L’attaque Man in the Cloud

Introduction

Vous connaissiez sans doute l’attaque Man in the middle (MITM) qui consiste à intercepter des données sur un flux de communication. Vous connaissiez peut-être également, l’attaque Man in the browser (MITB) qui permet de compromettre les flux (http mais également https) via un code malveillant installé sur le poste client et bien voici maintenant l’attaque Man in the Cloud (MITC) qui permet de compromettre vos données dans le Cloud.

Man in the Cloud, c’est le nom donné à cette attaque par Imperva, la société de sécurité israélienne à l’origine de cette découverte. L’attaque MITC vise exclusivement les applications de stockage en ligne. L’étude d’Imperva porte en particulier sur Box, Dropbox, Google Drive et OneDrive et démontre la possibilité de compromettre intégralement les données hébergées dans le Cloud avec en prime la possibilité d’infecter le poste client et d’exfiltrer des données via le service de synchronisation.

Dans ce type d’application, afin d’éviter que l’utilisateur ne soit obligé de se ré-authentifier à chaque requête, un jeton de synchronisation est créé puis stocké sur le poste client dans le registre (pour Google Drive), dans un fichier (Dropbox) ou dans le gestionnaire d’identités de Windows (pour OneDrive et Box). Deux mécanismes d’authentification différents sont utilisés sur les services testés par Imperva. Alors que Box, Drive et OneDrive s’appuient sur le standard OAuth 2.0, Dropbox utilise un système d’authentification propriétaire.

SYNCHRONIZATION APPLICATION	ONEDRIVE	BOX	GOOGLE DRIVE	DROPBOX
Token Type	OAuth Refresh Token	OAuth Refresh Token	OAuth Refresh Token	Proprietary
Location	Windows Credential Manager	Windows Credential Manager	Encrypted in Registry	Encrypted SQLite file

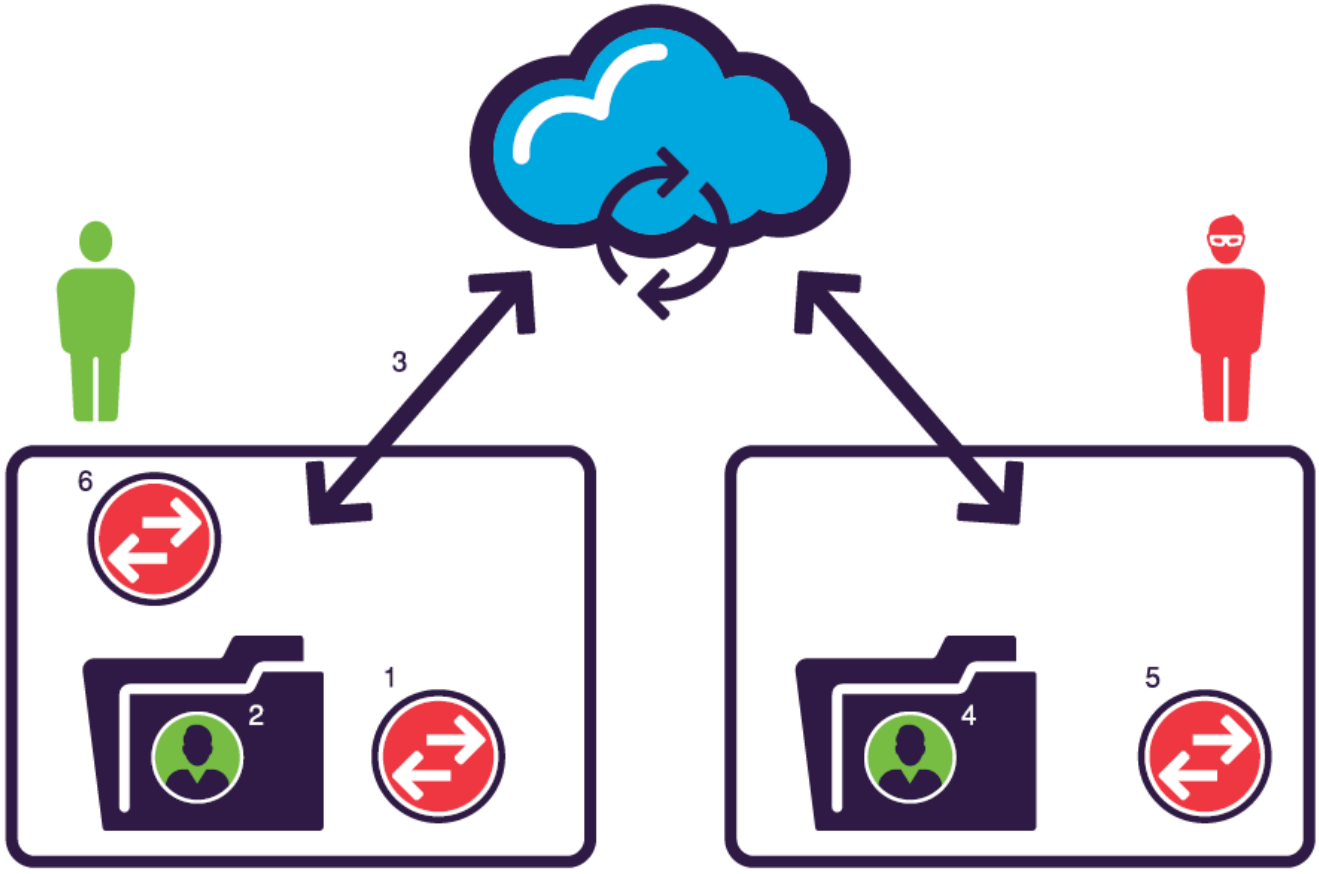
L'utilisation du jeton est très simple. Une fois installé sur le poste client, c'est le seul élément demandé par le service Cloud pour authentifier l'utilisateur et lui donner accès aux données hébergées. Les chercheurs d'Imperva ont remarqué que le jeton de synchronisation n'était pas lié à la machine ni à la session utilisateur en cours. Dans ces conditions, si un même jeton de synchronisation peut être utilisé sur des ordinateurs différents, il suffit de voler le jeton pour accéder au compte de l'utilisateur sans avoir à connaitre son identifiant ou son mot de passe.

Pour démontrer la vulnérabilité des services Cloud et matérialiser l'attaque, Imperva a développé l'outil Switcher. Un attaquant s'authentifie sur le service Cloud et génère un jeton. Switcher prend ce jeton et le stocke dans l'endroit approprié (selon le tableau ci-dessus) sur le poste Client de la victime. Switcher copie également le jeton original (celui de la victime) dans le répertoire de synchronisation. Le hacker peut maintenant récupérer le jeton de l'utilisateur et s'emparer de toutes ses données hébergées dans le Cloud. Une fois l'opération accomplie, Switcher remet en place le jeton original et donne à l'utilisateur l'impression que tout va bien dans le meilleur des mondes…

Dans son rapport, Imperva détaille trois scénarii possibles pour effectuer l'attaque : double échange rapide, double échange permanent et simple échange (rapide ou permanent).

Scénario double échange rapide

Cette attaque assez simple permet à l'attaquant de récupérer le jeton de synchronisation de la victime. L'attaquant est alors en mesure d'accéder aux fichiers qui sont synchronisés par la victime et peut infecter ces fichiers avec un code malveillant. L'attaque est décrite dans la figure suivante :



1. L’attaquant trompe l’utilisateur par ingénierie sociale (malware dans un email par exemple) ou exploite une faille dans le navigateur ou un de ses plugins (drive-by-download) pour exécuter Switcher sur le poste de la victime. Switcher installe le jeton de synchronisation de l’attaquant dans le système.
2. Switcher copie le jeton de synchronisation original dans le dossier de synchronisation
3. L’application synchronise le dossier avec le compte de l’attaquant.
4. L’attaquant a alors en sa possession le jeton de synchronisation de la victime.
5. En réutilisant Switcher sur son poste, l’attaquant installe le jeton volé et accède à toutes les données de la victime stockées dans le Cloud.
6. Switcher est utilisé une seconde fois sur le poste de la victime (double échange) afin de rétablir le jeton de synchronisation d’origine de la victime afin qu’il ne se doute de rien.

C’est la forme « plus propre » de l’attaque. En effet, une fois l’attaque terminée, l’état du dossier de synchronisation de la victime est la même qu’avant l’attaque. Le programme Switcher s’auto détruit et ne laisse aucune trace.

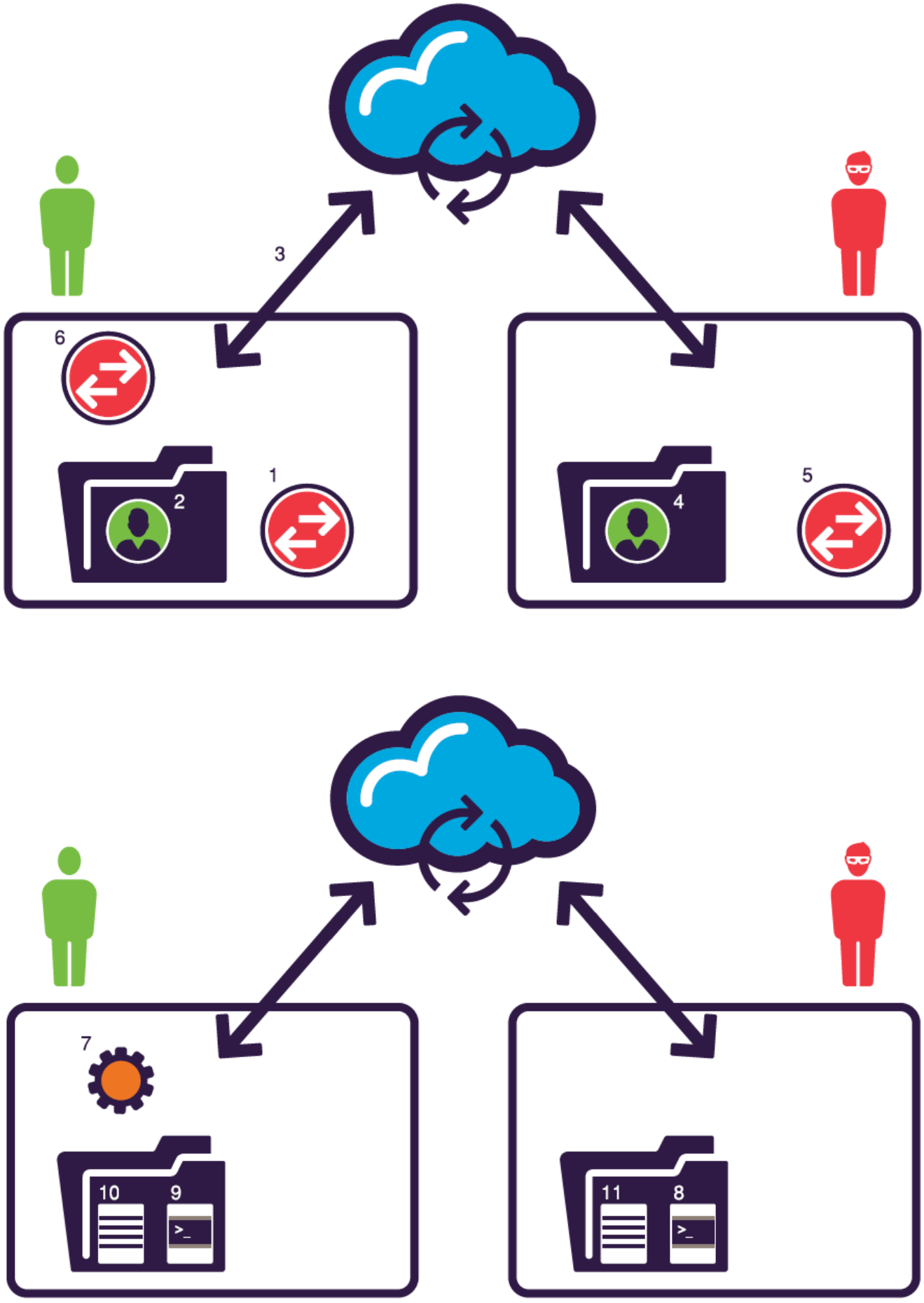
L’attaque en double échange est potentiellement très dangereuse car les services de synchronisation dans le Cloud ne restreignent pas l’accès de plusieurs appareils à partir de plusieurs endroits sur un même compte utilisateur. Ainsi, il est possible pour un attaquant de maintenir une activité de synchronisation fraduleuse avec le

compte de la victime à partir de n’importe où, à tout moment et ceci sans qu’aucune notification ne soit envoyée au propriétaire du compte.

En plus d’avoir accès aux données de l’utilisateur, l’attaquant peut manipuler les fichiers dans le dossier de synchronisation sur sa machine de sorte que les modifications se propagent à la machine de la victime. Par exemple, un attaquant peut insérer du code malveillant dans les documents (exemple un macro dans un document Office ou un script dans un document PDF) qui s’exécutera dès que la victime ouvrira un fichier infecté sur son poste. Cerise sur le gâteau, les résultats de l’exécution peuvent être envoyés dans le dossier de synchronisation puis récupérés par l’attaquant. Après l’opération, l’attaquant peut même supprimer les fichiers résultats dans le dossier de synchronisation et restaurer les fichiers originaux de la victime afin d’éliminer toute trace de l’attaque. Il est possible d’imaginer d’autres scénarios d’attaque comme par exemple une nouvelle façon de pratiquer le « Ransomware ». Dans ce schéma, l’attaquant crypte tous les fichiers de la victime. Une fois les fichiers synchronisés avec tous ses autres appareils, la victime se retrouve dans l’impossibilité d’avoir accès à ses propres documents tant qu’il n’accepte de payer une rançon au hacker.

Scénario double échange persistant

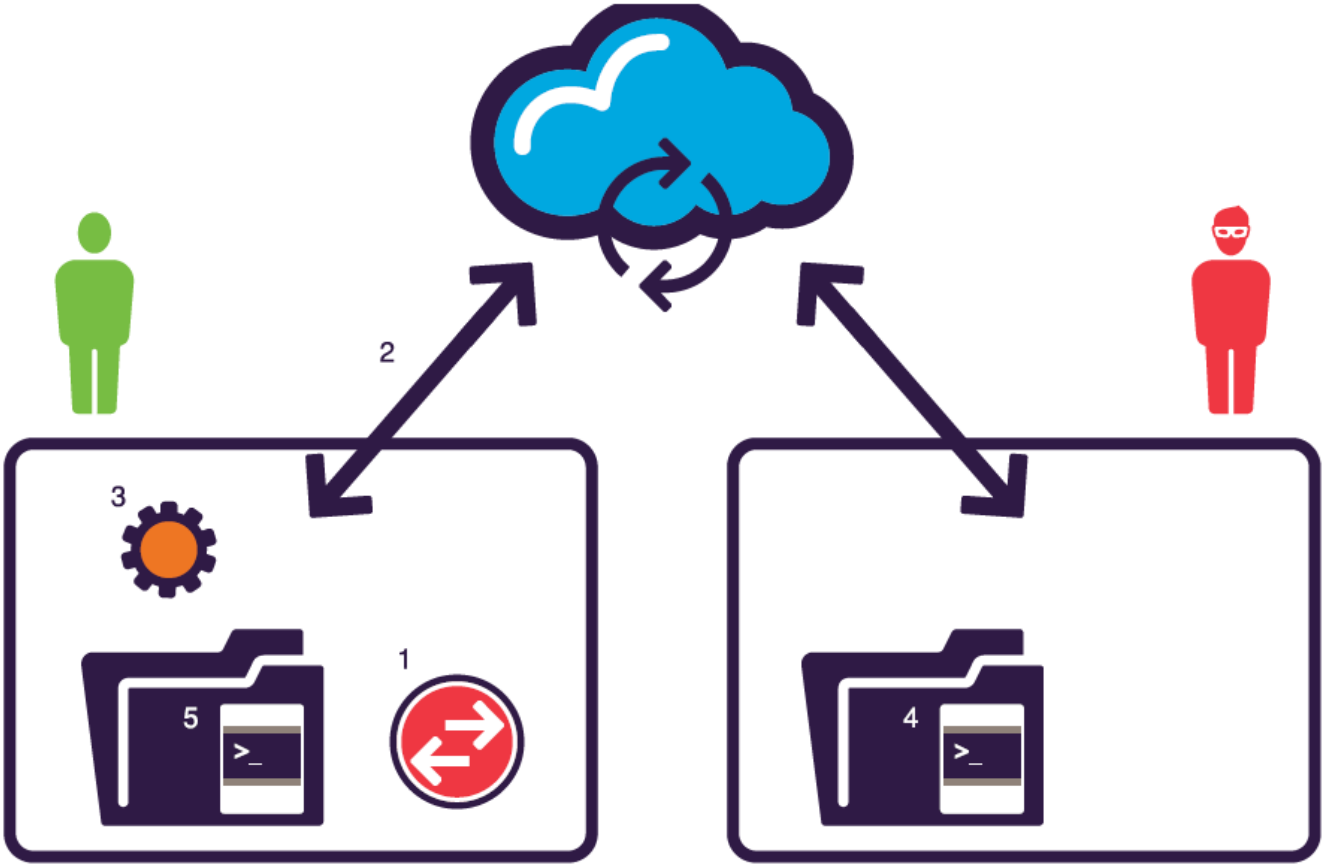
Cette attaque est semblable à la précédente, à l’exception que l’attaquant souhaite maintenir l’accès à distance à la victime. Cet accès permet à l’attaquant d’interagir avec la machine de la victime de temps à autre, exécuter du code arbitraire, et de recueillir la sortie de ce code. L’attaque est décrite en deux phases dans les deux figures suivantes :


3
6
2
1
4
5
7
10
9
11
8

1. L’attaquant trompe l’utilisateur par ingénierie sociale (malware dans un email par exemple) ou exploite une faille dans le navigateur ou un de ses plugins (drive-by-download) pour exécuter Switcher sur le poste de la victime. Switcher installe le jeton de synchronisation de l’attaquant dans le système.
2. Switcher copie le jeton de synchronisation original dans le dossier de synchronisation
3. L’application synchronise le dossier avec le compte de l’attaquant.
4. L’attaquant a alors en sa possession le jeton de synchronisation de la victime.
5. En réutilisant Switcher sur son poste, l’attaquant installe le jeton volé et accède à toutes les données de la victime stockées dans le Cloud.
6. Switcher est utilisé une seconde fois sur le poste de la victime(double échange) afin de rétablir le jeton de synchronisation d’origine de la victime afin qu’il ne se doute de rien.
7. Après le second échange, l’attaquant met en place un outil d’accès à distance de type RAT (Remote Access Tool) paramétré pour attendre l’apparition d’un fichier à un endroit particulier dans le dossier de synchronisation afin de l’exécuter.
8. Un code malveillant est mis dans l’emplacement spécifique dans le dossier de synchronisation de l’ordinateur de l’attaquant
9. Le dossier est synchronisé avec la machine de la victime. Le RAT l’identifie et l’exécute.
10. Le résultat de l’exécution est écrit dans le dossier de synchronisation sur la machine de la victime puis récupéré par l’attaquant via une synchronisation.
11. Une fois les données récupérées, l’attaquant peut alors supprimer le résultat et le code de l’attaque.

Scénario simple échange (rapide ou persistant)

Dans ce type d’attaque, les données de la victime sont synchronisés avec un compte contrôle par l’attaquant.



- L’attaquant lance l’exécution du programme Switcher sur le poste de la victime (typiquement via une opération d’ingénierie sociale ou une attaque de type drive-by-download). Switcher installe le jeton de synchronisation de l’attaquant dans le système.
- Le dossier de synchronisation de la victime est synchronisé avec celui de l’attaquant.
- L’attaque est désormais terminée et l’attaquant a maintenant accès aux données de l’utilisateur. Dans une attaque persistante, l’attaquant met en plus, sur le poste de la victime, un outil d’accès à distance de type RAT (Remote Access Tool) paramétré pour attendre l’apparition d’un fichier à un endroit particulier dans le dossier de synchronisation afin de l’exécuter.
- Un code malveillant est mis dans l’emplacement spécifique dans le dossier de synchronisation de l’ordinateur de l’attaquant
- Le dossier est synchronisé avec la machine de la victime. Le RAT l’identifie et l’exécute.

L’avantage de cette technique est que même si le service de synchronisation met en place un mécanisme de contrôle des accès suspicieux (pour détecter par exemple des accès simultanés à partir de deux endroits différents) la notification de l’anomalie sera envoyée à l’attaquant plutôt qu’à la victime puisque c’est le jeton de synchronisation de l’attaquant qui est utilisé. L’inconvénient est que, comme le jeton installé n’est pas celui de la victime, la synchronisation ne va pas s’effectuer correctement sur les autres dispositifs de l’utilisateur. Pour minimiser

les soupçons, l'attaquant peut périodiquement revenir réinstaller le jeton original de la victime pour permettre une synchronisation avec le compte d'origine.

Détection et remédiation de l'attaque

L'attaque MITC est difficilement détectable car elle s'appuie sur du code déjà installé (l'agent de synchronisation) et sur des canaux de communication légitimes car nécessaires au bon fonctionnement du service. Pour la détection, Imperva propose 2 approches possibles : La détection de la compromission du compte de synchronisation ou plus important encore la détection d'un usage abusif des données internes de l'entreprise. Imperva pense en effet que les attaquants seront probablement plus intéressés par d'autres données dans l'entreprise que celles situées dans les répertoires de synchronisation des postes clients.

Pour la détection de la compromission du compte de synchronisation, Imperva précise que la tâche risque d'être difficile avec les techniques traditionnelles (détection de code malveillant ou analyse des flux de communication vers le C&C). En conséquence, Imperva recommande d'utiliser des solutions de CASB (Cloud Access Security Broker) afin de surveiller l'utilisation des services de Cloud par les utilisateurs. Toujours, selon Imperva, les solutions de CASB sont tout à fait capables de détecter en temps réel ce type d'attaque. D'autres solutions de CASB déployées en mode SecaaS (dans le Cloud) peuvent également stopper l'attaque en bloquant l'accès aux périphériques non officiellement reconnus par l'entreprise.

Pour la seconde approche, Imperva recommande aux entreprise de déployer des solutions de type DAM (Database Activity Monitoring) ou FAM (File Activity Monitoring) pour détecter tout trafic suspicieux.

Les préconisations d'Imperva ne sont pas vraiment surprenantes puisque la société israélienne commercialise des produits CASB avec Imperva Skyfence Cloud Gateway , DAM avec Securephere Database Security et FAM avec File Activity Monitor. C'est de bonne guerre, les vendeurs de solutions de sécurité cherchent des vulnérabilités et des POC (proof of concept) dans le but d'expliquer en quoi leur offre répond à de véritables problématiques de sécurité. Mais n'y aurait-il pas d'autres solutions plus efficaces et moins chères ? Bien sûr que oui et commençons par traiter l'origine du problème. Et si les fournisseurs de service Cloud en profitaient pour mieux sécuriser leur service ? En mettant tout simplement en œuvre un jeton de synchronisation utilisable sur un seul et même device. C'est facile à faire, radical contre l'attaque et ne coûte pas un Kopeck à l'utilisateur. Une autre solution, tout à fait complémentaire, consisterait à chiffrer systématiquement les données que l'on envoi dans le Cloud. Outre le fait que l'attaquant ne pourra plus les lire, ni y insérer de malware, cela protégera également vos données contre un éventuel administrateur malveillant opérant chez le prestataire. La difficulté étant de

trouver une solution de chiffrement fiable, ergonomique et compatible avec les différents OS des dispositifs sur lequel on souhaite partager les informations. Enfin et contrairement à ce qu'affirme Imperva, l'attaque peut être détectée au niveau de poste client. Il suffit pour cela de mettre en œuvre une solution de contrôle d'intégrité. Le lecteur intéressé par cette approche pourra consulter l'article Detecting Man-in-the-Cloud (MitC) Attacks with Adaptive Threat Protection sur le site de Tripwire (éditeur de solutions de contrôle d'intégrité…).

Il est vrai cependant que dans la plupart des cas, l'attaque MITC sera assez difficile à détecter et même si l'utilisateur s'en aperçoit, il lui sera parfois difficile de la stopper. En effet, pour cela il faut impérativement révoquer le jeton de l'attaquant et la tâche n'est pas toujours facile selon le service de Cloud utilisé. La révocation du jeton est particulièrement simple avec Google Drive car il suffit d'effectuer un changement de mot de passe. Cette opération entraine alors la révocation de tous les jetons associés au compte utilisateur et impose pour chaque appareil une nouvelle authentification avec l'identifiant et le mot de passe. D'autre part, comme le changement de mot de passe entraine une révocation immédiate des jetons, toute tentative d'accès au service avec un jeton révoqué sera systématiquement refusée. La situation est assez similaire avec Microsoft Onedrive. La seule différence est toute session déjà en cours et initialisée avec un jeton avant révocation reste active et valide. Il faut donc supprimer manuellement ces périphériques associés dans l'onglet d'administration du compte OneDrive. Avec Box, il faut également changer le mot de passe mais utiliser en plus l'option « révoquer tous les jetons » pour stopper l'attaque. Pour finir, c'est avec Dropbox que la tâche est la plus ardue car un simple changement de mot de passe ne modifie pas le jeton (valeur de la variable host id présente dans le fichier SQLite config.dbx). Pour les détails techniques, on se référera au document d'Imperva. Dans ce dernier cas, il sera sans doute plus simple de supprimer le compte Dropbox existant et d'en créer un nouveau. Bienvenu dans le monde merveilleux du cloud…