Thomas Lépine – 5A SAGI (VA Cybersécurité)

Veille technologique : DNS Poisoning

- **Qu'est-ce qu'un serveur DNS ?**

Commençons par le commencement, qu'est-ce que le DNS (Domain Name Système) ? Le système de noms de domaines est le service informatique utilisé pour traduire un nom de domaine (ex : www.google.fr) en une adresse IP (ex : 216.58.213.163). Cela permet entre autres d'éviter à l'utilisateur de mémoriser les adresses IP de ses réseaux sociaux préférés (bien qu'il puisse tout de même s'il le souhaite, ça lui évitera en plus d'être victime du DNS poisoning).

Chaque « machine » connectée sur Internet possède une adresse IP qui est un numéro d'identification permettant la communication entre elles. Le DNS est hiérarchisé sous forme d'arborescence que nous pouvons illustrer ainsi :

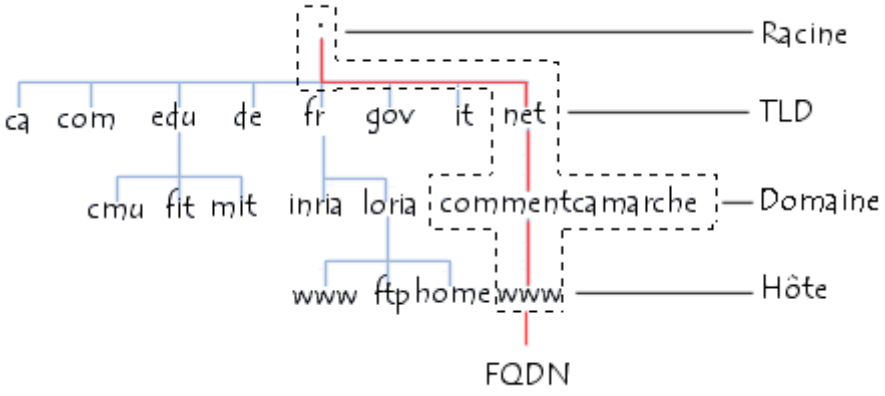

Figure 1: Hiérarchie du DNS (source commentcamarche.net)

Le sommet est appelé la racine, on représente cette dernière par un point. Dans un domaine, on peut créer un ou plusieurs sous-domaines. Les domaines se trouvant immédiatement sous la racine sont appelés domaine de premier niveau (TLD : Top Level Domain).

Le mot « domaine » correspond formellement au suffixe d'un nom de domaine, c'est-à-dire l'ensemble des étiquettes de nœuds d'une arborescence, à l'exception de l'hôte.

L'extrémité d'une branche est appelée hôte, et correspond à une machine ou une entité du réseau. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré, ou le cas échéant dans le sous-domaine.

La « traduction » / résolution du nom de domaine en adresse IP est donc réalisée en parcourant la hiérarchie depuis la racine et poursuivant sur chaque branche en dessous. Si on reprend l'exemple de Commentçamarche de la figure 1 avec un internaute qui taperait dans la barre de recherche de son navigateur préféré www.commentcamarche.net. Dans un premier temps, la machine de l'internaute va regarder dans son cache (requêtes précédemment traduites), si l'adresse n'est pas présente, le client va alors interroger un serveur DNS défini dans sa configuration réseau. La partie « résolution de nom de domaine » peut alors commencer par le serveur DNS dit « résolveur ». Celui-ci fait appel au DNS « racine » qui donne l'adresse du serveur TLD du DNS (ici pour le .net). Ce dernier sera interrogé à son tour puis retournera l'adresse IP du serveur DNS de domaine pour commentcamarche.net. Puis celui-ci retournera l'adresse IP du serveur DNS hôte « www », etc. Une fois que le résolveur DNS a récupéré l'adresse du site voulu, il le stock dans le cache jusqu'à expiration. Illustration de procédé :

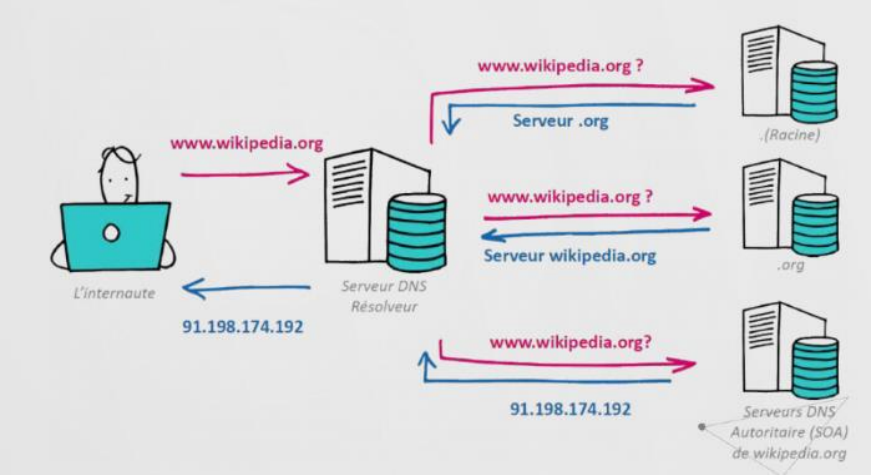

Figure 2: Fonctionnement du protocole DNS (source : cours de Mr Alligand)

- **Le DNS Poisoning**

Le DNS Poisoning ou empoisonnement du cache DNS, a été mis en lumière pour la première fois en 2008 par le chercheur Dan Kaminsky. Celui-ci a révélé une faille de sécurité permettant à des attaquants de modifier la réponse des serveurs DNS, afin d'orienter les internautes vers de faux sites.

Pour remédier à ce souci, des architectes informatiques ont inclus un identifiant de 16 bits afin qu'un résolveur DNS n'accepte que les réponses validant cette ID. Cependant, cela a tout de même une limite … 16 bits ne laissent que 65 536 possibilités, laissant donc encore des failles exploitables par des hackers. En finissant par obtenir un bon ID, un hacker pouvait alors réorienter les requêtes vers la nouvelle adresse et mettant à jour (empoisonnant) le cache.

Cette nouvelle découverte avait donc amené d'autres changements sur le protocole avec l'utilisation d'un port aléatoire en combinaison de l'identifiant (les requêtes DNS passaient toutes par le port 53 auparavant). Cela a permis de complexifier l'ensemble, mais sans pour autant tout résoudre, car ce nouveau « pansement » ajouté a été remis en question en montrant une nouvelle faille à celui-ci.

- **Explication générale de l'attaque**

Pour mener à bien une attaque par DNS Poisoning, l'attaquant exploite une vulnérabilité du serveur DNS qui accepte des informations incorrectes. Le serveur stock dans son cache les résolutions d'IP qu'il reçoit sans vérifier leur authenticité. En d'autres termes, si un résolveur DNS reçoit une réponse falsifiée, il accepte et met en cache les données de manière, car il n'a aucun moyen de vérifier si les informations sont exactes et proviennent d'une source légitime. Il les transmettra par la suite aux utilisateurs qui effectuent une requête vers un nom corrompu.

- **Étapes de l'attaque**

L'attaquant envoie une information vers le serveur DNS cible demandant la résolution du nom d'une machine. Le serveur DNS relaie la requête aux branches (au DNS qui a autorité sur le domaine). Le serveur DNS du pirate enverra alors, en plus de la réponse, des enregistrements additionnels qui seront alors mis dans le cache du serveur DNS cible.

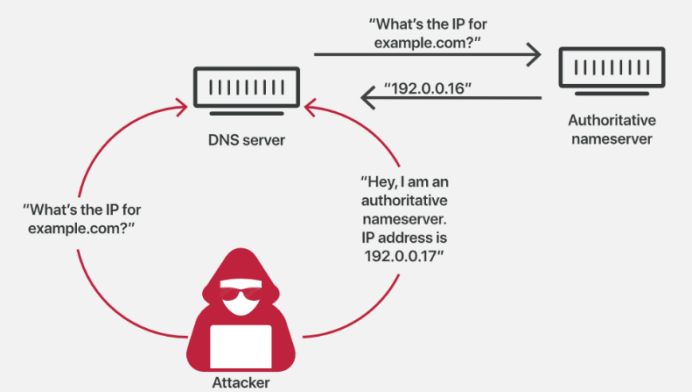

Figure 3 : Processus d'empoisonnement du cache DNS (source : cloudflare.com)

Une machine faisant alors une requête sur ce serveur DNS demandant la résolution d'un des noms corrompus se retrouvera avec comme réponse l'IP d'un site corrompu soigneusement préparé par le hacker.

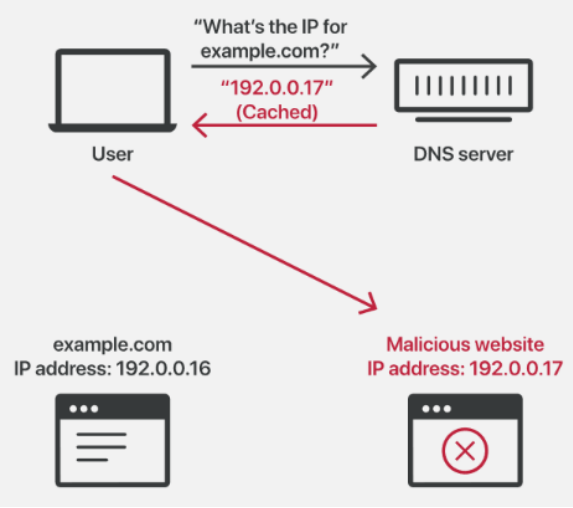

Figure 4 : Illustration du cache DNS empoisonné (source : cloudflare.com)

Les hackers doivent au préalable connaître ou deviner plusieurs facteurs pour mener ce type d'attaque :

- Les requêtes qui ne sont pas mises en cache par le résolveur DNS ciblé et pour lesquelles il devra interroger le serveur de noms faisant autorité
- Le port* utilisé par le résolveur DNS (les résolveurs utilisaient le même port pour toutes les requêtes, mais utilisent désormais un port différent et aléatoire à chaque fois)
- Le numéro d'identification de la demande
- Le serveur de noms faisant autorité vers lequel la requête ira

• Menaces de l'attaque

Ce type d'attaque par DNS Poisoning permet, par exemple, d'envoyer un utilisateur vers un faux site dont le contenu peut servir à du phishing (récupération d'informations personnelles) ou comme vecteur de virus et autres applications malveillantes.

• Solutions possibles

- Mettre à jour les serveurs DNS
- Limiter le cache et vérifier qu'il ne garde pas les enregistrements additionnels
- Vérifier les sites obtenus
- Configurer le serveur DNS pour qu'il ne résolve directement que les noms des machines du domaine sur lequel il a autorité
- Vider le cache DNS régulièrement
- Utiliser un VPN

Pour aller un peu plus loin, j'ai trouvé qu'il existait une variante au protocole DNS actuel avec le DNSSEC (Domain Name System Security Extensions) qui est un moyen de vérifier l'intégrité et l'origine des données DNS. Le DNS classique vue jusqu'ici a été initialement conçu sans vérification, c'est pourquoi l'empoisonnement DNS est possible. Le DNSSEC utilise le chiffrement à clé publique (signature numérique des éléments avec une paire clé publique et clé privée) pour vérifier et authentifier les données. Cette extension n'est pas encore généralisée et est encore aujourd'hui rare.

- **Sitographie**

https://www.youtube.com/watch?v=hpv4dCXXIl4

https://www.youtube.com/watch?v=1d1tUefYn4U

https://fr.wikipedia.org/wiki/Domain_Name_System

https://www.dz-techs.com/fr/check-your-dns-server

https://www.commentcamarche.net/contents/518-dns-systeme-de-noms-de-domaine

https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203373-dns-serveur-dns-domain-name-system-definition-traduction/

https://fr.wikipedia.org/wiki/Empoisonnement_du_cache_DNS

https://www.nextinpact.com/lebrief/44629/lempoisonnement-cache-dns-est-retour

https://www.kaspersky.com/resource-center/definitions/dns

https://www.cloudflare.com/fr-fr/learning/dns/dns-cache-poisoning/

https://www.securiteinfo.com/attaques/hacking/dnsspoofing.shtml