INTRODUCTION

Le DNS pour Domain Name System est un système qui permet de faire la correspondance entre une adresse IP et un site internet commewww.google.com. En effet, tout équipement sur le réseau IP est identifié par une adresse IP et c’est le serveur DNS qui gère la correspondance avec ces adresses IP et les noms que nous saisissons sur nos navigateurs. Sans cela, l’utilisateur ne pourra jamais accéder au site, d’où sa nécessité.

Le DNS est donc un service qui est indispensable au bon fonctionnement de l’Internet. Mais, comme tout serveur Web, il est exposé à de multiples attaques. Ce qui le rend très vulnérable. Ces attaques peuvent être très graves selon les circonstances et les intentions du pirate. A titre d’exemple, ...

Toutefois de nombreux mécanismes sont mis en place pour faire face à sa vulnérabilité. Parmi ceux-ci, nous avons le DNSSEC pour Domain Name Server Security Extensions. Comme son nom l’indique, il s’agit du serveur DNS avec une touche de sécurité en plus basée sur un principe de chiffrement et rendant le DNS plus robuste aux attaques.

Le DNS et le DNSSEC

1. C’est quoi le DNS ?
2. Utilité

Tous les équipements reliés à Internet ont une adresse IP qui les identifie sur le réseau IP. C’est L’ICANN\* qui gère ces identifiants et s’assure qu’ils soient uniques sur tout le réseau. Toutefois, il est presqu’impossible pour l’humain de retenir toutes ces adresses. Une correspondance entre chaque adresse avec un nom est donc mise en place à travers le système DNS. Il est plus facile pour l’humain de retenir un nom comme [www.googgle.com](http://www.googgle.com) que son adresse IP correspondante 8.8.8.8. A noter que pour les adresses IPv6, les adresses sont plus longues car représentées sous la forme « xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx » et sont encore plus difficiles à retenir. Ainsi, lorsqu’un nom est saisi, le serveur DNS utilise sa table DNS pour traduire le nom en son adresse IP correspondante. Le DNS n’est en effet rien d’autre qu’un annuaire ; il fonctionne par exemple comme un annuaire téléphonique. Nous retenons les noms de nos correspondants mais pas forcément leurs numéros de téléphone. La mise en place de serveurs DNS est donc indispensable au fonctionnement Internet d’où toute son utilité.

1. Architecture

Le DNS, comme expliqué précédemment traduit un nom dit nom de domaine dans le jargon DNS en une adresse IP. On parle de résolution DNS. Le DNS présente une architecture arborescente. Un nom de domaine est composé de plusieurs parties séparées par un point ; chaque partie correspond à un niveau dans l’arbre DNS. Nous avons un ‘’.’’ qui représente la racine et qui est rajouté par le serveur avant de faire la résolution. C’est la raison pour laquelle il n’est pas obligatoire de le mettre sur le navigateur. Puis nous retrouvons, le premier …..<https://openclassrooms.com/courses/apprenez-le-fonctionnement-des-reseaux-tcp-ip/le-service-dns> Comme nous pouvons le voir sur le schéma ci –dessous.

Nous pouvons par ailleurs remarquer que l’architecture du DNS présente un arbre inversé. En effet, cela permet de mettre en place plusieurs hôtes et de pouvoir passer par un autre si l’un d’eux ne fonctionnerait plus. Cela permet donc de rendre plus robuste le système DNS.

1. Fonctionnement

Pour traduire les noms de domaine en adresse IP, le DNS fait de la résolution qui est résumée sur le schéma ci-dessous.

Lorsque l’utilisateur saisit un FQDN sur la barre de recherche de son navigateur, le résolveur\* vérifie qu’il n’a pas l’adresse IP correspondante stockée dans son cache. Si oui, il renvoie l’adresse IP au client qui pourra accéder au site. Sinon, le résolveur interroge chaque niveau du FQDN en respectant la structure arborescente du DNS. Il commence à interroger la racine pour avoir le serveur qui sauvegarde toutes les informations qui concernent la zone \*\*, on dit que le serveur fait autorité sur cette zone.

Ensuite, il descend dans l’arborescence jusqu’à obtenir l’adresse IP correspondant au FQDN saisi par le client. A noter qu’à chaque étape de la résolution, le résolveur stocke les informations dans sa mémoire cache. Pour les prochaines requêtes, le DNS n’aura donc plus à faire les mêmes résolutions pour une durée TTL qui est le temps au bout duquel l’enregistrement dans le cache expire.

1. Vulnérabilités du DNS

Le serveur DNS est incontournable pour le fonctionnement de l’Internet ; ce qui fait de lui une cible idéale pour les cybercriminels. On admet aujourd’hui que le service DNS est l’un des services les plus critiques pour une entreprise. Il est en effet exposé à de multiples attaques. Parmi celles-ci, nous avons le cache poisoning et le \*\*\* que nous allons voir respectivement ci-dessous :

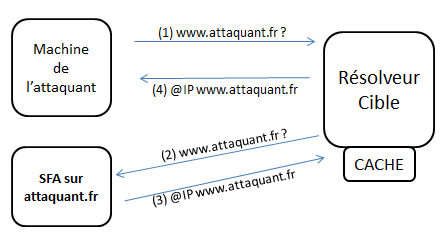
1. Cache poisoning

Le cache poisoning est l’une des attaques les plus fréquentes qui touchent le DNS. Comme son nom l’indique, cette attaque vise à empoisonner le cache où des enregistrements sont stockés pour une durée TTL. Cela permet d’améliorer les performances telles que la consommation de bande passante, la charge du serveur, la rapidité de consultation lors de l’utilisation d’un navigateur.

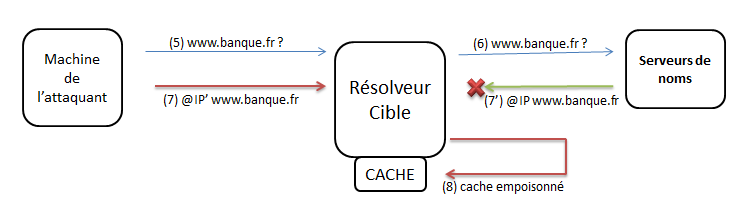
La finalité de l’empoisonnement DNS est d’acheminer les utilisateurs vers un site Web frauduleux. Par exemple, un utilisateur tape « gmail.com » dans un navigateur Web avec pour objectif d’aller consulter sa boîte email. Le DNS ayant été empoisonné, ce n’est pas la page gmail.com qui s’affiche mais une page frauduleuse choisie par l’attaquant, dans le but par exemple de récupérer les accès aux boîtes emails. Les utilisateurs saisissant le nom de domaine correct, ne se rendent pas compte que le site Web qu’ils visitent n’est pas authentique.

Cela permet aux attaquants de récupérer des informations confidentielles comme les informations d’identification à un site ou relatives à sa carte bancaire. L’attaque peut être dévastatrice, en fonction de plusieurs facteurs, selon l’intention de l’attaquant et la portée de l’empoisonnement DNS.

Comment les pirates mènent-ils cette attaque ? Pour se faire, l’attaquant commence par interroger le résolveur ciblé en faisant une requête sur un FQDN, n’importe lequel. Le résolveur va faire la résolution en interrogeant les serveurs faisant autorité. Il obtient ainsi une réponse qui est l’adresse IP correspondant au FQDN saisi par l’attaquant. Jusqu’ici rien d’anormal, nous retrouvons une résolution DNS classique. Mais l’attaquant par cette requête récupère l’ID\* présent sur la réponse DNS.

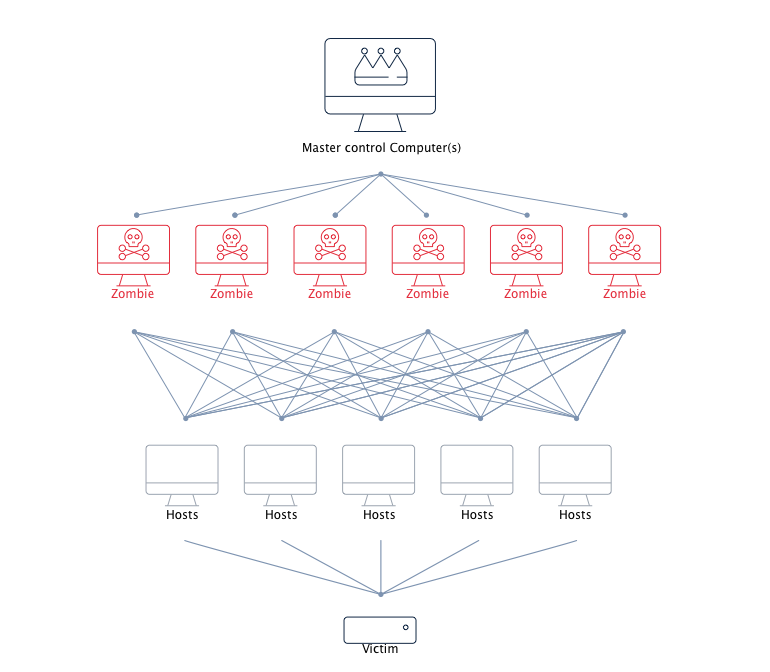


L’attaque se poursuit dans une deuxième partie. Où le pirate réinterroge le même résolveur pour accéder par exemple à un site de banque en ligne www.banque.fr. Le résolveur commence à faire sa résolution, mais pendant ce temps le pirate se fait passer pour le serveur faisant autorité sur banque.fr et envoie une adresse IP au résolveur sauf que celle-ci ne correspond pas au vrai site de ww.banque.fr mais à un autre site frauduleux qu’il gère. Normalement, le résolveur vérifie si l’ID sur la trame de réponse est identique à celui qui est sur la trame de requête qu’il a envoyé au serveur de noms. Toutefois, la première partie aura presque permis au pirate de trouver l’ID. En effet, il incrémente l’ID qu’il a récupéré précédemment jusqu’à trouver l’ID correspondant. Ainsi, il parvient à faire correspondre le site www.banque.fr avec une fausse adresse IP. Cette correspondance est mise dans le cache. Tous les autres utilisateurs qui interrogeront le résolveur pour accéder à ce site arriveront sur un site frauduleux ; le pirate peut récupérer pour ce cas-ci les informations de paiement de l’utilisateur. Le bon serveur de nom répondra quand même au résolveur mais sa réponse sera ignorée car un enregistrement dans le cache existe déjà.



1. DDOS ou Déni de service

L’attaque DDOS pour Distributed Deny Of Service vise à rendre le service DNS indisponible. Pour se faire, le hacker utilise un botnet qui est un ensemble de machines infectées et contrôlées à distance par le pirate. Ce botnet peut contenir des centaines voire des milliers de machines. Le pirate utilise cet important réseau d’ordinateurs pour faire multiples requêtes sur des noms de domaines inexistants. Il vise ainsi à faire tomber le résolveur et/ou le serveur faisant autorité sur la zone visée. En effet, ces derniers vont essayer de résoudre les requêtes DNS en vain, les FQDN étant inexistants. Ainsi, ils feront face à une saturation de la bande passante, un épuisement des ressources système de la machine les empêchant ainsi de réponde au trafic légitime.



1. L’apport de DNSSEC

En vue de toutes les attaques auxquelles DNS doit faire face, il devient nécessaire de s’assurer de l’intégrité des données et d’authentifier les résolveurs et les serveurs faisant autorité. Il faut donc assurer la sécurité d’accès aux ressources à tous les utilisateurs (3 milliards environ) avec une solution assez légère pour ne pas surcharger les serveurs de noms ou augmenter considérablement la taille des paquets DNS.

Pour répondre à ce besoin de sécurité du DNS, il existe depuis 2005 une méthode normalisée pour sécuriser le DNS contre les tromperies. Cette méthode consiste en une signature cryptographique des données du DNS.

Principe du DNSSEC

Le DNS repose sur des principes simples.

Le premier est le fait qu’il n’est pas une modification du protocole DNS ; c’est en effet une extension du DNS, pas un nouveau protocole. De ce fait, un client qui n’est pas configuré pour faire ses requêtes avec DNSSEC peut interagir avec un DNSSEC et réciproquement.

Le second principe est l’utilisation de la cryptographie pour signer les zones DNS et garantir l’authenticité de l’origine du message. Le fonctionnement de cette cryptographie est assez complexe et requiert une base solide en sécurité. Nous allons donc exposer dans cette partie le fonctionnement de cryptographie sans trop donner de détails et faciliter ainsi la compréhension.

Ainsi ce schéma nous montre que la cryptographie utilisée par DNSSEC est asymétrique. Car nous utilisons deux clés : une privée connue seulement par le propritaire et une autre publique qui peut être connue de tous. Ainsi, pour vérifier la véracité de l’origine des messages, le seerveur fasant autorité sur wikipédia.fr chiifre l’adresse IP correspondant au nom de domaine avec sa clé privéeet obtient donc une signature numérique de la donnée qu’il va transmetre au résolveur. Il envoie en même temps le message chiffré et non chiffré ainsi que sa clé publique qui est la seule à pouvoir déchiffrer le message. Le résolveur donc reçoit les deux messages avec la clé publique associée. Il déchhifre le message chiffré et le compare au message DNS non chiffré. S’il retrouve le meême message, alors l’authenticité est vérifiée, il pourra stocké ml’enregistrement dans son cache et le transmettre aux utilisateurs sans danger. Le DNSSEC permet aisi de résoudre un problème très fréquemment rencontré par le DNS qui est le cache posoning ou l’empoisonnement du cache vu précédemment.

