an extortion demand as a precursor to the attack.
- Search if anyone would have any interest into threatening the customer
 - Competitors
 - Ideologically-motivated groups (hacktivists)

Containment

3

Objective: Mitigate the attack's effects on the targeted environment

- Attempt to block DDoS traffic as close to the network's "cloud" as possible via F5, firewall, specialized device, etc.
- Terminate unwanted connections or processes on servers and routers and tune their TCP/IP settings.
- If possible, route traffic through a traffic-scrubbing service or product if exists via DNS or routing changes (e.g.: sink-hole routing), typically done by a service provider.
- Set up an alternate communication channel between networks and applications (e.g.: web server, mail server, voice server, etc.)
- Switch traffic to another ISP line if the customer has multiple lines.
- Configure egress filters to block the traffic that may send in response to DDoS traffic to avoid adding unnecessary packets to the network.
- In case of an extortion attempt, try to buy time with the fraudster. For example, explain that you need more time in order to get management approval.

If the bottleneck is at the ISP's side, only the ISP can take efficient actions. In that case, work closely with your ISP and make sure you share information efficiently.

Remediation

4

Objective: Take actions to stop the Denial of Service condition.

■ Contact client's ISP and make sure that it enforces remediation measures. For information, here are some of the possible measures:

- Filtering (if possible, at level Tier1 or 2)
- Traffic-scrubbing/Sinkhole/Clean-pipe
- Blackhole Routing

■ If the DDoS sponsors have been identified, consider involving law enforcement. This should be performed upon the direction of your company's executive and legal teams.

Technical remediation actions can mostly be enforced by your ISP.

Aftermath

6

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

■ Consider what preparation steps you could have taken to respond to the incident faster or more effectively.

■ If necessary, adjust assumptions that affected the decisions made during DDoS incident preparation.

■ Assess the effectiveness of DDoS response, involving people and communications.

■ Collaborate with legal teams if a legal action is in process

Recovery

5

Objective: Come back to the previous functional state.

Assess the end of the DDoS condition

- Ensure that the impacted services are reachable again.
- Ensure that your infrastructure performance is back to your baseline performance.

Rollback the mitigation measures

- Switch back traffic to your original network.
- Restart stopped services.

Ensure that the recovery-related actions are decided in accordance with the network teams. Bringing up services could have unexpected side effects.

DDoS incident response

Guidelines to handle Distributed Denial of Service incidents



IRM Author: Mounir Aarab
IRM version: 1.0

E-Mail: mounir.aarab@global.ntt

Abstract

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.

Who should use IRM sheets?

- Administrators
- Security Operation Center
- CISOs
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes and do not panic. Contact your CERT immediately if needed.

Incident handling steps

6 steps are defined to handle security Incidents

- Preparation: get ready to handle the incident
- Identification: detect the incident
- Containment: limit the impact of the incident
- Remediation: remove the threat
- Recovery: recover to a normal stage
- Aftermath: draw up and improve the process