INCIDENT RESPONSE METHODOLOGY

IRM #4
DDOS INCIDENT RESPONSE

Live Analysis on a suspicious Windows system

IRM Author: CERT SG
Contributor: CERT aDvens
IRM version: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

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 and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.

→ IRM CERT SG: https://github.com/certsocietegenerale/IRM

→ IRM CERT aDvens (French version): https://github.com/cert-advens/IRM

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process

IRM provides detailed information for each step of the incident response process. The steps come from NIST Computer Security Incident Handling Guide.

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

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 and to an Anti-DDoS services 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).
- Make sure your ISP and DDoS mitigation service have a 24/7 phone support.

Inventory

- Create a whitelist of the IP addresses and protocols you must allow if prioritizing traffic during an attack. Don't 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.
- Deploy a Web Application Firewall to protect against application-layer DDoS.
- 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 of the criticality of your services, consider setting-up a backup that you can switch on in case of issue.

Internal contacts

- Establish contacts for your IDS, firewall, systems, and network teams.
- Collaborate with the business lines to understand business implications (e.g., money loss) of likely DDoS attack scenarios.
- Involve your BCP/DR planning team on DDoS incidents.

IDENTIFICATION

Communication

- Prepare an internal and an external communication template about DDoS incidents.
- Identify channel where this communication will be posted.
- The “preparation” phase is to be considered as the most important element of a successful DDoS incident response.

Analyze the attack

- Keep in mind the DDoS attack could be a smokescreen hiding a more sophisticated and targeted attack.
- Check your anti-DDoS service analysis and your scrubbing centre reports:
  - Understand the logical flow of the DDoS attack and identify the infrastructure components affected by it.
  - Understand if you are 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 benign traffic:
  - Source IP addresses, AS, etc
  - Destination ports
  - URLs
  - Protocols flags

Network analysis tools can be used to review the traffic:
➔**Tcpdump, Tshark, Snort, Netflow, Ntop, MRTG, Cacti, Nagios**

If possible, create a NIDS signature to focus to differentiate between benign and malicious traffic.

Involve internal and external actors

- Contact your internal teams to learn about their visibility into the attack.
- Contact your ISP to ask for help. Be specific about the traffic you’d like to control:
  - Network blocks involved
  - Source IP addresses
  - Protocols

- Notify your company’s executive and legal teams.

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

Check the background

- Find out whether the company received an extortion demand as a precursor to the attack:
  - Check for emails in your security email gateway based on a keyword list.
  - Some threat actors send extortion demands directly to the email addresses in the Whois records of the targeted website.
- Look for revendications of the attack on Social Medias.
- Search if anyone would have any interest into threatening your company:
  - Competitors
  - Ideologically-motivated groups (hacktivists)
  - Former employees

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- If the bottleneck is a particular feature of an application, temporarily disable that feature.
- Attempt to throttle or block DDoS traffic as close to the network's "cloud" as possible via a router, firewall, load balancer, specialized device, etc.
- Terminate unwanted connections or processes on servers and routers and tune their TCP/IP settings.
- If possible, switch to alternate sites or networks using DNS or another mechanism. Blackhole DDoS traffic targeting the original IP addresses.
- Set up an alternate communication channel between you and your users/customers (e.g.: web server, mail server, voice server, etc.).
- If possible, route traffic through a traffic-scrubbing service or product via DNS or routing changes (e.g.: sinkhole routing).
- Configure egress filters to block the traffic your systems may send in response to DDoS traffic (e.g.: backsquatter 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 or anti-DDoS service's side, only they can take efficient actions. In that case, work closely with your ISP and/or anti-DDoS provider and make sure you share information efficiently.

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO STOP THE DENIAL-OF-SERVICE CONDITION.

- Contact your ISP and/or anti-DDoS provider and make sure that they enforce remediation measures. For information, here are some of the possible measures:
  - Filtering (if possible at level Tier1 or 2)
  - Traffic-scrubbing/Sinkhole/Clean-pipe
  - IP public balancing/splitting/switching
  - Blackhole Routing

Technical remediation actions can mostly be enforced by your ISP and/or anti-DDoS provider.

IF THE ATTACK HAD A MAJOR IMPACT, YOU MAY HAVE TO MAKE AN INCIDENT REPORTING TO REGULATORS.

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.

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

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.

For more details on authentication and infrastructure recovery, check the Large-scale malware compromise IRM-18

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

An incident report should be written and made available to all applicable actors.

The following topics should be covered:

- Initial detection
- Actions and timelines of every important events
- What went right
- What went wrong
- Impact from the incident
- Indicators of compromise

Lessons learned

Actions to improve the DDoS management processes should be defined to capitalize on this experience.

Consider what relationships inside and outside your organizations could help you with future incidents.