VECTRA
SECURITY THAT THINKS

RAPPORT

Rapport Spotlight 2020 sur Office 365

DÉTECTION
ET RÉSOLUTION
INTELLIGENTES
DES INCIDENTS

NATIF AU CLOUD

ENTREPRISE

SOMMAIRE

Vectra® protège les entreprises en détectant et en neutralisant les cyberattaques

Leader des solutions de détection et d'aide à la résolution des incidents sur le réseau (NDR), Vectra protège vos données, vos systèmes et votre infrastructure. Vectra permet aux équipes des SOC de détecter et bloquer rapidement les cyberpirates avant qu'ils ne passent à l'action.

Nous identifions en un rien de temps les activités et comportements suspects sur votre réseau étendu, tant sur site que dans le cloud. Vectra les détecte, les signale et avertit le personnel de sécurité afin qu'il puisse intervenir immédiatement.

Vectra met l'intelligence au service de la sécurité. Nous nous appuyons sur l'intelligence artificielle pour améliorer la détection et l'aide à la résolution des incidents au fil du temps, en éliminant les faux positifs afin que vous puissiez vous concentrer sur les véritables menaces.

6,5-7 MILLIARDS $

Le coût de la prise de contrôle de comptes d'utilisateur se situerait entre 6,5 et 7 milliards de dollars en pertes annuelles dans plusieurs secteurs d'activité.

Rapport *The Forrester Wave: Risk-Based Authentication*, 3e trimestre 2017

CHIFFRES CLÉS

4 Mios de comptes Microsoft Office 365 ont été échantillonnés aux fins de cette étude

96 % des clients de l'échantillon ont présenté des **comportements révélateurs de déplacements latéraux**

71 % des clients de l'échantillon ont présenté des **comportements suspects liés à Office 365 Power Automate**

56 % des clients de l'échantillon ont présenté des **comportements suspects liés à Office 365 eDiscovery**

Les cyberpirates sèment le chaos dans le cloud

Aujourd'hui, l'usurpation de l'identité et des privilèges d'accès des utilisateurs constitue le plus grand risque de sécurité dans les environnements SaaS. Avant de mettre en œuvre une plate-forme SaaS, réfléchissez au niveau d'accès réellement octroyé aux utilisateurs.

Pour s'introduire dans une entreprise, les cyberpirates se concentrent désormais sur la prise de contrôle de comptes d'utilisateur plutôt que sur la compromission de comptes de messagerie.

La principale question à se poser est : comment ces privilèges d'accès sont-ils utilisés ? Le principe du moindre privilège est encore plus important dans les environnements SaaS, où seule l'identité est contrôlée et où les données et les ressources sont fortement consolidées.

Dans l'univers SaaS, Office 365 domine le marché de la productivité avec plus de 250 millions d'utilisateurs actifs chaque mois. Pour bon nombre de ces utilisateurs, Office 365 constitue la pierre angulaire du partage de données, du stockage et de la communication d'entreprise, ce qui en fait une cible particulièrement convoitée par les cyberpirates.

Il n'est guère surprenant qu'Office 365 retienne toute l'attention des cyberpirates. Malgré l'adoption croissante de l'authentification multifacteur et d'autres contrôles de sécurité, les répercussions financières et les atteintes à la réputation dues aux violations de données Office 365 ne connaissent pas de fléchissement.

Parmi ces violations, la prise de contrôle de comptes d'utilisateur est la plus répandue et celle qui connaît la croissance la plus rapide. Pour s'introduire dans une entreprise, les cyberpirates se concentrent désormais sur la prise de contrôle de comptes d'utilisateur plutôt que sur la compromission de comptes de messagerie.

Aujourd'hui, les comptes Office 365 permettent aux cybercriminels de se déplacer latéralement pour atteindre d'autres utilisateurs et ressources nécessitant des privilèges. D'après les données recueillies par Vectra auprès de 4 millions de comptes entre juin et août 2020, le déplacement latéral est le comportement suspect le plus couramment observé au sein des environnements Office 365, suivi de près par les communications Command & Control.

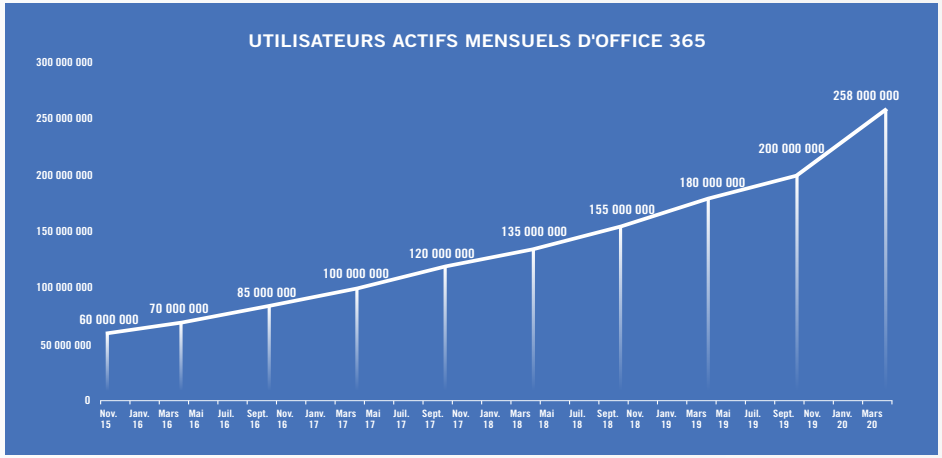


Figure 1. Utilisateurs actifs mensuels d'Office 365

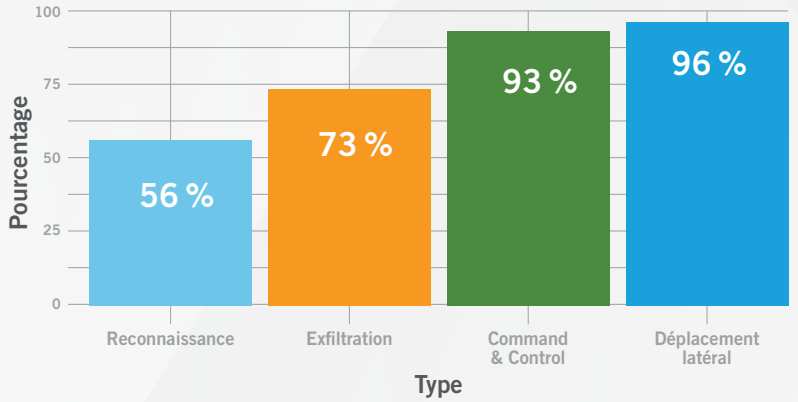


Figure 2. Fréquence des comportements suspects détectés par la solution NDR de Vectra dans les déploiements Office 365

Le cloud est un point d'entrée et l'objectif final des cyberpirates qui se déplacent latéralement à la recherche de ressources à dérober. Dans Office 365, les menaces échappent aux systèmes de détection traditionnels tout au long du cycle d'attaque, étant donné qu'aucune activité n'est enregistrée sur les terminaux et le réseau.

Le problème a pris une ampleur inquiétante. D'après le rapport *The Forrester Wave: Risk-Based Authentication* publié en 2017, le coût de la prise de contrôle de comptes d'utilisateur se situerait entre 6,5 et 7 milliards de dollars en pertes annuelles dans plusieurs secteurs d'activité.

Techniques couramment utilisées par les cyberpirates ciblant Office 365

- Recherche de mots de passe ou de données de valeur dans les e-mails, l'historique des conversations et les fichiers
- Configuration de règles de transfert permettant d'accéder à un flux continu d'e-mails sans avoir à se reconnecter
- Exploitation du canal de communication de confiance (l'e-mail n'imite pas un message du CEO, c'est un e-mail du CEO) pour piéger des employés, des clients ou des partenaires par le biais de techniques d'ingénierie sociale
- Dissimulation de malwares ou de liens malveillants dans des documents que beaucoup de personnes utilisent et considèrent comme fiables, en abusant une nouvelle fois de leur confiance pour contourner les contrôles préventifs susceptibles de déclencher des alertes
- Vol ou prise en otage de fichiers et de données en vue d'obtenir une rançon

Ces techniques d'attaque sont assez simples. Certains cyberpirates ingénieux sont toutefois capables de lancer des attaques bien plus sophistiquées.

OUTILS ET SERVICES LÉGITIMES UTILISÉS PAR LES CYBERPIRATES CIBLANT OFFICE 365

Power Automate

Microsoft Power Automate permet aux utilisateurs de créer des intégrations personnalisées et des workflows automatisés entre les applications Office 365. Il est activé par défaut et propose des connecteurs vers des centaines d'applications et de services tiers. Sa grande disponibilité et sa facilité d'utilisation en font un outil particulièrement utile pour les cyberpirates qui cherchent à orchestrer des activités malveillantes par Command & Control et déplacement latéral.

eDiscovery

Microsoft eDiscovery est un outil de découverte électronique capable d'effectuer des recherches dans les applications et données Office 365 et d'exporter les résultats. Les cyberpirates s'en servent comme d'un puissant outil de reconnaissance interne et d'exfiltration de données.

OAuth

OAuth est une norme ouverte pour l'authentification des accès. Elle est employée par des applications tierces pour authentifier les utilisateurs par le biais des services de connexion Office 365 et des identifiants associés. Les cyberpirates tirent parti des applications Azure malveillantes reposant sur OAuth pour conserver un accès persistant aux comptes Office 365 des utilisateurs.

Les cybercriminels peuvent utiliser Office 365 comme point d'entrée pour infiltrer les systèmes des utilisateurs et bénéficier d'un accès continu à ces derniers. Pour ce faire, ils peuvent passer par la configuration de règles de courrier déclenchées par des e-mails contenant un objet spécifique, ou simplement par la synchronisation du client Outlook. Ces méthodes permettent de transformer un compte Office 365 compromis en shell inversé persistant sur le système de l'utilisateur.

Deux outils Office 365 sont particulièrement utiles aux cyberpirates : Power Automate et la recherche de conformité eDiscovery.

APT33, un groupe de cyberpirates qui serait soutenu par l'État iranien, a utilisé le cloud comme point d'entrée pour infiltrer les systèmes physiques. Il est ainsi parvenu à accéder à Office 365 en lançant des attaques par pulvérisation de mots de passe. Il a ensuite configuré des règles de courrier pour installer un shell inversé sur les systèmes des utilisateurs compromis.

Une fois sur le réseau physique, APT33 a suivi un chemin d'attaque classique sur les systèmes physiques afin d'obtenir des privilèges d'administrateur de domaine. Cette attaque a démontré que les systèmes cloud étaient des points d'entrée et que les systèmes physiques étaient la cible.

Les cyberpirates sont également passés maîtres dans l'art de contourner l'authentification multifacteur d'Office 365. Les techniques d'ingénierie sociale sont une pratique courante visant à inciter les utilisateurs à installer des applications Azure malveillantes. Comme pour les applications mobiles, les utilisateurs acceptent des demandes d'autorisation qui octroient à l'application et au cyberpirate un accès illimité aux ressources. Cet accès peut persister pendant 90 jours sans demande d'authentification intermédiaire, même en cas de modification du mot de passe.

Plus grave encore, les cyberpirates tirent parti d'outils et de fonctionnalités légitimes d'Office 365 pour rester dans l'ombre et contourner les contrôles de sécurité.

Cette méthode d'attaque, largement attribuée à la Chine, a été utilisée à l'encontre d'entreprises australiennes. La technique d'ingénierie sociale employée passait par l'usurpation d'une application à partir de MailGuard 365, une application de sécurité déjà utilisée par les entreprises prises pour cibles. Une fois l'application installée, les cyberpirates se voyaient octroyer un accès persistant leur permettant de lire les profils des utilisateurs et de manipuler leurs e-mails.

Plus grave encore, les cyberpirates tirent parti d'outils et de fonctionnalités légitimes d'Office 365 pour rester dans l'ombre et contourner les contrôles de sécurité. Deux outils Office 365 leur sont particulièrement utiles : Power Automate et la recherche de conformité eDiscovery.

Microsoft Power Automate, anciennement Microsoft Flow, automatise les tâches quotidiennes des utilisateurs telles que la gestion des pièces jointes aux e-mails ou des flux d'approbation. Il est activé par défaut pour tous les clients Office 365 et peut être configuré pour réaliser des opérations permettant aux utilisateurs comme aux cyberpirates de gagner du temps et de s'épargner des efforts. Voici quelques exemples :

- Connexion à un point Command & Control via HTTP pour l'envoi de données
- Synchronisation automatique des fichiers OneDrive avec un espace Google Drive appartenant à un cyberpirate à chaque mise à jour de fichier
- Publication sous forme de tweets de tous les e-mails contenant certains mots clés

Avec plus de 350 connecteurs d'applications disponibles, sans compter ceux qui sont ajoutés chaque semaine, les possibilités qui s'offrent aux cyberpirates utilisant Power Automate sont étendues.

La recherche de conformité eDiscovery d'Office 365 permet de rechercher des informations dans l'ensemble des applications Office 365. À l'aide d'une commande simple, vous pouvez par exemple rechercher « mot de passe » ou « mdp » dans Microsoft Outlook, Teams, l'ensemble des fichiers hébergés dans SharePoint et OneDrive, ainsi que les blocs-notes OneNote.

Ces techniques sont aujourd'hui activement employées et souvent combinées tout au long du cycle d'attaque. Power Automate et eDiscovery figurent au nombre des comportements suspects les plus couramment observés au sein des environnements Office 365 des clients de Vectra.

Microsoft a mis en lumière les risques posés par les outils natifs d'Office 365 en publiant la chronologie d'une attaque ayant recours à des techniques de type « living-off-the-land » permettant de conserver un accès total à Office 365 pendant 240 jours. Les cyberpirates ont utilisé eDiscovery pour trouver des données et Power Automate pour les exfiltrer.

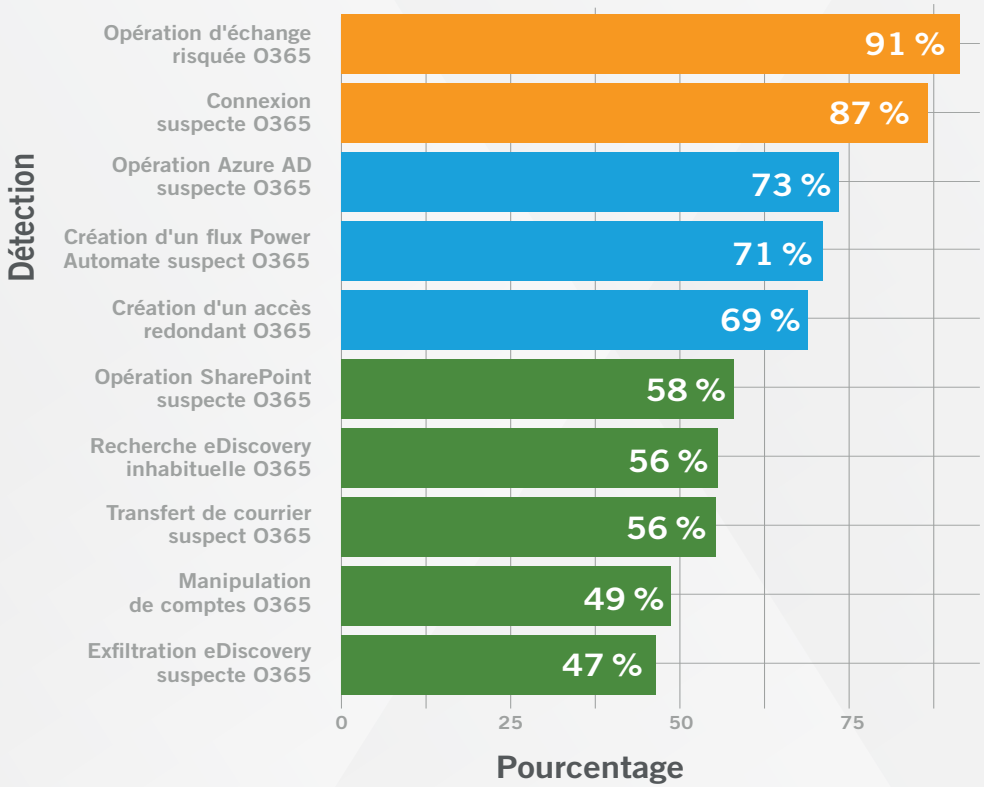


Figure 3. Fréquence des dix principaux comportements suspects détectés par la solution NDR de Vectra dans les déploiements Office 365

L'analyse de 4 millions de comptes Office 365 surveillés par Vectra a permis d'identifier les dix principaux comportements associés aux attaques ciblant Office 365. Ces comportements ont été observés chez des cyberpirates ayant employé des techniques d'attaque par Command & Control et par déplacement latéral.

Cadre MITRE ATT&CK : les dix principaux comportements suspects détectés par la solution NDR de Vectra dans les déploiements Office 365

MITRE ATT&CK™

Détections par Vectra dans Office 365	Cadre MITRE ATT&CK	Comportement d'attaque associé
Opération d'échange risquée	• T1484 Modification des stratégies de groupe • T1098 Manipulation de comptes	**Déplacement latéral** Un cyberpirate manipule Microsoft Exchange pour accéder à un ensemble spécifique de données ou permettre à l'attaque de poursuivre sa progression.
Connexion suspecte	• T1078 Comptes valides	**Command & Control** Un cybercriminel a piraté un compte valide et l'utilise dans le cadre d'une attaque.
Opération Azure AD suspecte	• T1078 Comptes valides	**Déplacement latéral** Il est possible que les cyberpirates élèvent leurs privilèges et effectuent des opérations de niveau administrateur après la prise de contrôle d'un compte d'utilisateur classique.
Création d'un flux Power Automate suspect	• T1041 Exfiltration via le canal C&C • T1008 Canaux de secours • T1105 Transfert d'outils d'infiltration • T1059 Interpréteur de commandes et de scripts • T1020 Exfiltration automatisée	**Command & Control** Un cyberpirate s'est servi de Power Automate comme d'un mécanisme de persistance au sein de l'environnement.
Création d'un accès redondant	• T1098 Manipulation de comptes	**Command & Control** Un cyberpirate a configuré un accès à un rôle sensible pour créer un accès redondant au réseau.
Opération SharePoint suspecte	• T1078 Comptes valides • T1213 Données issues de référentiels d'informations	**Déplacement latéral** Un cyberpirate a mis la main sur un compte administratif SharePoint et l'utilise pour permettre à l'attaque de poursuivre sa progression.
Recherche eDiscovery inhabituelle	• T1119 Collecte automatisée • T1213 Données issues de référentiels d'informations • T1083 Découverte de fichiers et de répertoires	**Reconnaissance interne** Un cyberpirate est parvenu à accéder à des fonctionnalités d'eDiscovery et les utilise pour procéder à une reconnaissance interne au sein de l'environnement.
Transfert de courrier suspect	• T1114 Collecte d'adresses e-mail	**Exfiltration de données** Un cyberpirate externe a établi un accès persistant aux contenus d'une boîte de messagerie spécifique sans avoir à maintenir la persistance en installant un logiciel.
Manipulation de comptes	• T1098 Manipulation de comptes	**Déplacement latéral** Un cyberpirate a élevé les droits d'accès Microsoft Exchange du compte pour faciliter le piratage de la messagerie d'entreprise ou la collecte d'informations supplémentaires afin de permettre à l'attaque de poursuivre sa progression.
Exfiltration eDiscovery	• T1048 Exfiltration via un protocole alternatif	**Exfiltration de données** Un cyberpirate est parvenu à accéder à des fonctionnalités d'eDiscovery et les utilise pour collecter ou exfiltrer des données.

Étude de cas : fabricant de taille moyenne

Un fabricant a été victime d'une attaque par piratage de la messagerie en entreprise.

Le cyberpirate a pris pour cible le service financier et s'est probablement servi de LinkedIn pour identifier les collaborateurs concernés. Une attaque par force brute lente et furtive a été menée contre des protocoles obsolètes et a permis d'identifier les zones non couvertes par l'authentification multifacteur en vue d'accéder à Office 365.

Le cyberpirate a ensuite configuré des règles pour transférer tous les e-mails liés à DocuSign ou aux factures, ce qui prouve que sa motivation était d'ordre financier. Très intelligemment, le cyberpirate a également défini des règles visant à effacer toute trace de son passage en supprimant automatiquement tous les e-mails relatifs aux mots de passe et à la sécurité.

Vectra a détecté en temps réel plusieurs phases du cycle d'attaque et a permis à l'équipe de sécurité de supprimer les règles de transfert et de modifier les mots de passe avant que des e-mails n'aient pu être envoyés en dehors de l'entreprise.

Figure 5. Détections par Vectra de tentatives de piratage de la messagerie en entreprise

Étude de cas : université de recherche

L'unité de recherche médicale d'une université a été victime d'une attaque de phishing qui faisait la promotion d'une application gratuite d'optimisation du calendrier et de gestion du temps.

Un utilisateur a mordu à l'hameçon et a installé l'application OAuth malveillante, contournant ainsi l'authentification multifacteur et octroyant involontairement aux cyberpirates un accès total à Office 365.

Grâce à cet accès, les cybercriminels ont envoyé des e-mails de phishing internes en tirant parti d'identités et de communications dignes de confiance pour se propager au sein de l'université.

Vectra a détecté l'installation de l'application suspecte et, dans le cadre de l'investigation, a constaté qu'une attaque de spear phishing interne avait également déclenché une alerte. L'équipe de sécurité a pu neutraliser la menace en supprimant l'application malveillante.

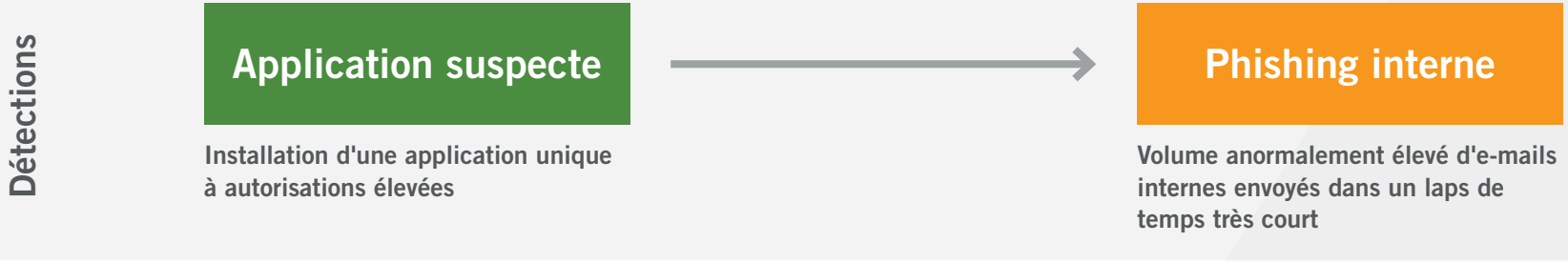
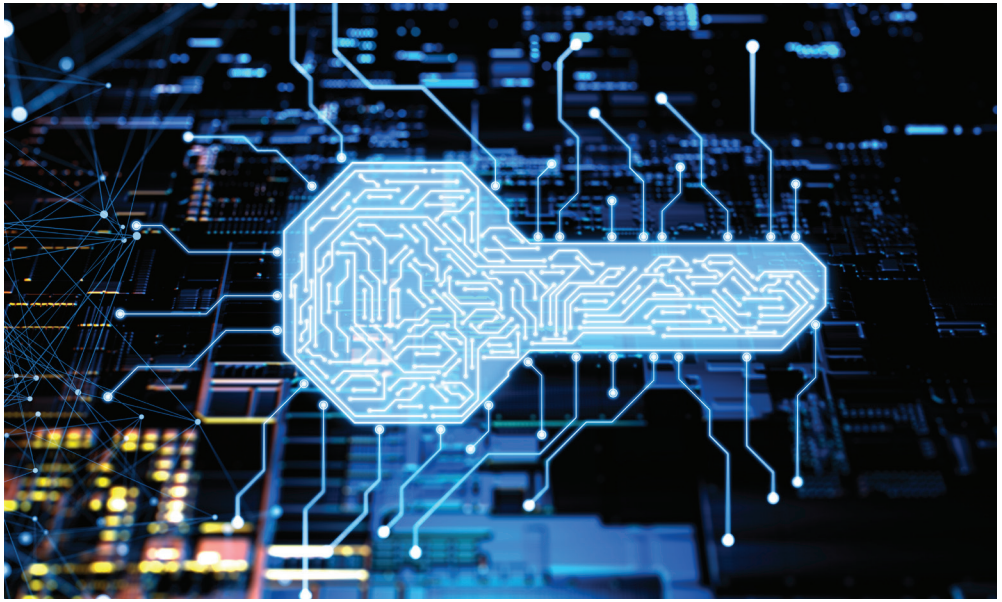


Figure 6. Détections par Vectra d'attaques par contournement de l'authentification multifacteur

Protection continue de vos déploiements Office 365

L'identification des utilisations abusives des accès des utilisateurs est considérée comme un problème statique et repose sur des approches basées sur la prévention, centrées sur le contrôle des politiques ou fondées sur des droits manuels qui détectent les menaces dès l'instant où elles font surface, ce qui laisse peu de temps pour mettre en place une réponse appropriée. Ces approches d'ancienne génération se soldent toujours par un échec.

Ce type de surveillance des accès montre seulement qu'un compte approuvé est utilisé pour accéder aux ressources. Il ne permet pas de déterminer comment ou pourquoi les cyberpirates utilisent ces ressources.



Se contenter de recueillir des informations sur les privilèges octroyés aux entités ne suffit pas. Les équipes de sécurité ont besoin de données contextuelles détaillées leur permettant de comprendre comment les entités utilisent leurs privilèges dans des applications SaaS telles qu'Office 365. De la même façon que les cyberpirates observent ou analysent les interactions entre les entités, l'équipe de sécurité doit adopter la même approche avec les cybercriminels.

Elle doit comprendre comment et à partir de quel emplacement les utilisateurs accèdent aux ressources Office 365, sans analyser la charge active complète des données afin de préserver leur confidentialité. L'important est d'identifier les comportements et les modèles d'utilisation, et non les accès statiques.

Il est essentiel de surveiller de près l'utilisation abusive des accès des utilisateurs étant donné sa prévalence dans les attaques réelles. Les plates-formes SaaS telles qu'Office 365 permettent aux cyberpirates de se déplacer latéralement sur les réseaux. Il est donc primordial de contrôler l'accès des utilisateurs aux comptes et aux services.

Idéalement, si les équipes de sécurité disposent d'informations fiables et d'attentes adéquates concernant les plates-formes SaaS, il leur sera bien plus simple d'identifier et de neutraliser rapidement les comportements malveillants et l'utilisation abusive de privilèges.

Les équipes de sécurité ont besoin de données contextuelles détaillées leur permettant de comprendre comment les entités utilisent leurs privilèges dans des applications SaaS telles qu'Office 365.

E-mail : info_france@vectra.ai / info_dach@vectra.ai vectra.ai/fr