



DDOS

Méthodologie de réponse à incident

IRM-03 08/09/2023



Introduction

Cette méthodologie de réponse à incident est une feuille de route dédiée aux gestionnaires et aux cellules de crise menant une investigation sur un problème de sécurité précis.

- La fiche IRM s'adresse aux personnes ou fonctions suivantes :
 - Les RSSI et leurs adjoints
 - Les DSI et leurs adjoints
 - Les administrateurs

Rester calme et contacter immédiatement l'équipe de réponse à incident Cyna.
Nos canaux de discussion :

- Cybersecurity@cyna-it.fr
- +33 9 70 70 41 81 (Heure ouvrés)

En cas d'urgence, veuillez insérer la balise [URGENT] dans l'objet du courriel. Veuillez noter que notre CERT est disponible 24 heures sur 24 et 7 jours sur 7, mais que l'assistance téléphonique n'est pas disponible en dehors des heures de bureau.

Identification & Processus d'endiguement

Objectif : Détecter l'incident, déterminer son ampleur et impliquer les acteurs appropriés.

1.1. Détection d'un DDOS

Comment détecter une attaque par dénis de service distribué (DDOS)

1. Accès au service limité :

- **Latence excessive :**
 1. Si le service que vous essayez d'utiliser met trop de temps à répondre.
- **Service indisponible :**
 1. Si le service que vous essayez d'utiliser ne réponds pas.

2. Traffic inhabituel :

- Augmentation anormale du nombre de requêtes.

3. Messages d'erreur (serveur web) :

- Des messages d'erreur tels que "504 Gateway Timeout" ou "503 Service Unavailable".

Préparer les investigations

Dans cette section nous verrons toutes les données qui sont à récupérer pour préparer les investigations des équipes CYNA.

Logs

Dans un premier temps, il faut récupérer les logs des machines qui ont été exposées à l'attaque. Cela comprend les machines/serveurs cibles mais également les serveurs proxy/reverse proxy et firewall qui ont transmettre les premières requêtes de l'attaque.