Agence Nationale de la Sécurité des Systèmes d'Information
Centre Opérationnel de la SSI

Fiche d'information sur les annonces d'attaques de sites institutionnels du 15 janvier 2015

Date de création : 13/01/2015

Depuis le 7 janvier 2015, plusieurs annonces ont été publiées par des groupes d'attaquants appelant à défigurer ou rendre indisponibles des sites institutionnels français. Ces opérations sont regroupées sous le nom « OpFrance ».

La présente fiche vise à rappeler quelques éléments nécessaires à la protection des sites ciblés ainsi que certaines mesures à appliquer en cas d'attaque avérée. Dans tous les cas, il convient de remonter les tentatives avérées ou les attaques réussies, à la chaîne SSI.

A. Recommandations relatives à la protection des sites contre les défigurations

1. PREPARATION

Plusieurs éléments sont à vérifier afin de limiter au maximum la défiguration d'un site. Les vecteurs les plus courants sont :

- le défaut de sécurisation d'accès à une interface de gestion du site ;
- l'utilisation d'un mot de passe faible pour l'administration du site ;
- l'utilisation d'un gestionnaire de contenu (*CMS*) non maintenu ou dont les derniers correctifs de sécurité n'ont pas été appliqués ;
- l'utilisation d'une brique logicielle non maintenue ou dont les derniers correctifs de sécurité n'ont pas été appliqués.

Il est important de veiller à ce que ces éléments soient vérifiés et corrigés si nécessaire. Pour cela, il est possible de s'appuyer sur le guide de sécurisation des sites Web :
http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-applications-web/recommandations-pour-la-securisation-des-sites-web.html

La granularité des évènements journalisés liés aux services exposés et aux équipements réseaux doit être augmentée. Ces journaux serviront à analyser le type de trafic et les requêtes illégitimes utilisés lors d'une éventuelle attaque. Ils doivent être conservés en cas de dépôt de plainte.

Enfin, la réalisation de sauvegardes régulières permettra, en plus de restaurer le contenu du site, de détecter un ajout ou une modification illégitime d'un fichier.

2. REACTION

En vue d'effectuer un dépôt de plainte, il est nécessaire de collecter l'ensemble des éléments techniques décrivant l'attaque (journaux, captures réseaux, copie de disques, etc.), et de garder une trace des échanges effectués avec des tiers pendant le traitement de l'incident.

Il est important de garder à l'esprit qu'un site ayant été compromis contient a minima une vulnérabilité qui doit être identifiée et corrigée. L'ensemble des actions ayant pu être réalisées par les attaquants doit être analysé. En aucun cas la restauration d'une sauvegarde ou la suppression de l'élément ajouté/modifié ne pourra être considérée comme étant une réponse adaptée.

Enfin, en cas d'hébergement d'un site sur un serveur mutualisé, il est important de veiller à ce que l'intégrité du serveur et des autres sites soit vérifiée.

En cas d'attaque, il convient de se reporter à la note d'information sur les défigurations de sites Web :
http://www.cert.ssi.gouv.fr/site/CERTA-2012-INF-002/index.html

B. Recommandations relatives à la protection des sites contre les attaques en déni de service

1. PREPARATION

1.1 Organisationnelle

Pour faire face à une attaque par déni de service, il est primordial de recenser les systèmes susceptibles d'être visés, et de connaître les équipes responsables de l'administration de ces systèmes. En outre, afin de favoriser un traitement rapide de

l'attaque, il est impératif de disposer des contacts appropriés en interne, ainsi que chez les opérateurs de transit, ou encore auprès de l'éventuel fournisseur d'un service de protection contre les attaques DDoS.

En dehors des solutions de protection spécifiques abordées ci-après, de bonnes pratiques peuvent contribuer à améliorer la résistance à une attaque par déni de service. Parmi celles-ci, on peut notamment citer :

- la segmentation du réseau de l'entité de manière à faciliter le filtrage en cas d'attaque, et l'isolement éventuel de certains sous-réseaux ou de certains serveurs ;
- la réduction de la surface d'attaque possible en autorisant seulement les flux nécessaires en entrée comme en sortie du réseau.

1.2 Équipements commerciaux spécifiques administrés par l'entité

Des protections spécifiques contre les attaques en déni de service distribué peuvent également être mises en place. Certains produits commerciaux sont spécialisés dans le filtrage de trafic. Ils se basent sur des listes blanches ou noires, la position géographique des sources ou des filtres sur les paquets transmis.

Leur mise en œuvre nécessite une prise en main préalable, et un paramétrage adapté au trafic de l'entité. De plus l'achat et le maintien à jour de ces équipements peuvent être onéreux et nécessiter des modifications dans le schéma du réseau de l'entité.

1.3 Services proposés par les opérateurs de transit et les hébergeurs

Si le déni de service sature le lien réseau et non pas des services applicatifs, l'intervention de l'opérateur de transit est parfois nécessaire. Celui-ci peut offrir un service de filtrage de trafic. Dans le cas où ce service est opéré par le client, ce dernier doit s'assurer de maîtriser la configuration des différentes contre-mesures offertes par la plate-forme.

Les hébergeurs offrent parfois une protection contre les attaques de ce type. Les différentes options proposées peuvent constituer une solution pour les structures faisant appel à une société externe pour l'hébergement de leurs services, par exemple :

- le recours à un Content Delivery Network (CDN), qui permettra de répartir les ressources sur un grand nombre de serveurs et améliorera la résistance aux attaques en déni de service distribué ;
- le recours à des services commerciaux de protection dédiés contre les attaques par déni de service distribué.

Il est recommandé de se rapprocher des différents prestataires en trafic et en hébergement afin de connaître les services éventuellement proposés, ainsi que les contacts à activer en cas d'attaque.

2. REACTION

2.1 Identifier le trafic illégitime

Avant de mettre en œuvre une contre-mesure, il est important d'identifier :

- l'élément défaillant : liens réseau, surcharge d'un serveur ou d'une application, etc. ;
- le ou les protocole(s) utilisé(s). En effet le protocole de transport UDP ne permet pas d'identifier les sources d'une attaque (possibilité d'usurpation de l'adresse IP source) ;
- les sources de l'attaque : nombre de sources, opérateur de provenance, etc. ;
- un ou plusieurs discriminants permettant de distinguer le trafic légitime du trafic généré par l'attaque, comme des motifs récurrents dans le contenu des paquets, des valeurs remarquables dans les en-têtes HTTP, etc.

2.2 Contre-mesures

Une fois les caractéristiques de l'attaque identifiées, plusieurs actions peuvent être décidées. Par exemple, si la bande passante des liens réseau fournis par les opérateurs est saturée, ceux-ci doivent être contactés afin de filtrer le trafic. Par ailleurs, l'entité peut mettre en œuvre le service de protection éventuel dont elle peut bénéficier si celui-ci n'est pas actif.

En outre, un certain nombre de dispositions peuvent être prises au niveau de l'entité ciblée. Parmi celles-ci, on peut notamment citer :

- le blocage des adresses IP sources identifiées comme étant à l'origine de l'attaque ;
- le blocage de certaines classes de trafic impliquées dans l'attaque, et non nécessaires au bon fonctionnement de l'entité (filtrage sur le port destination, ou de protocoles par exemple) ;
- la limitation du nombre de connexions concurrentes, ou sur une période de temps limitée, par adresse IP source au niveau d'un pare-feu ;
- la réduction des délais de garde des connexions TCP (par exemple sur des serveurs Web ou SMTP) ;
- le blocage du trafic à destination des cibles, en fonction de l'impact de l'attaque sur le reste de l'infrastructure réseau ;
- le changement d'un site Web dynamique en site statique si l'élément défaillant est une application Web.

Enfin, en vue d'effectuer un dépôt de plainte, il est nécessaire de collecter l'ensemble des éléments techniques décrivant l'attaque (journaux, captures réseaux), et de garder une trace des échanges effectués avec des tiers pendant le traitement de l'incident.

Note d'information sur les dénis de service :
http://www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001/index.html