Distributed Denial of Service

Incident Response Playbook

By

Jonathan Lim

ACKNOWLEDGEMENT

This IRP used the following reference(s):

- AlertOps, ‘How to Create an Effective Incident Response Playbook’ on AlertOps (16 July 2018) <https://alertops.com/create-incident-response-playbook/>
- FBIIC, ‘D/DoS Incident Response Plan/Runboook’ on FBIIC (27 March 2013) <https://www.fbiic.gov/public/2013/mar/DDoS-RunBook.doc>
- Incapsula, ‘DDoS Response Playbook’ on Incapsula (15 August 2014) <lp.incapsula.com/rs/incapsulainc/images/DDoSResponse.pdf>
- Incident Response Consortium, ‘Playbook – DdoS’ on Incident Response Consortium (2019) <https://www.incidentresponse.com/playbooks/ddos>
- Lenny Zeltser, ‘Network DDoS Incident Response Cheat Sheet’ on Lenny Zeltser (2019) <https://zeltser.com/ddos-incident-cheat-sheet/>
- Noction, “DDoS Amplification Attacks’ on Noction (2019) <https://www.noction.com/blog/ddos-amplification-attacks>
- Suryawanshi, Chandra Prakash, ‘Playbook for DDOS Security Response’ on CISO Platform (6 May 2017) <http://www.cisoplatform.com/profiles/blogs/response-strategy-for-ddos>
- Weisman, Steve, ‘What is a distributed denial of service attack (DDoS) and what can you do about them?’ on Symantec Corporation (2019) <https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html>
- Williams-Shaw, Sydney, ‘How to build an incident response playbook’ on Swimland (1 May 2018) <https://swimlane.com/blog/incident-response-playbook/>

This Threat Intelligence and Incident Response Report was created for the community of the With You With Me - Cyber Security Analyst course.

PURPOSE

The purpose of this Incident Response Playbook (IRP) is to provide the organisations and cyber security analysts with a quick and easy-to-use set of procedural steps in responding to a given network security incident.

The IRP is designed to give as much possible information of dealing with a particular event or cyber security incident. However, due to the uniqueness of organizational networks, new technologies, and new forms of attacks – the level of detail of the advice rendered is more objective than subjective in nature.

Where a cyber security incident has occurred, the analyst is recommended to either create a new playbook for the given incident or modify an existing one; and then add in the specific details and hopefully step-by-step detailed process.

Indeed, cyber security analysts are encouraged to create or modify playbooks in anticipation of specific events. Each playbook follows the same format in a logical process flow:

1. Description
   - This provides the general description of the IRP and what incident it is suited for.
2. Flow Chart
   - An illustrated process flow to follow for an incident, which allows for an analyst for quick lookup. Should more detail steps be needed then the other sections can be referenced.
3. Detect and Analyse
   - The beginning phase, which is the detection and analyse stage of an incident.
4. Contain
   - This stage covers the steps for containing and minimizing the impact of the incident.
5. Eradicate and Recover
   - Once contained, then the incident needs to be removed and then to recover.
6. Resolution
   - The end of an incident, with this stage generally the same for all incidents, but may have some added material as some incidents have special or specific items of interests.

Note; the Prevention Stage has not been listed, as such steps should be done in a proactive manner to prevent the incident from occurring. When an incident does occur, the means of preventing it no longer applies.

Contents

Description

The Distributed Denial of Service (DDoS) IRP

This playbook is to be used for the purposes of modelling an effective incident response to the threat of DDoS attacks on your organization. This IRP will progress through the following processes:

1. Identifying the situation
2. Detection and Analysis
3. Containment
4. Eradication and Recovery
5. Resolution

How To Use This IRP

This IRP can be used either as a strict set of procedural steps (like a pre-flight checklist by pilots), as a flow chart, or as a reference guide. The classification of importance assigned to an IRP is determined by an organization's policies, management directives and/or analyst level of experience and judgement.

To use this IRP, first begin with the flowchart and identify the situation that best fits the incident.

Once identified, then refer to the step in the Detect and Analyse stage and proceed as follows. The steps in this stage will help to determine the particulars of the incident to then go to the correct means of containing the incident.

The Containment stage will aid in minimizing the impact of the incident and once done to then proceed to the next stage of Eradication and Recovery. Once the incident has been contained, then it will be removed and the impacted entity or entities (computers, network devices, users, etc.) can return to an operable state.

When the incident has been resolved, the Resolution reviews the details and response applied to the incident, and seeks to establish how an organisation can preclude a similar event from occurring in the future again.

Management Approval

Once a given stage has been completed, the analyst is recommended to notify the manager to proceed to the next stage - this will be specified within an organization's policies and plans. The assumption is that there is an Incident Response Team (IRT) already in place and will be notified when an incident has occurred.

If there is a conflict between an organization's policies and plans with the IRP, the organization's policies and plans take precedent. Thereafter, the IRP will need to be modified to be suited to the organization.

Other Information

DDoS attacks are intended to prevent a server or network resource from performing actions it is charged with providing. These attacks are divided into three types:

1) **Network (OSI model layers 3& 4) attacks**

   This clogs the access points connecting your network to the internet – involving the sending of huge amounts of traffic which overwhelm connection capacity until your systems become unavailable.

   Where SYN floods and DNS amplication methods of attack under this method have exceeded 200Gbps, the rise of these volumetric penetrations have been enabled by the growing availability of cloud infrastructure, the mass proliferation of IoT devices, and growth in network traffic capacities.

2) **Protocol attacks**

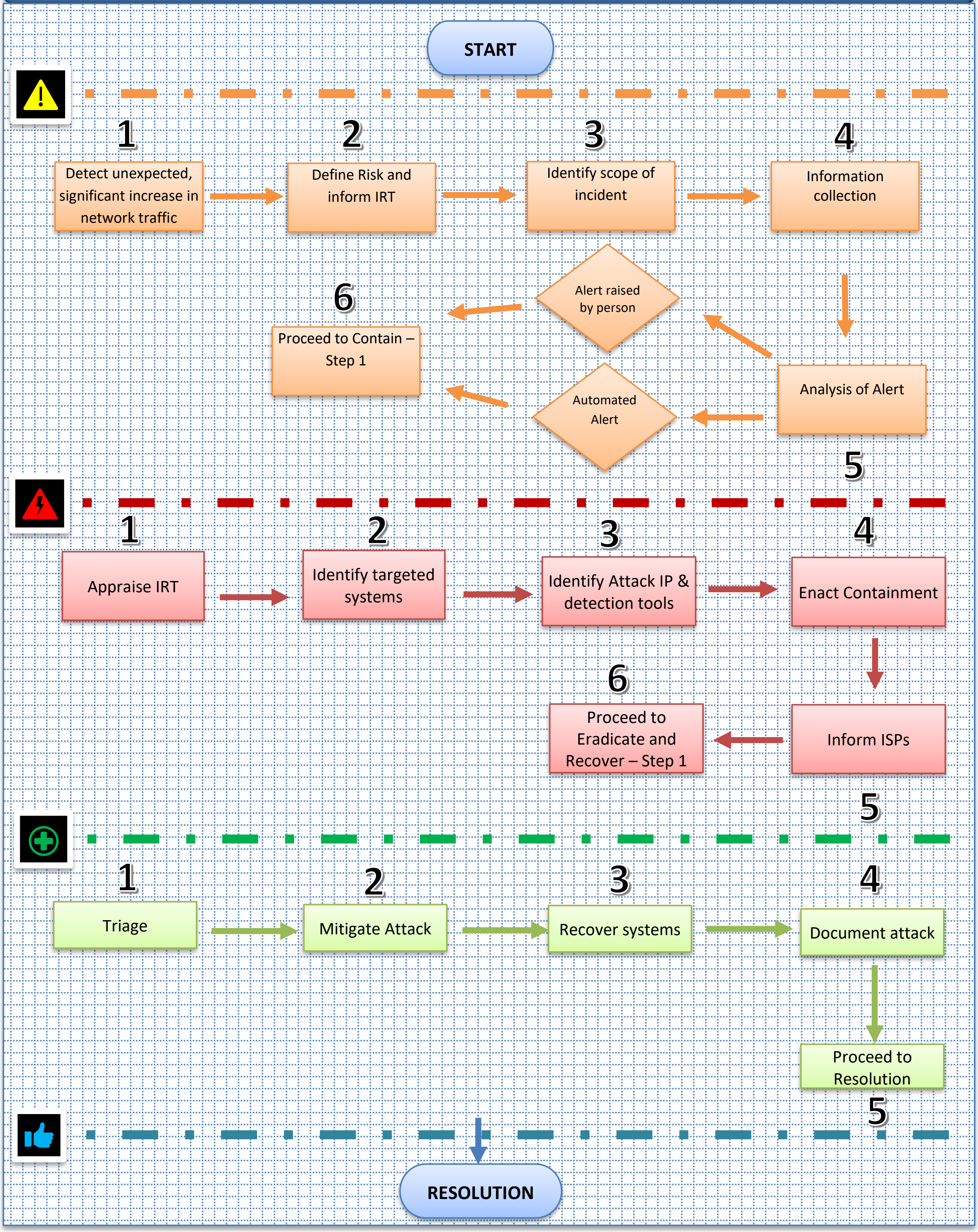
   Consume actual server resources – including firewalls and load balancers. Such is measured in packets per second (p/s).

3) **Application (OSI Model layer7) attacks**

   This seeks to overload resources upon which an application is running – resulting in its crash and the site being taken offline. Layer 7 penetrations can mimic legitimate user traffic, and can thus evade an organisation's common security measures.

Where over 80% of DDoS attacks employ multiple methods – creating smokescreens, bypassing protective solutions, and targeting multiple resources – these multi-vector assaults can prove overbearing for the majority of commercial networks.

Flow Chart


START
1
Detect unexpected, significant increase in network traffic
2
Define Risk and inform IRT
3
Identify scope of incident
4
Information collection
Analysis of Alert
5
Alert raised by person
Automated Alert
6
Proceed to Contain – Step 1
1
Appraise IRT
2
Identify targeted systems
3
Identify Attack IP & detection tools
4
Enact Containment
Inform ISPs
5
6
Proceed to Eradicate and Recover – Step 1
1
Triage
2
Mitigate Attack
3
Recover systems
4
Document attack
Proceed to Resolution
5
RESOLUTION

Detection and Analyse

DDoS based anomalies can be of a variety of reasons and can have some of the following symptoms:

- Slow access to files, either locally or remotely
- A long-term inability to access a particular website
- Internet disconnection
- Problems accessing all websites
- Excessive amount of spam emails

The Detection and Analysis stages seeks to verify the occurrence of an active DDoS attack on IT infrastructure, clarify the target of the attack, and identify

STEP	PROCEDURE
1	Detect an overflow of network servers.
2	Define Risk - Inform the Security Manager to gather the Incident Response Team (IRT), and brief them concerning the actions that will be needed to deal with this incident.
3	Identify scope - Determine if alert affects more than just the person(s)/node(s) that sent the alert. Attempt to connect to affected asset via a web-browser on the external interface . Perform DNS lookup to determine which IP address the DNS is pointing to a) Establish that DNS is responding and pointing to correct host b) Make sure DNS of all nodes agree with and respond to correct IP
4	Information collection - Verify that domain has not expired, and collect timestamps and monitor duration of attack event.
5	Analysis - Identify whether alert raised by person or automated system: a) If by person, identify: ❖ Where the user is connecting from? ❖ Which web servers were they connected to? ❖ What DNS servers are they using? ❖ What browsers were used? ❖ Does user have connectivity to other websites? b) If automated, identify which node(s) have identified the issued by ISP and IP
6	Proceed to **Contain Step 1** when authorized by the IRT or Security Manager

Contain

This Containment stage is employed to mitigate the effects of an ongoing DDoS attack, and eliminate the possibility of further damage to the victim's online services and IT infrastructure.

The incident response team is responsible for limiting the impact of the attack by implementing a quick-fix solution to minimize incident damage.

STEP	PROCEDURE
1	Appraise the IRT of the information and situation
2	Identify targeted systems: a) Identify systems which have suffered outages or reduction in services. b) Identify affected IT services c) Identify systems at risk from further DDoS attacks
3	Identify responsible IP addresses behind the attack, and tools used to detect attack.
4	Enact containment procedures: a) Filter incoming traffic by blocking IP addresses identified as sending throttle traffic at perimeter router-firewall b) Allow/prioritize only whitelisted IPs c) Service Hardening and avoiding the default configuration
5	Inform ISPs to block the suspicious range of IP addresses and multiple connection requests for the same resource
6	Proceed to **Eradicate and Recover Step 1** when authorized by the IRT or Security Manager.

Eradicate and Recover

Following the incident, the incident response team must determine how to eliminate the problem – requiring the implementation of various measures, and evaluation of the effectiveness of such measures.

During the recovery period, the incident response team tracks its incident response, summarises the content of the incident for future record, and reflects upon its strategies in responding to similar incidents in the future.

STEP	PROCEDURE
1	Triage and confirm incident report: a) Request system patch b) Request network segment c) Change affected systems/networks
2	Mitigate attack and remove vulnerabilities: a) Block DDoS traffic as close to the network's cloud as possible via router/firewall b) Terminate unwanted connections c) Add servers or network bandwidth to handle the DDoS load d) Clearing network backlog – temporarily disable bottleneck features
3	Recover systems and resume normal operations: a) Load backup servers b) Running antivirus c) Replace malfunctioning physical hardware and systems. d) Blacklist IPs behind the attack
4	Document the attack for delivery to authorities: a) Raw-write data from relevant logs if intended for forensics b) Document all steps taken, all individuals, IP addresses involved, and which times all steps were taken. Note the event in the security log and continue to monitor for 24 hours.
5	Proceed to **Resolution Step 1**.

Resolution

With the incident resolved, the process of learning and improving upon the incide An IRT collaborative discussion will be conducted about this incident with the foll objectives:

- Lessons Learned
- Evidence Retention
- Proposal of new or modification changes

Lessons Learned

The Lessons Learned is a review process of the incident by all team members. From the analyst's point of view, this will be of how the incident was detected, contained and mitigated. Some items that may be addressed:

- Were there any problems that were encountered during the incident?
- Were there any conflicts with existing policies?
- What could be improved upon to reduce the time of the incident?

Evidence Retention

The discussion with the IRT will determine of what is evidence is required and of how to retain them. This would be already addressed by the organization's policies, but if not, then this is the time to develop such a policy.

Proposal of Changes

From the discussion there should be of some new or modification changes of policies, procedures, directives rules and even of safeguards. These proposed changes may also help aid in future incidents.