Traitement d'incidents de type Déni de service distribué (DDoS)

Date du document : 12 décembre 2017
Version du document : 1.0

24, rue du Gabian
98000 MONACO
Tel. : (+377) 98 98 24 93
amsn@gouv.mc

Département de l'Intérieur

Sommaire

1- Préparation

Pour être à même de faire face à un incident de type déni de service distribué, le jour où il survient, l'AMSN recommande de prendre connaissance de la note suivante, qui définit les bonnes pratiques en matière de traitement de DDoS :

- https://www.cert.ssi.gouv.fr/information/CERTA-2012-INF-001/

Une bonne connaissance préalable, par les équipes techniques, de la méthodologie à suivre, permet un traitement plus efficace de l'incident.

2- Actions à diligenter durant l'incident

Afin de pouvoir caractériser au mieux les incidents de type déni de service distribué, l'Agence Monégasque de Sécurité Numérique préconise que soient effectuées les actions suivantes :

- **Noter précisément le type d'attaque DDoS:**
  - Inondation par envoi en grand nombre de paquets SYN (SYN flood) ;
  - UDP par rebond sur une adresse de type broadcast ;
  - Déni de service volumétrique par saturation de bande passante ;
  - DDoS par amplification (DNS, SSDP, NTP…) ;
  - …

- **Si l'attaque semble atypique (ex : attaque applicative), enregistrer des échantillons du trafic reçu et les conserver :**
  - pendant une durée de quelques secondes/minutes selon le débit ;
  - sous forme de fichier PCAP ;
  - Ces fichiers pourront être utiles à l'AMSN ou, le cas échéant, aux autorités judiciaires si elles sont sollicitées ultérieurement, afin de donner des suites au traitement de l'incident.

- **Etablir la liste des impacts relevés sur le système d'information :**
  - durée de l'indisponibilité éventuelle ;
  - effets de bord générés par l'attaque;

- **Noter la durée et le nombre de vagues d'attaque** :
  - Nombre d'itérations ;
  - Durée totale de l'attaque ;
  - Durée de chaque type d'attaque ;

- **Déterminer la volumétrie constatée** :
  - Type de trafic enregistré dans les différentes phases de l'attaque (bps et pps)

- **Déterminer les sources de l'attaque :**
  - Dans la mesure du possible et en fonction des types d'attaque (TCP/UDP), les adresses IP d'origine ou a minima une estimation du nombre d'adresses ;
  - Si possible, les indicatifs de routage internet des opérateurs sources (ASN) ;

- **Prendre note de la cible de l'attaque :**
  - Systèmes visés ;
  - Ports de destination sur ces systèmes ;

- **S'il est déterminé, noter l'objectif supposé de l'attaque ainsi que les manœuvres de dissimulation ayant pu être utilisées par les attaquants**
  - Le DDoS a-t' il servi « *d'écran de fumée* » pour masquer une attaque plus ciblée ?
  - Des dysfonctionnements de services, apparemment sans rapport, ont-ils été constatés pendant ou après l'attaque ?

- **Conserver les revendications éventuelles :**
  - Par messages électroniques (menaces proférées, rançon réclamée, attaque revendiquée) ;
  - Par enregistrement des publications en ligne relatives à l'attaque (twitter …) ;

- **Noter les mesures prises :**
  - contre-mesures prises en réaction à l'attaque ;

- **Communiquer les éléments complémentaires**
  - L'attaquant semble-t-il avoir surveillé l'efficacité de son DDoS ?
  - Des éléments précurseurs ont-ils été enregistrés par l'opérateur avant que cette attaque se produise ?
  - Retour d'expérience éventuel.

Les récentes vagues hacktivistes et l'arrivée, en parallèle, d'outils automatisés accessibles à tous, ont permis la démocratisation de certaines de ces attaques que tous les acteurs de la sécurité des systèmes d'information doivent anticiper.

L'ensemble de ces informations collectées doit être adressé à l'AMSN, il permet ainsi au CSIRT-MC d'estimer les évolutions éventuelles des capacités et méthodes d'attaque de chaque mouvance, permettant indirectement d'adapter les guides et recommandations afin de s'en protéger au mieux.

3- Suites à donner à l'incident

L'Agence Monégasque de Sécurité Numérique préconise une prise de contact avec un investigateur en cybercriminalité de la Direction de la Sureté Publique.

Celui-ci pourra recueillir un dépôt de plainte, qui constitue un prérequis à la mise en œuvre d'actions de coopération policière et judiciaire, au niveau international.

Les éléments recueillis (cf paragraphe 2-) seront fournis lors du dépôt de plainte afin de matérialiser au mieux l'infraction et d'étoffer la description des faits constatés.