AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

ATTAQUES ET MANIPULATIONS DNS

Contenu

I. Contexte

L'organisme international qui attribue les adresses internet (ICANN) avertit que des efforts pour compromettre le système des noms de domaine (« Domain Name System », DNS) sont en cours, ce qui pourrait entraîner des redirections à grande échelle du trafic mondial de données.

Pour imager, l'ICANN a pour fonction de coordonner « un annuaire » permettant d'associer à différents niveaux un nom de domaine et une IP. C'est cette coordination qui permet instantanément de joindre google.com depuis votre navigateur.

II. Historique

En janvier cette année, les fournisseurs de sécurité Mandiant FireEye et Cisco Talos avaient déjà signalé qu'une attaque de grande envergure dans le monde entier avait compromis des données DNS pour les domaines de la télécommunication, des gouvernements et les organismes d'infrastructure d'internet.

Les équipes de renseignements et les cellules de crise ont identifié une vague de détournements DNS qui a affecté des dizaines de domaines appartenant au gouvernement, à la télécommunication et les entités d'infrastructure d'internet à travers le Monde.

Même si cette campagne emploie des tactiques traditionnelles, elle est différenciée d'autres activités malveillantes précédemment vues car elle exploite les détournements DNS à grande échelle. L'attaquant utilise cette technique comme point d'ancrage initial, qui peut par la suite être exploité d'une multitude de manières. Nous allons détailler dans les prochains jours, les différentes manières de manipulation d'enregistrements DNS que nous avons observé pour permettre la corruption des victimes. Mais nous pouvons déjà affirmer que la première technique implique la création d'un certificat Let's Encrypt et le changement de l'enregistrement DNS de type A.

III. Quel est l'intérêt de cette attaque ?

L'usurpation : en modifiant les informations de cet annuaire, les hackers redirigent les flux d'Internet vers leur infrastructure puis vers celle de votre entreprise. Il est donc possible pour eux de lire vos échanges (formulaire), email professionnel.

Coupure de service : il est également possible à tout moment de rompre le flux Internet en bloquant la résolution du nom de domaine ciblé et ainsi paralyser une grande partie d'Internet.

IV. Que faut-il faire ?

Pour contrer ce type d'attaque, le protocole DNSSEC permet de signer les différentes couches de l'infrastructure gérant les noms de domaine. Le fait d'assigner des clés permet de valider que l'ensemble des serveurs discutant entre eux sont bien légitimes.