Réunion conjointe AFRALO/AfrICANN
ICANN71 – Forum de politiques virtuel

Mercredi 16 Juin 2021

Déclaration

Sujet : Stratégies d'atténuation des abus DNS

Nous, membres de la communauté africaine de l'ICANN participant au forum de politiques virtuel de l'ICANN 71 à La Haye et assistant à la réunion conjointe AFRALO/AfrICANN du mercredi 16 juin 2021, avons discuté de la question de l'Abus du système de noms de domaine (DNS) et de l'importance d'avoir une stratégie unifiée pour l'atténuation des Abus DNS qui inclut toutes les parties prenantes.

L'abus de DNS est un terme général qui fait essentiellement référence à l'utilisation du DNS pour mener des actes frauduleux et/ou malveillants sur Internet. Pour être en mesure de répondre aux incidents d'abus DNS et de les éliminer autant que possible, la collaboration entre toutes les parties prenantes concernées est nécessaire. L'ICANN, en tant qu'entité principale responsable de la sécurité et de la stabilité du DNS, joue un rôle clé en veillant à ce que les problèmes techniques qui permettent l'utilisation abusive du DNS soient identifiés et résolus ; contacter les parties prenantes concernées pour résoudre les problèmes de déploiement pertinents, tels que les attaques par déni de service distribué (DDOS) qui utilisent le DNS et sensibiliser et promouvoir les bonnes pratiques.

Une stratégie réussie d'atténuation des abus DNS doit prendre en compte les éléments suivants :

- Méthodes et qualité du signalement des abus
- Capacité à identifier où se trouvent les menaces, que ce soit dans un domaine spécifique ou d'un point de vue technique - telles que les menaces dues à des problèmes de déploiement
- Offrir des incitations qui favorisent l'adoption de bonnes pratiques
- Standardiser les définitions et les méthodes d'atténuation
- Matériels pédagogiques et la sensibilisation
- Collaboration entre toutes les parties prenantes. La collaboration est un élément principal et essentiel pour une atténuation efficace et efficiente des abus DNS.

Les efforts actuels qui abordent les éléments de la stratégie d'atténuation des abus DNS comprennent :

- Le projet d'ICANN de signalement des cas d'utilisation malveillante des noms de domaine (DAAR), qui est un bon début pour étudier et signaler les menaces d'enregistrement de noms de domaine et de sécurité dans les registres de domaines de premier niveau (TLD). Le système permet aux registres TLD de voir où les menaces sont concentrées au sein du TLD et comment cette menace évolue au fil du temps. Ainsi, le système rassemble et fournit des informations qui pourraient être utiles pour atténuer les abus DNS. Cependant, une participation plus large du registre est nécessaire pour identifier les menaces au sein d'un plus grand nombre de TLD. Nous proposons également l'inclusion de personnes et d'institutions intéressées et impliquées dans la surveillance des abus DNS en tant qu'observateurs dans des groupes tels que TLD-OPS qui fait partie de l'organisation de soutien aux noms de code de pays (ccNSO).

- La responsabilité de travailler sur la résolution des problèmes de conception et de déploiement DNS qui ont permis des actes abusifs DNS n'incombe pas principalement à l'ICANN, mais aux opérateurs DNS et aux opérateurs de réseaux ainsi qu'aux fabricants. Cependant, l'ICANN devrait améliorer sa communication avec les parties prenantes, pour les sensibiliser aux problèmes non résolus et promouvoir les solutions.
- Travailler sur le maintien d'une base de données des déclarants à jour précédemment connue sous le nom de WHOIS. Cependant, comme il s'agit toujours d'un travail en cours, il n'est toujours pas certain que les praticiens de la Cybersécurité soient en mesure d'obtenir les données du titulaire relatives aux domaines abusifs impliqués dans les réseaux de zombies, les logiciels malveillants ou d'autres formes de fraude en temps opportun. De même, des réponses rapides en matière d'hameçonnage et de contrefaçon de marque sont encore douteuses.

Recommandations:

En regardant les éléments susmentionnés de la stratégie d'atténuation des abus DNS et certains des efforts actuels à cet égard, il est évident que la collaboration entre les parties prenantes est essentielle. Par conséquent, nous suggérons que l'ICANN crée une plate-forme à travers laquelle toutes les parties prenantes peuvent travailler ensemble pour mettre en œuvre les éléments de stratégie d'atténuation des abus DNS ci-dessus, sensibiliser et partager des informations et des données. La plate-forme permettrait aux parties prenantes de s'entendre sur les définitions, les actions et les outils des méthodes d'atténuation générales et d'essayer d'équilibrer les problèmes de sécurité et de confidentialité.

Merci !