Les attaques de l'homme du milieu

De quoi s'agit-il ?

Comment les éviter ?

Lorsque nous utilisons Internet, nous estimons que nos communications sont confidentielles et n'ont pas été modifiées ni altérées en cours de transfert. Quand vous saisissez votre mot de passe pour la gestion de votre compte bancaire en ligne, vous partez du principe que : a) votre mot de passe correspond à votre dossier bancaire, b) la banque reçoit le mot de passe sous sa forme correcte, et c) aucun tiers ne peut voir, intercepter ou modifier votre mot de passe lorsqu'il est envoyé à la banque. Il s'agit d'un exemple simplifié, mais, pour l'essentiel, les « attaques de l'homme du milieu » (HDM) fonctionnent en s'attaquant au deuxième ou au troisième de ces principes.

Une attaque HDM ne se contente pas nécessairement de perturber les communications entre humains, mais elle peut également affecter des interactions entre machines, qui sont vitales pour la fiabilité des communications sur Internet. Par exemple, un appareil connecté, comme un assistant virtuel, partage généralement des informations avec un serveur central qui héberge les données.

Si vos connexions aux sites Internet et aux services en ligne ne sont pas fiables, vous pouvez être vulnérable à des risques de sécurité tels que la fraude, l'usurpation d'identité, les malwares, etc. Si vos appareils et objets connectés ne peuvent pas communiquer de manière sécurisée, ils peuvent vous exposer, ainsi que les membres de votre foyer, à des risques.

Qu'est-ce qu'une attaque de l'homme du milieu ?

Lors d'une attaque HDM, un tiers intercepte une communication entre utilisateurs (ou machines). Cela est généralement fait en secret, mais l'utilisateur en est parfois averti. Les attaques HDM se présentent généralement sous deux formes : dans le premier cas, un tiers peut chercher à lire le contenu d'un message ; dans le second, le tiers peut changer le contenu du message, ou altérer de toute autre façon la communication, par exemple en envoyant un malware à la victime. La première attaque concerne la **confidentialité** du message, la seconde son **intégrité**.

Bien que certaines attaques HDM soient effectuées à l'insu des fournisseurs d'accès aux services de communication, d'autres sont conçues au sein même de l'infrastructure des services de communication.

En 2013, des médias ont signalé que certains gouvernements avaient mis en œuvre d'importants systèmes de collecte de données sur Internet avec des techniques de HDM. L'ajout de capacités HDM à des parties de l'infrastructure d'Internet, parfois avec l'aide des fournisseurs d'accès à Internet, a permis à des agences de sécurité nationale d'intercepter et de lire une partie du trafic sur Internet. Si la totalité du trafic était chiffrée, il serait plus difficile pour ces agences d'accéder aux données. Après avoir appris l'existence de ces activités de

surveillance, d'importants fournisseurs d'accès ont pris des mesures visant à chiffrer leurs services, en ajoutant un chiffrement de bout en bout et en activant le chiffrement par défaut.

Les attaques HDM sont une réelle menace pour Internet, quelle que soit l'entité qui y a recours. Les attaques HDM menacent la confidentialité des communications et affaiblissent la confiance de l'utilisateur dans la non-altération de ces communications durant leur transit. Les attaques HDM ébranlent donc la confiance qui accompagne les fonctions de base et la fiabilité d'Internet.[1]

Le chiffrement aide à se prémunir contre les attaques HDM.

Le chiffrement est un moyen pour les individus de se protéger contre une attaque HDM. Il leur permet d'éviter que les données de leurs communications soient lues ou modifiées par des tiers.

Par exemple, si vous envoyez un courriel **non chiffré**, son contenu est visible par tout intermédiaire et nœud du réseau par lequel le trafic passe. Envoyer un courriel non chiffré, c'est comme envoyer une carte postale : le facteur, le personnel du centre de tri et toutes les personnes ayant accès à la boîte aux lettres du destinataire peuvent, s'ils le souhaitent, en lire le contenu.[2]

Chiffrer le message protège sa confidentialité : il ne peut pas empêcher un tiers de visualiser le contenu, mais ce contenu sera incompréhensible, car le message aura été brouillé.

Utiliser le chiffrement pour la signature numérique de données, d'un document ou d'une communication permet de s'assurer que, si un tiers parvient à modifier ces données, cette modification sera flagrante. Avec la plupart des algorithmes de chiffrement, la modification du moindre élément du message initial engendre une version chiffrée du message entièrement différente. Cette propriété peut servir à aider le destinataire à s'assurer que le message original n'a pas été altéré, de la même façon qu'un sceau rompu sur une enveloppe.

Transport Layer Security 1.3 (TLS 1.3) est un important protocole de sécurisation d'Internet, qui assure une couche supplémentaire de protection face aux attaques HDM. TLS 1.3 crée une confidentialité itérative obligatoire pour le trafic sur Internet, ce qui permet au trafic intercepté de ne pas être déchiffré, même si l'attaquant réussit à obtenir une clé privée par la suite. Cela est dû au fait que chaque session est chiffrée avec une nouvelle clé de session. Cela signifie qu'un adversaire doit découvrir les clés de chiffrement pour chaque session, ce qui augmente considérablement la difficulté d'une attaque HDM.

Les attaques HDM visant à accéder à des données chiffrées

Plusieurs gouvernements dans le monde entier ont proposé ou mis en place diverses mesures permettant d'obtenir l'accès à des communications ou à des appareils chiffrés pour des motifs de sécurité nationale ou d'application des lois. Une des méthodes employées pour ces mesures est l'attaque HDM.

Exemple : une attaque HDM sur un trafic HTTPS

Selon Zdnet[3], en 2019, des utilisateurs des opérateurs de mobile du Kazakhstan tentant d'accéder à Internet ont reçu des SMS leur indiquant qu'ils devaient installer les certificats racine attribués par le gouvernement sur leurs appareils mobiles et leurs ordinateurs. Le fait d'imposer aux utilisateurs l'installation de certificats racine appartenant au gouvernement peut donner à ce gouvernement la capacité d'intercepter le trafic HTTPS chiffré et d'effectuer une attaque HDM pour accéder à des communications sécurisées. Cela signifie que le gouvernement peut voir, surveiller, enregistrer et même bloquer les interactions entre les utilisateurs kazakhs et tous les sites Internet, notamment les banques, les fournisseurs de messagerie, les réseaux sociaux, mais aussi des services publics essentiels, tels que l'électricité, les élections, les hôpitaux et les transports. Une fois

1 https://datatracker.ietf.org/doc/rfc7258/
2 https://www.internetsociety.org/resources/doc/2018/encryption-brief/
3 https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/

ces certificats installés, les utilisateurs n'ont aucun moyen de savoir si la sécurité de leurs communications est compromise. Les navigateurs afficheront toujours le symbole du cadenas ou un autre symbole pour indiquer que le trafic est « chiffré et sécurisé », mais ce trafic, même s'il semble sécurisé, ne l'est pas. L'introduction de cette vulnérabilité affaiblit la sécurité d'Internet et érode la confiance dans les infrastructures publiques les plus importantes.

Les attaques HDM ne se contentent pas de s'attaquer à la confidentialité et à l'intégrité ; elles perturbent également l'accès à Internet. Par exemple, en 2012, la tentative d'attaque HDM par une agence de sécurité en Syrie a détruit une partie essentielle de l'infrastructure d'Internet du pays, ce qui a privé la population syrienne d'accès à l'Internet mondial.[4]

Conclusion

Les gouvernements doivent s'abstenir de recourir à des attaques HDM pour permettre aux forces de l'ordre d'accéder à des communications privées. La création de moyens de ce type nuit fortement à la sécurité de tous les utilisateurs et à la sécurité d'Internet. Des acteurs malveillants pourraient utiliser les méthodes créées par les forces de l'ordre pour effectuer leurs propres attaques.[5] Les attaques HDM présentent une menace réelle, non seulement pour la confiance des utilisateurs dans la confidentialité et l'intégrité des communications sur Internet, mais aussi pour la sécurité et la fiabilité d'Internet au niveau mondial.

Références pour en savoir plus :

« Keys Under Doormats » – Rapport technique, MIT Computer Science and Artificial Intelligence Laboratory, 2015

4 https://www.wired.com/2014/08/edward-snowden/

5 https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal