Trafiquage du service de noms de domaine (DNS)

AOUT 2022

ITSAP.40.021

Les requêtes DNS sont nécessaires à presque toutes les activités que vous effectuez en ligne ou sur les applications réseau. Les auteurs de menace ciblent souvent les services de noms de domaine (DNS pour *Domain Name Service*) afin de diriger le trafic Web légitime vers des domaines malveillants de manière à compromettre non seulement vos réseaux, mais aussi ceux de vos clients. Ils peuvent mener une panoplie d'attaques sur vos systèmes DNS pour trafiquer les paramètres et caches DNS de votre infrastructure ou les entrées du registre DNS de votre organisation. Les mesures d'atténuation et les conseils fournis dans cette publication sont présentés en deux volets : les attaques par trafiquage de DNS sur les serveurs d'hébergement, comme la compromission du registre, et les attaques par trafiquage visant la résolution DNS, comme l'empoisonnement, le détournement et le dévoiement.

En quoi consiste le DNS?

Le DNS est un protocole qui traduit des adresses Web conviviales, comme « cyber.gc.ca », en adresses IP (*Internet Protocol*) lisibles par machine, comme 20.151.96.73. On l'appelle souvent le carnet d'adresses d'Internet. Le DNS est utilisé à la fois pour les actions lancées par l'humain (comme consulter un site Web) et pour celles lancées par la machine (comme exécuter une mise à jour). Ce processus de traduction est ce qu'on entend par résolution DNS. Un résolveur DNS recherche les domaines demandés jusqu'à ce qu'il trouve un serveur de noms faisant autorité qui fournit l'adresse IP du domaine.

En quoi consiste le trafiquage DNS?

Les attaques par trafiquage DNS visent à rediriger les utilisateurs vers du contenu malveillant. Pour y arriver, les auteurs de menace peuvent compromettre les justificatifs d'identité des utilisateurs qui permettent d'accéder à votre infrastructure DNS interne ou d'en assurer la maintenance, ou encore injecter des entrées DNS erronées en exploitant des vulnérabilités dans le protocole DNS. Les justificatifs d'identité compromis permettent aux auteurs de menace d'accéder à votre DNS et d'apporter des changements à votre serveur de noms DNS.

Compromission du serveur de noms DNS

Les auteurs de menace peuvent compromettre les justificatifs d'identité DNS d'administration d'un domaine et changer des enregistrements DNS légitimes. Ils sont ainsi en mesure de rediriger le trafic utilisateur vers leur propre infrastructure ou d'obtenir des certificats de domaines valides qui contiennent une clé non autorisée. Les auteurs de menace peuvent ensuite utiliser des sites Web malveillants ou lancer une attaque de l'intercepteur pour déchiffrer les connexions TLS (*Transport Layer Security*) à ce domaine. Il est important que votre organisation mette en place les mesures d'atténuation suivantes pour se protéger contre la compromission de ses enregistrements du serveur de noms DNS :

- Mettez en place l'authentification multifacteur si cette fonction est disponible pour les comptes du serveur de noms;
- Vérifiez les comptes d'utilisateur qui ont accès au registraire et au serveur de noms;
- Surveillez les journaux de transparence des certificats (CT pour *Certificate Transparency*) associés aux certificats de votre domaine pour voir si des nouveaux ont été ajoutés;
- Mettez en œuvre les programmes Client Lock, Change Lock ou Registry Lock offerts par le registraire de votre nom de domaine pour ajouter des contrôles et des protections supplémentaires aux changements apportés à vos entrées DNS.

Sécurité DNS (DNSSEC)

La sécurité DNS (DNSSEC) est une méthode permettant d'améliorer l'intégrité des données et la sécurité de l'authentification.

La DNSSEC sécurise les données transmises par l'intermédiaire du DNS et aide à protéger l'information sensible stockée dans vos enregistrements DNS. Elle fournit les fonctions nécessaires à l'authentification cryptographique des données DNS, ainsi que le déni d'existence authentifié qui permet au résolveur sur lequel le protocole DNSSEC a été activé de confirmer l'existence d'un domaine en particulier. La DNSSEC améliore également l'intégrité des données.

Elle renforce la sécurité des serveurs DNS et constitue une mesure d'atténuation efficace pour ce qui est de protéger votre organisation des attaques par trafiquage DNS, en particulier l'usurpation et le détournement DNS. Les auteurs de menace ont ainsi un vecteur de moins à utiliser pour exploiter d'autres vulnérabilités potentielles dans votre infrastructure DNS.

No de cat. D97-1/40-021-2022F-PDF
ISBN 978-0-660-44754-4

Mesures d'atténuation pour les attaques courantes par trafiquage de la résolution DNS

Le trafiquage DNS peut être effectué en menant différentes attaques ciblant la résolution DNS. Les méthodes d'attaques suivantes sont fréquemment employées et il convient de mettre en place les mesures d'atténuation connexes pour protéger votre résolution DNS.

Usurpation DNS (empoisonnement du cache)

Les auteurs de menace peuvent obtenir accès au système DNS et y insérer des associations de noms de domaine menant vers des adresses IP malveillantes. Ils peuvent « empoisonner » votre cache DNS avec un domaine malveillant de manière à ce qu'il maintienne la mauvaise association lors des futures requêtes acheminées au serveur DNS par les utilisateurs finaux.

- Mettez en place la DNSSEC pour valider les résolutions DNS.
- Désactivez les fichiers d'hôtes locaux.
- Connectez-vous à un réseau privé virtuel (RPV).
- Videz votre cache DNS régulièrement.
- Utilisez le protocole DoT (*DNS over TLS*) pour chiffrer les requêtes DNS transmises aux résolveurs DNS externes.
- Désactivez le protocole DoH (*DNS over HTTPS*) dans la configuration du navigateur Web.

Détournement DNS

Les auteurs de menace peuvent rediriger les utilisateurs vers des serveurs DNS récursifs malveillants, qui les redirigent ensuite vers des sites malveillants. Il est généralement possible d'y arriver en compromettant un point terminal ou un périphérique réseau afin de modifier ses configurations réseau.

- Mettez en œuvre l'authentification multifacteur pour les comptes et les systèmes utilisés pour modifier votre registre DNS.
- Exécutez l'antivirus et l'antimaliciel sur les points terminaux et les serveurs.
- Mettez en place des règles de pare-feu qui limitent les requêtes DNS et les forcent à accéder uniquement à des résolveurs DNS dans lesquels vous avez confiance.
- Adoptez des protocoles rigoureux de contrôle des modifications pour ce qui est d'apporter des changements aux résolveurs DNS internes.

Dévoiement

Les auteurs de menace peuvent compromettre un routeur et manipuler le cache DNS, ou encore modifier les paramètres de DNS de manière à pointer vers d'autres résolveurs DNS.

- Modifiez le nom et le mot de passe par défaut de vos routeurs pour utiliser des phrases de passe ou des mots de passe robustes, et mettez en œuvre l'authentification multifacteur, le cas échéant.
- Vérifiez régulièrement les paramètres de configuration DNS de votre routeur afin de relever tout changement possible.
- Mettez à jour les micrologiciels de votre routeur et veillez à ce que tous les correctifs de sécurité soient bien installés.

Mesures à prendre pour assurer la sécurité du DNS

Il est recommandé de mettre en œuvre les mesures de sécurité suivantes pour mieux protéger votre organisation des attaques liées au DNS, dont le trafiquage DNS :

- Bloquez les noms de domaine ou les adresses IP susceptibles d'être malveillants ou de poser une menace pour votre organisation;
- Définissez des règles relatives aux requêtes DNS suspectes;
- Mettez en place des restrictions sur vos réseaux pour ce qui est de la longueur, du type ou de la taille des requêtes DNS entrantes ou sortantes;
- Renforcez la sécurité de vos systèmes d'exploitation en appliquant régulièrement les correctifs et les mises à jour;
- Assurez-vous de comprendre les capacités de résolution de noms et déterminez l'ordre de recherche;
- Assurez une surveillance continue des systèmes et des données d'analyse des comportements des utilisateurs afin de détecter automatiquement les anomalies;
- Installez une solution DNS de protection pour empêcher vos utilisateurs de visiter des domaines potentiellement malveillants.

Pour en savoir plus

- *Système d'adressage par domaine de protection (ITSAP.40.019)*
- *Protéger son organisation contre les attaques par déni de service (ITSAP.80.100)*
- *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)*
- *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)*
- *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)*