Comment Proofpoint empêche la prise de contrôle de comptes cloud

Prévention et blocage des prises de contrôle de comptes cloud aux conséquences potentiellement dévastatrices

Produits

- Proofpoint Cloud App Security Broker
- Proofpoint Zero Trust Network Access
- Proofpoint Browser Isolation
- Proofpoint Email Isolation
- Plate-forme Proofpoint Threat Protection
- Proofpoint Targeted Attack Protection

Principaux avantages

- Prévention de la prise de contrôle initiale de comptes en bloquant les attaques de phishing ayant pour but de voler des identifiants de connexion ou d'activer des malwares
- Détection et blocage de toutes les tentatives de prise de contrôle de comptes cloud
- Protection de vos ressources de valeur contre les menaces
- Prévention de l'infiltration de menaces dans votre environnement due à la négligence de vos collaborateurs
- Collecte de renseignements précieux pour vous préparer à contrer les menaces émergentes potentielles

Les cybercriminels s'adaptent à la migration des entreprises vers le cloud. Face à l'adoption croissante par les entreprises de messageries hébergées et de webmails, d'applications de productivité cloud telles que Microsoft 365 et Google Workspace, ainsi que d'environnements de développement cloud comme AWS et Azure, les cybercriminels se sont rapidement rendu compte que les identifiants de connexion aux comptes d'entreprise de base peuvent leur apporter argent et pouvoir. Ils ciblent désormais ces identifiants dans un nombre croissant de campagnes de menaces. Leurs efforts inlassables ne sont que la première étape de leur mission visant à exécuter des fraudes aux virements bancaires, des campagnes d'espionnage industriel, des vols de données personnelles et bien plus encore.

Dans le cadre de la prise de contrôle de comptes cloud, les cybercriminels commencent par compromettre des identifiants de connexion afin de pouvoir infiltrer les systèmes des utilisateurs. Ces attaques sont souvent distribuées par des emails contenant des malwares ou incitant des utilisateurs à divulguer leurs identifiants de connexion. Une fois qu'ils prennent le contrôle d'un compte, les cybercriminels peuvent se faire passer pour des personnes légitimes ou de confiance au sein de l'entreprise de l'utilisateur. Les infiltrateurs peuvent se déplacer latéralement et causer des dommages considérables. Ils peuvent voler ou chiffrer des données importantes. Ils peuvent également charger des malwares afin d'utiliser les fonctionnalités de synchronisation et de partage entre vos endpoints, Microsoft 365 et d'autres référentiels cloud. À partir de là, ils peuvent se propager rapidement au sein de votre entreprise ou télécharger des fichiers sensibles à des fins d'extorsion.

Face à l'utilisation croissante de systèmes d'authentification unique, il suffit d'un seul identifiant de connexion compromis pour permettre à un cybercriminel d'accéder à de nombreux systèmes différents de l'entreprise.

Les ransomwares constituent l'un des types les plus dangereux et déstabilisants de prise de contrôle de comptes cloud. Ce type de cyberattaque interrompt les activités de ses victimes, contraint les hôpitaux à renvoyer les patients chez eux et peut mettre des gouvernements entiers à l'arrêt. Rien que l'année dernière, les États-Unis ont essuyé plus de 65 000 attaques de ransomwares.

D'après Unit 42, l'équipe de threat intelligence de Palo Alto Networks, les trois quarts de ces attaques ont été distribuées par des emails[1]. Il s'agit d'une préoccupation majeure pour les RSSI. Elles sont même devenues un enjeu de sécurité nationale.

Solutions Proofpoint

Les cybercriminels utilisent un grand nombre de stratégies et de vecteurs de menaces pour infiltrer votre réseau. Ils emploient souvent des approches hybrides pour mettre la main sur les informations dont ils ont besoin. Leur arsenal peut inclure des attaques par force brute, des campagnes d'ingénierie sociale et des malwares. Vous avez besoin de défenses complètes et multicouches pour vous protéger contre leurs stratagèmes. Proofpoint propose des produits et services qui peuvent vous aider.

Utilisées conjointement, les solutions Proofpoint contribuent à vous protéger contre la prise de contrôle de comptes cloud par les moyens suivants :

- Prévention de la prise de contrôle initiale de comptes
- Détection et blocage de la prise de contrôle de comptes cloud
- Protection de vos ressources de valeur (collaborateurs et systèmes) contre les menaces externes
- Prévention de l'infiltration de menaces dans votre environnement due à la négligence de vos collaborateurs
- Collecte de renseignements précieux pour vous préparer à contrer les menaces émergentes potentielles

Prévention, détection et blocage

La plate-forme Proofpoint Threat Protection est une solution multicouche et intégrée qui réduit le risque de prise de contrôle de comptes cloud. Elle offre une détection des menaces de pointe qui évite aux utilisateurs de recevoir des malwares, des tentatives de phishing d'identifiants de connexion et autres types d'attaques distribuées par email. Elle orchestre également la sécurité afin de neutraliser les comptes compromis. Le délai de réponse aux incidents et la charge de travail de l'équipe informatique s'en trouvent ainsi réduits. Les utilisateurs ciblés et ceux qui se laissent duper par les tentatives de compromission d'identifiants de connexion peuvent suivre de courtes sessions opportunes de formation et de sensibilisation à la sécurité informatique. Grâce à des bannières HTML informatives et personnalisables, la plate-forme peut encourager les utilisateurs à se méfier des messages potentiellement dangereux. Elle peut authentifier les messages entrants et sortants via DMARC. Elle est également à même d'identifier les comptes fournisseurs compromis. Cette approche de protection multicouche est la raison pour laquelle plus de 60 % des entreprises du classement Fortune 1000 font confiance aux solutions de protection contre les menaces de Proofpoint pour réduire le risque de prise de contrôle de comptes cloud.

1 Unit 42, Palo Alto Networks *(https://unit42.paloaltonetworks.com/ransomware-families/)*, « Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report » (Familles de ransomwares : données 2021 en complément du rapport sur les ransomwares de Unit 42), juillet 2021.

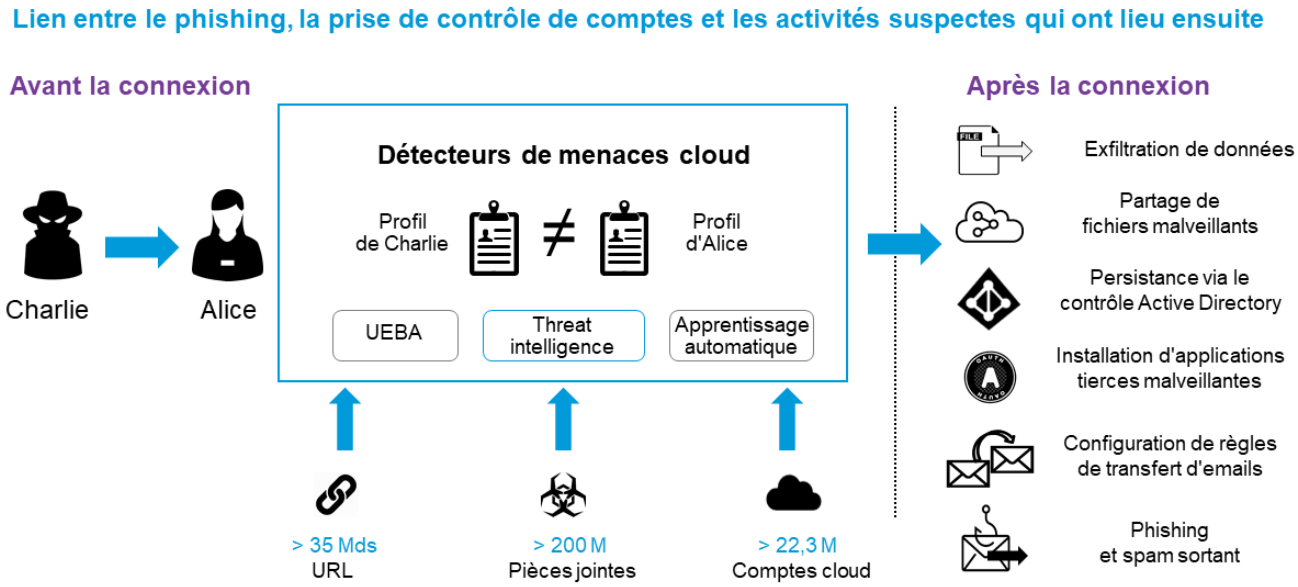

Figure 1. Détection des comptes compromis par Proofpoint CASB

Proofpoint Cloud App Security Broker (CASB) est la pierre angulaire de notre défense contre la prise de contrôle de comptes cloud. Grâce à son approche centrée sur les personnes, il protège vos utilisateurs contre les menaces dans le cloud et préserve vos données sensibles. Sa défense commence par une visibilité et des contrôles d'accès. En effet, sans ces éléments essentiels, il est impossible de mettre en place une protection efficace contre la prise de contrôle de comptes cloud. Proofpoint CASB vous aide à déployer des mesures de sécurité préventives telles que des contrôles d'accès adaptatifs, notamment une authentification renforcée. Nous détectons toutes les tentatives de prise de contrôle et vous informons des activités des cybercriminels une fois qu'ils ont obtenu un accès à un compte. Proofpoint CASB suspend les comptes compromis et neutralise toutes les menaces suivant la prise de contrôle. Ainsi, même si un cybercriminel a accès à l'un de vos comptes, Proofpoint CASB peut l'empêcher de l'utiliser à des fins de transfert d'emails ou de délégation, d'exfiltration de données ou d'envoi d'emails de phishing ou de spam.

Alternative Zero Trust aux VPN

Les effectifs mobiles et les collaborateurs en télétravail sont en forte augmentation dans le monde entier. Avec la migration croissante des applications vers le cloud, le périmètre réseau est en passe de disparaître. Bon nombre d'entreprises commencent seulement à composer avec les nouveaux défis en matière de sécurité qui accompagnent cette tendance. Elles ne découvrent donc que maintenant que leurs systèmes de sécurité d'ancienne génération, qui s'appuient sur une connectivité et des piles de sécurité centrées sur les sites, ne sont pas capables de les protéger contre les menaces de plus en plus innovantes basées dans le cloud.

Proofpoint Zero Trust Network Access (ZTNA) permet à vos utilisateurs d'accéder en toute sécurité aux applications hébergées dans le centre de données et dans le cloud. Cette alternative centrée sur les personnes aux VPN microsegmente les autorisations, ce qui réduit considérablement la surface d'attaque d'un réseau. Son périmètre défini par logiciel offre un accès au réseau Zero Trust.

Isolation du navigateur et de la messagerie

Les équipes informatiques et de sécurité doivent garantir un environnement d'exploitation sécurisé à leurs utilisateurs. Mais elles doivent également leur permettre d'effectuer des recherches et de collaborer efficacement avec les membres de leur équipe. La tâche est loin d'être aisée, étant donné que deux des principaux vecteurs de prise de contrôle de comptes cloud sont justement les outils utilisés pour les recherches et la communication, à savoir le Web et les emails. Proofpoint propose deux solutions permettant à vos équipes de combiner le meilleur des deux mondes. Celles-ci offrent des expériences de navigation et de communication fluides, tout en protégeant les utilisateurs des compromissions de comptes cloud.

Proofpoint Browser Isolation vous protège des compromissions de comptes cloud en permettant aux utilisateurs de naviguer sur le Web tout en les empêchant de cliquer par inadvertance sur des liens de phishing et de télécharger des fichiers malveillants sur les terminaux de votre entreprise.

Proofpoint Email Isolation étend les capacités de Proofpoint Targeted Attack Protection (TAP). Il isole les clics sur les URL dans la messagerie d'entreprise en fonction du niveau de risque qu'elles présentent. Il peut également mettre en évidence les utilisateurs les plus visés par les attaques et identifier les URL à haut risque qui arrivent dans les boîtes de réception de vos collaborateurs.

Informations à jour

Une connaissance étendue et approfondie du paysage des menaces est essentielle pour vous préparer à contrer les prochaines menaces. Le graphique des menaces Nexus de Proofpoint vous offre la threat intelligence complète dont vous avez besoin pour vous protéger contre les cybermenaces actuelles les plus redoutables. Il combine des billions de points de données en temps réel sur de nombreux vecteurs de menaces à travers le monde, des technologies avancées d'intelligence artificielle et d'apprentissage automatique, ainsi qu'une équipe mondiale d'experts en cybersécurité.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.