proofpoint.

FICHE MENACE

# Compromission et prise de contrôle de comptes cloud

## En bref

### DESCRIPTION

La compromission de comptes cloud consiste à prendre le contrôle du compte cloud d'un service de messagerie ou de collaboration d'un utilisateur légitime afin d'accéder à un large éventail de données, contacts, événements de calendrier, emails et autres outils système. Au-delà des données de l'utilisateur compromis, le cybercriminel peut se servir du compte pour usurper l'identité de l'utilisateur dans le cadre d'attaques d'ingénierie sociale telles que le piratage de la messagerie en entreprise (BEC, Business Email Compromise), que ce soit à l'intérieur ou à l'extérieur de l'entreprise. Les cybercriminels peuvent accéder à des données sensibles, convaincre des utilisateurs ou des partenaires commerciaux externes de transférer de l'argent, ou mettre à mal la réputation et les finances d'une entreprise. Ils peuvent également installer des portes dérobées afin de conserver un accès pour de futures attaques.

### ARSENAL

- Attaques de phishing, notamment phishing de jetons OAuth
- Attaques par force brute qui automatisent la recherche systématique d'identifiants de connexion, comme Aircrack-ng et Jack the Ripper
- Recyclage d'identifiants de connexion, également appelé « credential stuffing », qui utilise des combinaisons de nom d'utilisateur et de mot de passe volées précédemment
- Malwares, notamment enregistreurs de frappe et voleurs d'identifiants de connexion tels que PunkeyPOS et Spyrix

### TYPES

- Vol d'identifiants de connexion : les cybercriminels exploitent des mots de passe faibles, des systèmes de sécurité insuffisants et des mots de passe réutilisés provenant d'autres sites pour pirater des systèmes.
- Applications OAuth malveillantes : les cybercriminels recourent au phishing de jetons OAuth et à l'usurpation d'applications pour inciter des titulaires de comptes à leur déléguer des autorisations afin d'accéder aux ressources système.
- Menaces internes : un comportement négligent ou des intentions malveillantes peuvent entraîner la fuite d'identifiants de connexion.
- Malwares : des logiciels malveillants installés sur des systèmes peuvent échapper à toute détection pendant de longues périodes. Ces malwares peuvent voler des identifiants de connexion et communiquer avec les cybercriminels.

### FACTEURS DE RISQUE

- Utilisation d'applications et de services cloud ou non approuvés (Shadow IT) sans l'accord du département informatique
- Outils peu efficaces de surveillance de la sécurité de la messagerie et du cloud
- Partage d'identifiants de connexion entre collaborateurs ou avec des partenaires externes
- Faible sensibilisation des utilisateurs aux bonnes pratiques de sécurité et aux techniques de phishing courantes

La plupart des entreprises ayant migré leurs ressources vers le cloud, les cybercriminels n'ont pas tardé à leur emboîter le pas. À commencer par les messageries hébergées et les webmails, les applications de productivité cloud telles que Microsoft 365 et Google Workspace, ainsi que les environnements de développement cloud comme AWS et Azure, les cybercriminels ont pris conscience de la valeur inestimable des identifiants de connexion et en font la cible d'innombrables campagnes de phishing. Étant donné que l'authentification unique offre un accès latéral à de nombreux systèmes différents au sein d'une entreprise, un seul compte compromis peut causer des dommages considérables.

## La compromission de comptes cloud dans les médias

### Capital One condamnée à payer une amende de 80 millions de dollars pour le piratage de 100 millions de demandes de carte de crédit en 2019

Le ministère américain de la Justice a arrêté Paige Thompson, ancien ingénieur logiciel chez Amazon, pour fraude informatique et abus. Elle aurait accédé aux données de Capital One. Grâce à une attaque de falsification de requêtes côté serveur (SSRF, Server-Side Request Forgery), elle a mis la main sur les identifiants de connexion d'une personne ayant accès à des informations sensibles stockées dans le service de stockage de fichiers Amazon S3. Selon l'accusation, Paige Thompson se serait vantée de ses exploits sur son canal Slack et aurait publié sur GitHub des instructions permettant de reproduire l'attaque[1].

### La NSA et le FBI accusent la Russie d'attaques par force brute d'envergure ciblant Microsoft 365

Un rapport conjoint publié par les services de renseignement britanniques, la National Security Agency, le FBI et le ministère américain de la Sécurité intérieure a identifié le groupe cybercriminel russe Fancy Bear comme étant le responsable d'une campagne de longue haleine visant à compromettre des comptes Microsoft 365. Le groupe a notamment eu recours à la pulvérisation de mots de passe, une attaque dans le cadre de laquelle des ordinateurs tentent d'accéder à un compte à de nombreuses reprises en utilisant différentes combinaisons de mots de passe[2].

1 Devling Barrett *(The Washington Post)*, « Capital One Fined $80 Million for 2019 Hack of 100 Million Credit Card Applications » (Capital One condamnée à payer une amende de 80 millions de dollars pour le piratage de 100 millions de demandes de carte de crédit en 2019), août 2020.
2 Thomas Brewster *(Forbes)*, « NSA and FBI Blame Russia for Massive 'Brute Force' Attacks On Microsoft 365 » (La NSA et le FBI accusent la Russie d'attaques par force brute d'envergure ciblant Microsoft 365), juillet 2021.

# Anatomie d'une prise de contrôle de comptes cloud

Voici comment se déroulent la plupart des prises de contrôle de comptes cloud.

1. **Vol d'identifiants de connexion.** Le cybercriminel met la main sur les identifiants de connexion de l'utilisateur grâce au phishing d'identifiants de connexion, à des attaques par force brute, au recyclage d'identifiants de connexion (« credential stuffing »), à des applications OAuth malveillantes ou à des malwares voleurs d'identifiants de connexion (voir **Arsenal**, page 1).
2. **Infiltration.** Une fois connecté au compte de l'utilisateur, le cybercriminel a accès aux emails, aux contacts, au calendrier et aux fichiers de la victime. Il peut alors dérober directement ces données ou s'en servir pour usurper l'identité de l'utilisateur de manière convaincante.
3. **Persistance et propagation.** Certains fraudeurs répondent à des fils de discussion existants ou envoient des emails contenant des malwares ou des URL dangereuses à des collègues et à des partenaires commerciaux externes. En se faisant passer pour l'utilisateur compromis, le cybercriminel peut ensuite cibler d'autres personnes à l'intérieur comme à l'extérieur de l'entreprise en leur envoyant des factures factices ou des instructions de détournement de paiements. Il peut également charger des malwares dans des partages de fichiers d'entreprise ou saboter l'entreprise par d'autres moyens. Bien souvent, le cybercriminel configure des règles de transfert automatique lui permettant d'accéder aux emails de l'utilisateur même si celui-ci modifie son mot de passe. En ayant accès à tous les emails et à toutes les invitations de calendrier de l'utilisateur, le cybercriminel obtient des informations essentielles dont il pourra tirer parti lors de futures attaques.
4. **Monétisation.** Si une compromission de compte n'est pas détectée à temps, elle peut entraîner le vol d'argent ou de données de valeur (p. ex., dossiers financiers ou éléments de propriété intellectuelle).

## Les attaques engendrent des fuites de données, des fraudes aux virements bancaires et des violations système

| | |
|---|---|
| **1** | **RECONNAISSANCE** |
| | **Phishing d'identifiants de connexion** |
| | **Fuite ou vidage** |
| | **Enregistreur de frappe ou malware** |
| | **Utilisateur interne malveillant** |
| | **Ingénierie sociale** |
| **2** | **INFILTRATION** |
| | **Recherche systématique d'identifiants de connexion** |
| | **Connexion directe** |
| | **Malwares cloud (applications tierces)** |
| **3** | **PROPAGATION, PERSISTANCE ET APPRENTISSAGE** |
| | **Conservation d'un accès**<br>• Création de règles de transfert d'emails<br>• Modification des autorisations<br>• Création de comptes administrateur<br>• Désactivation de l'authentification multifacteur<br>• Établissement d'un accès tiers |
| | **Utilisation de comptes de confiance pour lancer des attaques**<br>• Envoi d'emails de phishing internes et externes<br>• Chargement et partage de malwares |
| | **Mesure du potentiel**<br>• Consultation d'emails et de fichiers<br>• Exploration de la structure organisationnelle<br>• Étude des processus métier |
| **4** | **MONÉTISATION** |
| | **Piratage de la messagerie en entreprise / Fraude par email**<br>• Fraude aux virements bancaires<br>• Fraude aux salaires<br>• Escroqueries aux cartes cadeaux<br>• Fraude dans la chaîne logistique |
| | **Exfiltration de données**<br>• Email<br>• Téléchargement<br>• Partage |
| | **Sabotage**<br>• Ransomwares cloud<br>• Destruction |
| | **Violation de systèmes**<br>• Spam<br>• Fraude sous forme de service<br>• Cryptominage |

Facteurs de risque et conséquences de la prise de contrôle de comptes cloud

## Comment protéger votre entreprise

- Empêchez les emails de phishing d'identifiants de connexion d'atteindre la boîte de réception des utilisateurs.
- Transformez les utilisateurs en véritables piliers de défense en leur proposant des formations sur les bonnes pratiques en matière de mots de passe et en leur apprenant à reconnaître les emails de phishing. Idéalement, ils doivent également pouvoir signaler facilement les messages suspects.
- Envisagez d'adopter une solution CASB (Cloud Access Security Broker) pour bénéficier d'une vue consolidée des services cloud de votre entreprise. Cette solution devrait inclure des informations sur les utilisateurs et les applications OAuth disposant d'un accès aux données dans les services cloud à partir de n'importe quel terminal ou emplacement.
- Adoptez une approche Zero Trust de l'accès au réseau et aux applications afin de limiter les dommages causés par un compte compromis.
- Analysez les emails internes, et pas seulement les messages entrants, afin de détecter les menaces telles que les malwares et la fraude par email.
- Activez l'authentification multifacteur. Bien qu'il ne s'agisse pas d'une solution miracle contre la prise de contrôle de comptes, elle complique fortement la tâche des cybercriminels.
- Identifiez les utilisateurs les plus à risque et surveillez les incidents.
- Configurez et hiérarchisez les alertes en fonction des facteurs de risque les plus critiques pour votre entreprise.
- Mettez en corrélation les menaces dans l'environnement de messagerie et le cloud pour détecter avec précision les comptes compromis.
- Assurez la gouvernance des applications OAuth et révoquez les applications malveillantes ou dangereuses.
- Empêchez les utilisateurs de cliquer sur des URL malveillantes et de télécharger des malwares en isolant la navigation Web.
- Analysez les incidents de sécurité à l'aide d'une solution proposant des données d'investigation numérique détaillées et des rapports personnalisables.
- Bloquez les accès non autorisés aux applications et services cloud grâce à des contrôles d'accès adaptatifs, en particulier pour les terminaux non gérés.
- Automatisez les mesures de réponse aux incidents de sécurité grâce à des contrôles des règles flexibles qui déclenchent une alerte en cas d'incident ou de modification du profil de risque d'un utilisateur. Il est possible que les utilisateurs ciblés par des attaques ou présentant un risque plus élevé en raison de leurs habitudes numériques ou de leurs privilèges d'accès doivent se réauthentifier régulièrement.

## Le point sur la recherche

Proofpoint surveille des milliers de locataires cloud et plus de 20 millions d'utilisateurs cloud actifs. Une étude des données sur les menaces cloud de 2020 nous a permis de tirer les conclusions suivantes :

**95 %** des entreprises ont été ciblées.

**52 %** des entreprises ont subi au moins une compromission de compte.

**32 %** des entreprises victimes d'une compromission ont constaté des activités postérieures à l'accès, telles que la manipulation de fichiers, le transfert d'emails et des activités au sein des applications OAuth.

**10 %** des entreprises avaient autorisé des applications OAuth malveillantes.

Selon 86 % des responsables informatiques interrogés pour les besoins d'un rapport 2021 du Ponemon Institute commandité par Proofpoint, les compromissions de comptes cloud coûtent aux entreprises plus de 500 000 dollars par an[3]. Les sondés ont également signalé 64 compromissions de comptes cloud par an en moyenne, dont 30 % ont entraîné la divulgation de données sensibles[4].

Près de 60 % des sondés ont indiqué que les comptes Microsoft 365 et Google Workspace sont particulièrement ciblés par des attaques de phishing et par force brute dans le cloud.

Globalement, plus de 50 % des sondés ont déclaré que le phishing était la méthode la plus fréquemment employée par les cybercriminels pour mettre la main sur des identifiants de connexion cloud légitimes.

3 Ponemon Institute, « Cost of Cloud Compromise and Shadow IT » (Le coût de la compromission de comptes cloud et du Shadow IT), avril 2021.
4 Ibid.

## En savoir plus

Pour lutter contre la compromission de comptes cloud, les entreprises doivent s'assurer d'avoir mis en place des mesures de sécurité efficaces. Les plates-formes de sécurité doivent permettre le chiffrement de bout en bout et la surveillance continue des données, ainsi que détecter rapidement les incidents afin que les administrateurs puissent limiter et corriger les éventuels dommages.

Pour découvrir comment lutter contre la compromission de comptes cloud, consultez le site **www.proofpoint.com/fr**.