efcse.eu

CYBER ATTAQUE CONTRE LES NOMS DE DOMAINES INTERNET

Auteur : Ubiquitous Solutions – Membre EFCSE
23/02/2019

Cibles : les infrastructures DNS[1]

Gouvernements, compagnies aériennes, industries de transformation, services de renseignement ou de police, grands groupes industriels, etc… autant de cibles touchées et d'impacts difficiles à mesurer face aux attaques informatiques en cours qui affectent la structure même d'internet où les opérateurs sont en position de 1ère ligne.

Le principe : modification de l'adresse des serveurs censés faire transiter une information pour la faire passer par un serveur espion, qui au passage capte la donnée (email, mots de passe…)

D'un point de vue technique, ce type d'attaque de redirection n'est pas nouvelle, en 2013 le New York Times a été visé, en 2017 les géants Microsoft, Google et autre Facebook auraient déjà fait les frais d'assauts sur leur trafic « copié » pendant quelques minutes. La nouveauté se situe plutôt niveau profil des attaquants qui semblent être des groupes bien organisés.

Ces attaques ciblent le système de standard des noms de domaine (DNS), service informatique qui traduit les noms de domaine Internet en adresse IP (Internet Protocole) ou tout autres enregistrements et qui agit comme un annuaire.

Conçu pour faciliter la recherche sur internet, le DNS permet de faire une association entre le nom de votre recherche et une adresse en chiffres, l'IP. Rappelons que l'IP est un des éléments de la base du système d'acheminement des données sur internet, en permettant d'identifier chaque ordinateur il est en quelque sorte l'équivalent de l'empreinte digitale pour un humain.

Tous les noms de domaines d'une entreprise, d'une institution ou de toutes organisations, ainsi que les services internet associés sont dépendants du DNS.

Il s'avère que le DNS est souvent le moins sécurisé, d'où la gravité des attaques, les pirates peuvent ainsi explorer les données en transit et éventuellement récupérer complètement le trafic vers leurs serveurs.

Les principales conséquences de ces attaques sont la rupture de services (emails, site web, services web) et la perte de données stratégiques et confidentielles, perte généralement associée à l'utilisation frauduleuse des informations par les cyber pirates.

Dans ce contexte il est nécessaire de pourvoir au minimum, identifier immédiatement l'attaque, isoler les flux malveillants et préserver la circulation des flux légitimes. L'ICANN[2] préconise le déploiement du protocole de protection "Domain Name System Security Extensions" (DNSSEC).

[1] DNS : Domain Name System
[2] ICANN : Internet Corporation for Assigned Names and Numbers

Principe du DNSSEC : il sécurise les données envoyées par le DNS en permettant d'établir une chaine de confiance remontant à la racine du DNS, ceci grâce à un mécanisme de cryptographie pour la signature des enregistrements DNS.

Sa spécificité par rapport à d'autres protocoles est de sécuriser, non seulement le canal de communication, mais également d'assurer la protection des données et des enregistrements DNS du début à la fin du traitement de l'information, y compris si un serveur intermédiaire est corrompu.

Scénario côté internaute :

- Je me connecte à internet, mon fournisseur d'accès attribue automatiquement une adresse IP à mon ordinateur,
- L'IP est soit permanente, soit renouvelée à chaque connexion, ce changement permettant éventuellement de contrer le traçage,
- J'envoie un email ou j'effectue un téléchargement sur un site internet, ce dernier vérifie l'adresse IP de mon ordinateur avant d'autoriser la requête,
- À chaque accès à une page sur internet cette adresse IP sert d'identifiant.
- Avec le PIRATAGE, je crois être sur la page internet que je connais alors qu'en réalité je suis sur un espace créé par un hacker qui en profite pour détourner les informations que je fournis.

Face à cela la vigilance est essentielle ne serait-ce qu'en vérifiant l'URL[3] de la page pour y détecter d'éventuelles anomalies, des mots inutiles ou suspects par exemple. Survoler l'URL avant de cliquer permet également de lire l'ensemble des caractères et de pouvoir vérifier vers quelle URL se fait la redirection.

La sensibilisation des personnes est primordiale tant à titre privé que professionnel, c'est un véritable enjeu d'éducation et de formation.

Même si de nombreuses entreprises sont déjà organisées pour mener des actions dédiées à la cyber sécurité au sein de leurs équipes, il reste beaucoup à faire. L'inventivité des hackers et la vitesse de l'évolution des profils des cyber attaques semblent plus rapides que la capacité des organisations à anticiper et à être pro actifs par rapport aux attaques.

Il ne s'agit pas d'être alarmiste mais bien de faire en sorte que les entreprises européennes soient « cyber-affutées » techniquement et humainement, y compris la myriade de PME, TPE et ETI qui constituent un tissu social fondamental et alimentent de nombreux pans de l'économie européenne.

[3] URL : Uniform Ressource Locator – adresse web permettant d'accéder à un site internet.