Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Unité de pilotage informatique de la Confédération UPIC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI
GovCERT.ch

Mesures à prendre contre les attaques DDoS

MELANI / GovCERT.ch

Version:	v1.00
Auteur:	MELANI / GovCERT.ch

[1] http://creativecommons.org/licenses/by-nd/3.0/

Introduction

Le terme DDoS (Distributed Denial of Service = déni de service distribué) désigne une attaque destinée à rendre inaccessibles des systèmes informatiques. Les dommages économiques peuvent être graves pour la victime. A la différence d'une simple attaque DoS, un grand nombre d'ordinateurs disséminés à différents endroits opèrent simultanément. Une attaque DDoS peut être menée au niveau du réseau ou des applications, ou combiner les deux approches. Elle fait généralement appel à des réseaux de zombies (grand nombre de systèmes infectés et contrôlés à distance par l'agresseur) ou à des systèmes tiers mal configurés (p.ex. des résolveurs DNS ouverts) qui, suite à des requêtes falsifiées leur étant adressées, vont rediriger des réponses volumineuses vers la cible de l'attaque (attaque par amplification). Le volume du trafic ainsi généré atteint fréquemment plusieurs centaines de gigabits par seconde. Une seule organisation n'est généralement pas en mesure d'absorber un tel trafic sans aide extérieure. Quant aux pare-feu et aux dispositifs de prévention des intrusions (IPS, intrusion prevention system) spécialement configurés, ils n'ont qu'une utilité limitée en pareil cas.
En règle générale, les attaques DDoS relèvent de l'activisme politique, constituent une arme de chantage ou visent à nuire à un concurrent. MELANI observe à l'heure actuelle une recrudescence d'attaques DDoS avec demande de rançon en crypto-monnaies, telles que Bitcoin ou Litecoin.

Aucune organisation n'est à l'abri des attaques DDoS!

Mesures préventives

Idéalement, la problématique DDoS vous est familière et vous avez déjà atteint un certain niveau de préparation à ce genre d'attaques.

- Vous connaissez votre infrastructure et ses points faibles. Il vous faut déterminer les services dont l'importance est telle qu'une défaillance aurait de graves conséquences pour toute votre organisation. Pensez également aux systèmes de base sans lesquels vos applications critiques ne fonctionneraient pas.
- Vous connaissez la «situation normale» de vos réseaux et systèmes et savez identifier les anomalies (système de détection des intrusions [IDS, intrusion detection system], gestion centralisée des journaux d'événements). Il importe de découvrir une attaque DDoS avant que vos clients ne s'en aperçoivent.
- Contrôlez aussi la disponibilité de vos applications dans l'optique de votre clientèle, autrement dit à partir d'Internet.
- Vos systèmes doivent être durcis (absence de services inutiles, gestion stricte des droits, authentification forte, etc.) et à jour au niveau des programmes correctifs. Les SYN-cookies sont activés, etc.
- Un pare-feu en amont n'autorisera que les protocoles nécessaires au système. Il disposera de ressources système suffisantes pour rester opérationnel même en cas d'attaque DDoS. Il convient d'accorder une grande importance à la table de connexion ainsi qu'à une bonne gestion des règles, de façon à pouvoir adopter en cas d'urgence des règles de blocage supplémentaires.
- Examinez les possibilités d'un blocage basé sur la géolocalisation (GeoIP). Si vos clients viennent essentiellement de Suisse et des pays proches, vous pouvez prédéfinir un profil qui accorde la priorité aux adresses IP de ces pays, ou qui bloque d'autres adresses IP. En cas d'attaque, il vous suffira d'activer ce profil pour obtenir des possibilités d'action immédiates et bénéficier d'une protection accrue.
- Un pare-feu d'applications (Web application firewall, WAF) réduira les attaques dont pourraient faire l'objet les services Internet.

- Les systèmes exposés à une attaque DDoS (par ex. site Web) devraient emprunter une autre liaison montante Internet que les autres systèmes de l'organisation. Il sera ainsi plus facile de les placer sous la protection d'un fournisseur de services de mitigation DDoS, sans que les autres systèmes nécessaires à la gestion opérationnelle soient affectés.
- Prévoyez des solutions de rechange, à l'instar d'un site Web statique livrant un minimum d'informations et confié à un autre fournisseur d'hébergement, que vous pourrez activer par simple modification du DNS.
- Veillez en général à définir pour les serveurs DNS une durée de vie (TTL) adéquate, qui vous permette une migration suffisamment rapide de DNS.
- Vous disposerez d'une stratégie de défense en cas d'attaque DDoS. Les personnes doivent connaître la marche à suivre et les contacts tant internes qu'externes (fournisseurs de services, services de police, etc.).
- Dans le pire des cas, vous pouvez recourir à des ressources internes ou alors externes garanties par contrat (personnel et infrastructure notamment).
- Vous avez discuté et exercé aussi le scénario d'une attaque DDoS avec vos services internes et vos partenaires externes. Chacun connaît son rôle et ses interlocuteurs!

Mesures à prendre en cas d'attaque

En cas d'attaque DDoS, il importe en priorité de faire comprendre à l'agresseur qu'il n'a pas atteint son objectif. Si vous résistez suffisamment longtemps, il abandonnera vraisemblablement.

1. Consignez l'attaque (flux Netflow, fichiers journaux des serveurs, échange de correspondance avec les maîtres-chanteurs, etc.). Ces informations sont précieuses pour une analyse ultérieure et pour une éventuelle plainte.
2. Veillez à disposer de canaux donnant des informations de base au monde extérieur, par exemple site Web statique vous permettant d'informer vos clients et de leur offrir d'autres possibilités de contact (par ex. téléphone, télécopie, courriel).
3. Analysez l'attaque et définissez une stratégie de défense:

    a. Si l'attaque provient d'un nombre limité d'adresses IP, il suffira le cas échéant de filtrer ces adresses à l'aide d'un routeur ou pare-feu. Si le volume du trafic dépasse la bande passante à votre disposition, votre fournisseur de services Internet devra s'en charger.
    b. Déplacez le cas échéant votre système attaqué dans un autre sous-réseau (en cas d'agression uniquement basée sur IP). Il convient ici de rechercher une solution en étroite collaboration avec votre fournisseur de services Internet ou un fournisseur de services de mitigation DDoS.
    c. Il peut s'agir d'une attaque où les adresses IP source sont falsifiées: cela vaut notamment en cas d'attaque par saturation (flooding) SYN, UDP, BGP ou SNMP. Un filtrage des adresses IP n'aurait aucun sens ici et aboutirait même à exclure des utilisateurs légitimes. Il est indiqué de rechercher une solution avec votre fournisseur de services. Il pourra dévier ou filtrer ce trafic. Mais vous devriez déjà savoir quels sont vos protocoles en activité et lesquels pourraient être filtrés sans dommages. Les présences publiques sur le Web s'en tiennent généralement aux protocoles basés sur TCP (HTTP, HTTPS, SMTP, etc.), ce qui fait qu'on peut filtrer sans hésiter les protocoles sans état comme UDP (exception éventuelle: DNS).
    d. Attaques contre une application:
    De nombreuses requêtes (complexes) paralysent votre application. Les attaques utilisent en règle générale TCP comme protocole réseau. D'où la difficulté de falsifier l'adresse de l'expéditeur, qui pourra être filtrée à l'aide de divers critères.

e. Attaques contre le protocole SSL/TLS: il peut être utile de planifier une liaison SSL auprès d'un service en nuage (cloud), qui transmettra par la suite la liaison filtrée à vos systèmes.
f. Si la majeure partie de votre clientèle se trouve dans des pays bien précis, la géolocalisation par adresse IP (GeoIP) permet de la filtrer ou de la classer par ordre de priorité. Le service restera ainsi plus longtemps accessible, même si peut-être l'un ou l'autre des utilisateurs légitimes sont ignorés ou obtiennent un faible niveau de priorité.

4. Attendez-vous à ce que l'agresseur cherche à trouver une parade à vos mesures de défense et recoure à de nouvelles tactiques. Le cas échéant, analysez sa nouvelle attaque DDoS et prenez les mesures qui s'imposent.
5. Signalez l'incident à MELANI et portez plainte auprès des autorités de police compétentes pour (tentative de) détérioration de données (Art. 144bis CP) et le cas échéant pour (tentative d') extorsion et chantage (Art. 156 CP). Une détérioration de données existe également lorsque des données sont, en raison d'une attaque, rendues indisponibles pendant une certaine période et sont en ce sens inutilisables.
6. MELANI déconseille fortement d'entrer en matière sur les exigences des maîtres chanteurs.

Vos contacts avec MELANI

www.melani.admin.ch