Office 365 sous le feu d'attaques par force brute

Si le Cloud facilite le déploiement de nouveaux services et fluidifie la mobilité, il peut aussi augmenter la surface d'attaque des organisations. La société de sécurité Skyhigh Networks le constate. Depuis le début de l'année, elle traque les attaques par force brute des comptes Office 365 d'employés de plusieurs entreprises. Pénétrer un compte Office permettrait à l'attaquant d'accéder à des données confidentielles et stratégiques, notamment s'il s'agit d'un dirigeant ou responsable de haut niveau. Données aussi sensibles que monnayables.

100□000 attaques

En quelques mois, Skyhigh déclare avoir détecté plus de 100□000 tentatives d'attaques sur 48 compte Office 365 en provenance de 67 adresses IP et 12 réseaux différents. De toute évidence, les attaquants ont trié sur le volet les comptes à pénétrer. *« Les attaquants ont ciblé un ensemble d'entreprises et d'employés de haut niveau*, commente Sandeep Chandana, data scientist principal chez Skyhigh, *et ils ont lancé une attaque « lente et faible » pour éviter d'être repérés par le fournisseur de services Cloud. »*

Rappelons que la force brute consiste à tester une combinaison d'identifiants et mots de passe correspondants jusqu'à trouver le bon. Mots de passe qui pourraient avoir été recueillis d'un précédent vol de données comme le milliard de comptes dérobés à Yahoo. Surtout quand certaines études pointent le fait que les utilisateurs tendent à conserver le même mot de passe pour tous leurs services. La force brute n'a cependant rencontré aucun succès parmi les comptes surveillés par Skyhigh. Qui plus est, à la vue des premières alertes, le fournisseur a travaillé avec les utilisateurs concernés pour renforcer leur protection. Mais ailleurs□? Et ce qui vaut pour Office vaut pour tous les services en ligne. En moyenne, une grande entreprise utilise 1□427 services Cloud, dont moins de 10% sont contrôlés par les services IT. Autant de vecteurs d'attaques potentiels.

Attaque de Cloud à Cloud

Le responsable ne dévoile évidemment aucun nom des entreprises ciblées en question. Mais la société spécialisée dans la protection des services Cloud souligne que ces attaques visent des responsables haut placés de plusieurs organisations du Fortune 2000. Et rappelle que plus de 58% des données sensibles stockées dans le Cloud le sont aujourd'hui dans Office 365.

Autre caractéristique distinctive de la charge, *« il s'agissait d'une attaque de Cloud à Cloud dans la mensure où les attaquants se sont servis d'infrastructures d'hébergements publics pour lancer une attaque sur un service SaaS »*. Ce qui permet d'orchestrer des charges visiblement coordonnées et distribuées. Par exemple, un conseiller exécutif a vu 95 tentatives de pénétration sur son compte Office 365 en 5 secondes en provenance de 13 adresses IP qui, chacune, testaient identifiants et mot de passe différents. Ce qui évite d'être repéré aussi vite que lorsque les tentatives proviennent de la même adresse.

Des attaques instructives

Certes, remarque Sandeep Chandana, ces attaques par force brute peuvent être contrées par un système de protection par authentification multifacteurs. *« Mais même activé, les pirates exploitent parfois une autre vulnérabilité au sein de l'infrastructure SSO »*, souligne le responsable dans sa contribution. Selon la réponse que fait le système à la demande d'authentification, le hacker peut en effet en déduire la validité de l'identifiant de connexion même avec un mauvais mot de passe. Une information validée qui peut servir ultérieurement pour des campagnes de phishing ou de spam, par exemple.

Bref, il est difficile pour une entreprise de contrôler tous les protocoles de sécurité de son réseau et les comportements des utilisateurs. Aux yeux de Skyhigh, seule une solution de veille de l'activité en temps réel de type CASB (Cloud Access Security Broker), permet de prendre les devants et limiter les dégâts. Solution que propose évidemment le fournisseur de sécurité.

Lire également
Un ransomware inonde des millions d'utilisateurs d'Office 365
Sécurité renforcée pour Office 365 et Azure
Les mots de passe d'apps mobiles vulnérables à la force brute