VECTRA
SECURITY THAT THINKS

RAPPORT SPOTLIGHT T2 2021

Vision et visibilité : les dix détections de menaces les plus fréquentes dans Microsoft Azure AD et Office 365

DÉTECTION
ET RÉSOLUTION
INTELLIGENTES
DES INCIDENTS
SOLUTION NATIVE AU CLOUD
POUR ENTREPRISES

SOMMAIRE

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

Vectra® est le leader de la détection et de l'aide à la résolution des incidents, du cloud jusqu'aux centres de données, en passant par les équipements IoT et les terminaux des utilisateurs. La plate-forme Cognito® accélère la détection et l'investigation des menaces grâce à une technologie d'intelligence artificielle permettant d'enrichir les métadonnées réseau qu'elle collecte et stocke avec des données contextuelles pertinentes. Objectif : détecter, traquer et analyser les menaces connues et inconnues en temps réel. Sur la plate-forme Cognito, Vectra propose quatre applications qui permettent de résoudre les cas d'utilisation à priorité élevée. Cognito Stream™ envoie des métadonnées enrichies par des informations de sécurité aux lacs de données et aux solutions SIEM. Cognito Recall™ est une application cloud destinée à stocker et à investiguer les menaces grâce à des métadonnées enrichies. Cognito Detect™ s'appuie sur l'intelligence artificielle pour identifier rapidement les attaquants inconnus et furtifs et gérer le problème selon une échelle de priorités appropriée. Enfin, Cognito Detect pour Office 365 et Azure AD™ détecte et neutralise les attaques au sein des applications SaaS d'entreprise et de l'écosystème Microsoft 365. Pour plus d'informations, rendez-vous sur le site vectra.ai.

71 %

des utilisateurs ont subi en moyenne sept prises de contrôle de comptes d'utilisateur légitimes au cours de l'année écoulée*.

POINTS CLÉS

- Une technologie d'intelligence artificielle sophistiquée permet d'analyser en continu la façon dont les utilisateurs accèdent aux applications cloud, les utilisent et les configurent. Elle peut jouer un rôle essentiel dans votre protection en détectant et en neutralisant les menaces telles que la prise de contrôle de comptes d'utilisateur.

- Le classement des dix détections de menaces les plus fréquentes dans Microsoft Azure AD et Office 365 permet aux équipes de sécurité de détecter les comportements inhabituels ou à risque au sein de leurs environnements.

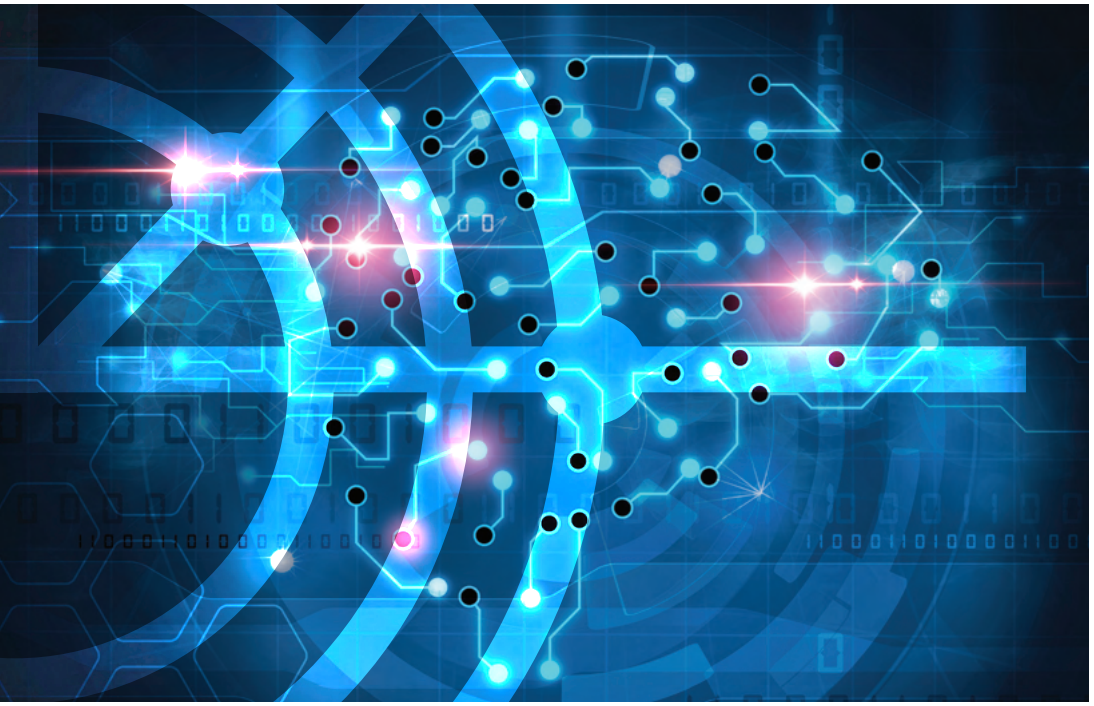
- Quelle que soit la taille de l'entreprise, la détection « Opération d'échange risquée Office 365 » arrive en haut (si ce n'est en première place) du classement des détections observées par les clients de Vectra.

- Les actions courantes ayant été exécutées par des cybercriminels dans l'environnement Azure AD lors d'une récente attaque de la chaîne logistique ont été détectées par Vectra, qui a alerté les équipes de sécurité de la menace.

* Sécuriser Microsoft Office 365 face à la nouvelle normalité

Détection des comportements sortant de l'ordinaire

Le cloud ne cesse de révolutionner le domaine de la sécurité et rend obsolète l'approche traditionnelle de la protection des ressources. Toutefois, grâce à la collecte de données pertinentes et à une technologie d'intelligence artificielle sophistiquée, les entreprises peuvent mieux cerner les tenants et aboutissants des attaques et ainsi permettre aux équipes de sécurité de se concentrer sur les menaces nécessitant leur intervention, plutôt que de perdre un temps précieux à traiter des alertes anodines. Ce rapport présente les dix détections de menaces les plus fréquemment observées chez la clientèle de Vectra, qui permettent de ratifier les attaques ciblant Microsoft Azure AD et Office 365. Toutes les données présentées proviennent de véritables exemples de détections envoyées par Vectra aux équipes de sécurité en cas d'identification d'un comportement sortant de l'ordinaire.



Interprétation des détections de menaces

Bien que ce rapport se concentre sur les dix détections les plus couramment observées par nos clients dans l'environnement Azure AD et Office 365 selon leur fréquence relative, il est important de garder à l'esprit que la détection et l'aide à la résolution des incidents sont bien plus simples lorsque la malveillance des actions des cybercriminels est évidente. Malheureusement pour les équipes de sécurité réseau, les attaquants délaissent de plus en plus ces actions peu discrètes au profit du contrôle et de l'utilisation inappropriée ou abusive des accès et services existants des entreprises.

Il est donc essentiel que les équipes de sécurité réseau prennent conscience des similarités qui existent entre les actions mises en œuvre par les cybercriminels pour atteindre leurs objectifs et les comportements habituels des utilisateurs autorisés de l'entreprise. Les principaux facteurs permettant de faire la distinction entre les actions d'un attaquant ou d'un utilisateur interne malveillant et celles d'un utilisateur inoffensif sont l'intention, le contexte et l'autorisation. Une technologie d'intelligence artificielle sophistiquée peut faire toute la différence en permettant d'analyser en continu la façon dont les utilisateurs accèdent aux applications cloud, les utilisent et les configurent afin d'obtenir des informations et des connaissances exploitables, tout en offrant une visibilité sur l'accès aux systèmes, comptes et charges de travail.

Les principaux facteurs permettant de faire la distinction entre les actions d'un attaquant ou d'un utilisateur interne malveillant et celles d'un utilisateur inoffensif sont l'intention, le contexte et l'autorisation.

L'intelligence artificielle permet notamment de faire facilement le tri entre les alertes sérieuses, p. ex. une détection vous avertissant d'un transfert de courrier suspect dans Office 365, et la multitude de notifications ne présentant aucun danger. Les menaces telles que la prise de contrôle de comptes d'utilisateur confrontent les entreprises à des enjeux sans précédent et à des pertes annuelles estimées à plusieurs milliards de dollars. La bonne nouvelle, c'est que les comportements propres à ces techniques d'attaque n'auront plus aucun secret pour vous si vous faites appel à l'intelligence artificielle. Étudions en détail les dix détections les plus fréquentes.

Les dix détections de menaces les plus fréquentes

Bon nombre des détections évoquées dans ce rapport sont déclenchées par un comportement inhabituel, mais toutes ne sont pas la preuve d'une activité malveillante. Certaines peuvent être liées à un comportement inhabituel pour l'environnement, tandis que d'autres peuvent signaler un comportement contraire aux règles. Quelle que soit l'activité concernée, ces détections mettent toujours en lumière une vaste surface d'attaque qui doit être gérée par nos clients. Pour en savoir plus sur la science au service de ces détections, consultez le livre blanc La science des données au cœur du modèle d'intelligence artificielle de Vectra pour la détection des menaces.

Quelle que soit l'activité concernée, ces détections mettent toujours en lumière une vaste surface d'attaque qui doit être gérée par nos clients.

Vision et visibilité : l'intersection entre les cybercriminels et les équipes de sécurité

Vision :

Des attentes claires de ce qui est autorisé doivent être établies, généralement sous la forme de règles prescriptives, sans quoi les équipes de sécurité éprouveront des difficultés à faire quoi ce soit outre éliminer les menaces évidentes. C'est pourquoi les entreprises doivent avoir une ***vision***, généralement définie par des règles, de l'utilisation autorisée des services cloud auxquels elles ont recours.

Votre vision de l'utilisation autorisée des services cloud doit tenir compte des questions suivantes :

- Quels services et comportements sont autorisés ?
- Dans quel contexte sont-ils autorisés ?
- Les utilisateurs sont-ils autorisés à utiliser le stockage cloud et comment doivent-ils interagir avec les entités externes ?
- Quels paramètres opérationnels et dispositifs de protection sont censés accompagner les comportements associés à ces services cloud ?

C'est pourquoi les entreprises doivent avoir une ***vision***, généralement définie par des règles, de l'utilisation autorisée des services cloud auxquels elles ont recours.

Visibilité :

Même si elles disposent d'une vision clairement définie, les entreprises sont rapidement confrontées à des difficultés lorsqu'elles manquent de ***visibilité***, car elles n'ont pas la possibilité de surveiller ni d'évaluer les écarts par rapport à leur vision. Pour résoudre ce problème, il est nécessaire d'identifier les comportements que les cybercriminels ont tendance à adopter, ainsi que de collecter et d'agréger les données permettant de les détecter selon un processus pouvant être opérationnalisé par le personnel de sécurité.

Même si elles disposent d'une vision clairement définie, les entreprises sont rapidement confrontées à des difficultés lorsqu'elles manquent de ***visibilité***.

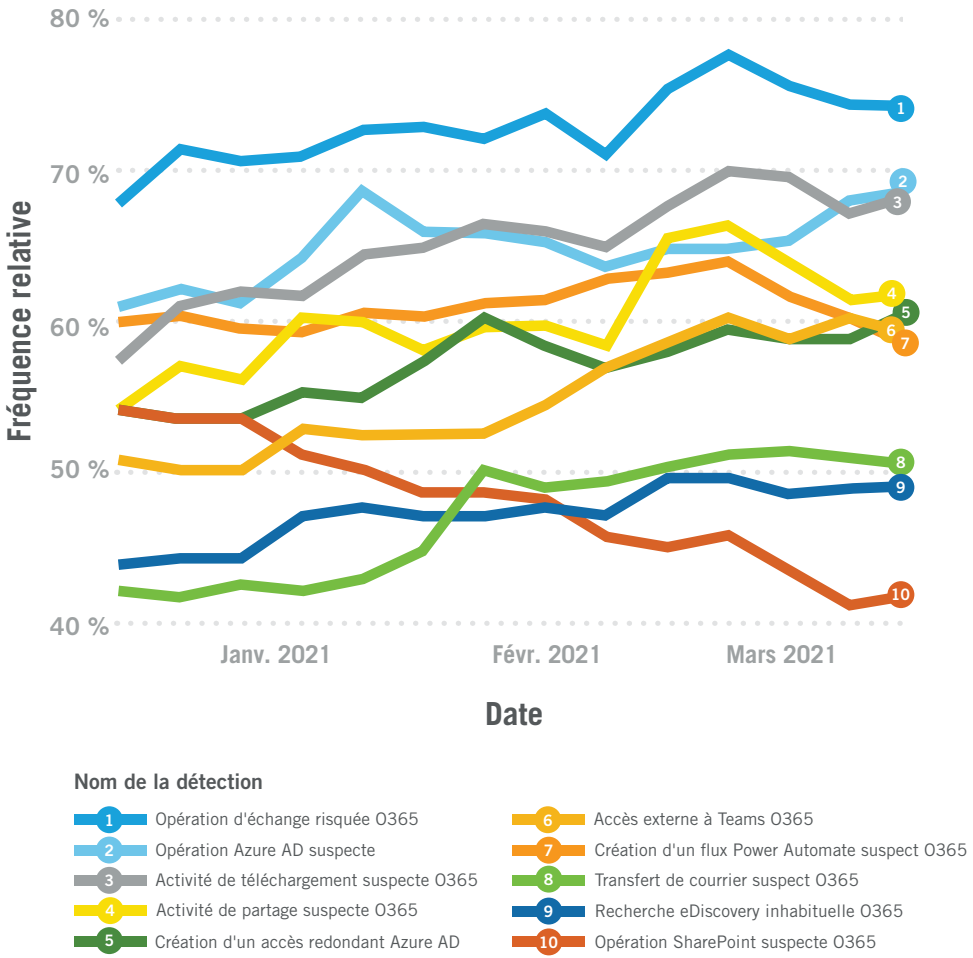
Renforcer la visibilité

- **Services** : les équipes de sécurité sont-elles capables de détecter les attaques exécutées via des services cloud d'entreprise ? Par exemple, sont-elles capables de détecter toute utilisation abusive de Power Automate à des fins de commande et de contrôle (C&C) malgré les protections déployées autour de ces fonctionnalités ?
- **Gestion** : les équipes de sécurité sont-elles capables d'identifier toute utilisation inappropriée ou abusive des fonctions d'administration et de gestion, p. ex. les opérations d'échange risquées permettant à des cybercriminels et à des utilisateurs internes d'élever leurs privilèges ou de collecter et d'exfiltrer des informations sensibles ?
- **Chaîne logistique** : les équipes de sécurité sont-elles capables de détecter toute compromission des fournisseurs et des prestataires de services de confiance permettant aux cybercriminels de contourner les contrôles préventifs et les dispositifs de protection d'une entreprise ?

Les responsables de la sécurité doivent pouvoir répondre à ces questions avec assurance. Le meilleur moyen d'y parvenir, c'est d'effectuer des analyses actives, de traquer les menaces et de procéder à des tests de la sécurité, car ces aspects exigent plus que de simples analyses comparatives ou vérifications de la conformité.

Les dix détections de menaces les plus courantes par fréquence relative

Ce graphique chronologique montre les dix détections de menaces les plus couramment observées chez la clientèle de Vectra selon leur fréquence relative. Il indique le pourcentage de clients ayant déclenché chaque détection par semaine.



Les dix détections de menaces les plus fréquentes

1. **Opération d'échange risquée O365**
   Des opérations d'échange inhabituelles pouvant indiquer qu'un attaquant manipule Exchange pour accéder à des données spécifiques ou permettre à une attaque de poursuivre sa progression ont été détectées.
2. **Opération Azure AD suspecte**
   Des opérations Azure AD inhabituelles pouvant indiquer que des attaquants élèvent les privilèges et réalisent des opérations de niveau administrateur suite à la prise de contrôle d'un compte d'utilisateur ont été détectées.
3. **Activité de téléchargement suspecte O365**
   Un compte a téléchargé un nombre inhabituel d'objets, ce qui peut indiquer qu'un attaquant utilise les fonctions de téléchargement de SharePoint ou de OneDrive pour exfiltrer des données.
4. **Activité de partage suspecte O365**
   Un compte a partagé un volume de fichiers et/ou de dossiers plus élevé que d'habitude, ce qui peut indiquer qu'un attaquant utilise SharePoint pour exfiltrer des données ou conserver un accès une fois l'accès initial révoqué.
5. **Création d'un accès redondant Azure AD**
   Des privilèges administrateur ont été attribués à une entité, ce qui peut indiquer la création d'un accès redondant par un attaquant en vue de se protéger des mesures correctives.
6. **Accès externe à Teams O365**
   Un compte externe a été ajouté à une équipe dans O365 Teams, ce qui peut indiquer qu'un attaquant a ajouté un compte dont il a le contrôle.
7. **Création d'un flux Power Automate suspect O365**
   La création d'un flux Power Automate inhabituel a été détectée, ce qui peut indiquer qu'un attaquant configure un mécanisme de persistance.
8. **Transfert de courrier suspect O365**
   Le transfert de courrier peut être utilisé comme un canal de collecte ou d'exfiltration sans avoir à maintenir la persistance.
9. **Recherche eDiscovery inhabituelle O365**
   Un utilisateur crée ou met à jour une recherche eDiscovery, ce qui peut indiquer qu'un attaquant est parvenu à accéder à des fonctionnalités d'eDiscovery et les utilise pour procéder à une reconnaissance.
10. **Opération SharePoint suspecte O365**
    Les opérations SharePoint administratives inhabituelles peuvent être associées à des activités malveillantes.

La collaboration ouvre la voie aux cybercriminels

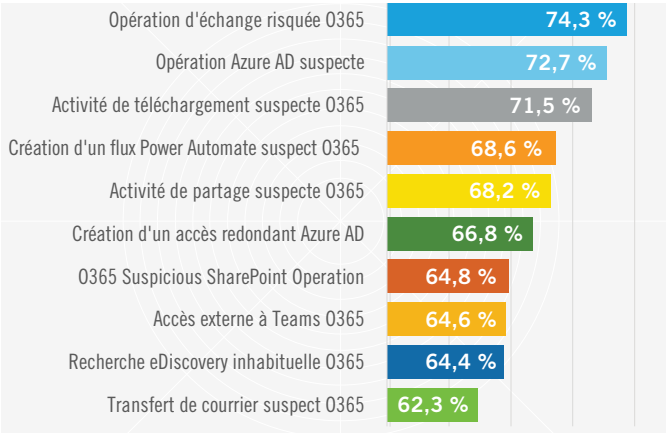
Certaines de ces détections de menaces sont déclenchées par des activités favorisant le confort d'utilisation, la collaboration avec les intervenants externes ou encore le provisionnement d'un accès administrateur à l'environnement Azure AD. L'envoi aisé de documents à partir de OneDrive ou de SharePoint simplifie le partage d'informations avec les intervenants externes, mais permet également aux attaquants d'accéder aux informations déjà stockées sur ces services ou transférées vers ceux-ci. Dans ce cas, la plupart des détections sont liées à une activité de téléchargement suspecte, à une opération SharePoint suspecte ou à une activité de partage suspecte dans Office 365.

Certaines de ces détections peuvent être déclenchées par les échanges avec des utilisateurs externes via l'application très pratique Microsoft Teams. Mais si celle-ci est pratique pour les utilisateurs légitimes, elle l'est aussi pour les attaquants, qui en profitent pour mettre la main sur des données de valeur ou s'emparer de documents et d'informations. Il est d'ailleurs assez fréquent que des détections soient déclenchées par un accès externe à Teams dans Office 365.

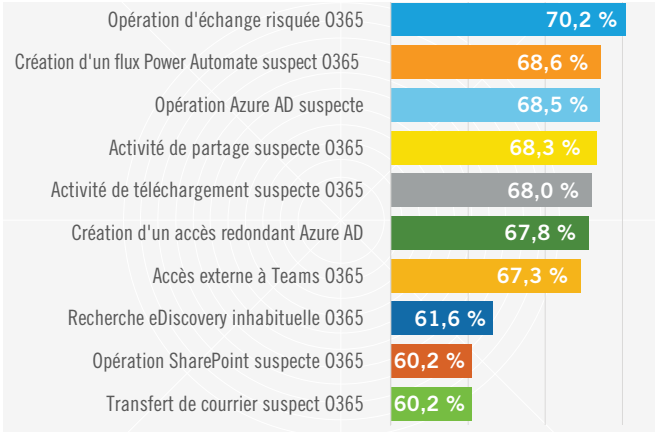
Certaines de ces détections de menaces sont déclenchées par des activités favorisant le confort d'utilisation, la collaboration avec les intervenants externes ou encore le provisionnement d'un accès administrateur à l'environnement Azure AD.

Comparaison des détections par taille d'entreprise

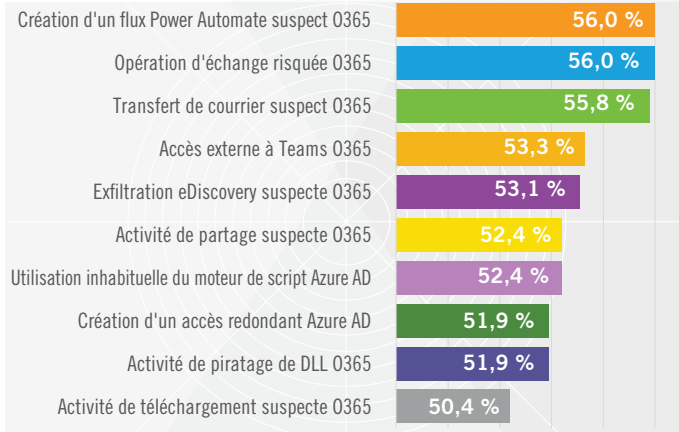
Les dix détections de menaces les plus fréquentes – Petite entreprise



Les dix détections de menaces les plus fréquentes – Moyenne entreprise



Les dix détections de menaces les plus fréquentes – Grande entreprise



Vectra a calculé la fréquence relative des détections de menaces déclenchées sur une période de trois mois en fonction de la taille de l'entreprise. Si l'on examine le classement des dix détections de menaces les plus fréquentes par taille d'entreprise (petite, moyenne et grande), on constate que plus l'entreprise est grande, plus le pourcentage de détections déclenchées par type de détection est faible. Cette tendance générale dans les grandes entreprises, qui enregistrent moins de détections que les entreprises de plus petite taille, peut indiquer que les utilisateurs et administrateurs des grandes entreprises effectuent des activités Azure AD et Office 365 plus fréquemment que ceux des entreprises de plus petite taille. Voici nos conclusions :

Il est possible que les utilisateurs et administrateurs des grandes entreprises effectuent des activités Azure AD et Office 365 plus fréquemment que ceux des entreprises de plus petite taille.

Similitudes entre les détections déclenchées par les petites et moyennes entreprises

Résultat : si l'on s'intéresse à la répartition des types de détection dans le classement pour chaque taille d'entreprise, on constate que les dix détections de menaces les plus fréquentes sont identiques pour les petites et moyennes entreprises, malgré un ordre différent. Les détections « Piratage de DLL Office 365 », « Utilisation inhabituelle du moteur de script Office 365 » et « Exfiltration eDiscovery suspecte Office 365 » font partie des dix détections les plus fréquentes dans les grandes entreprises, mais pas dans les moyennes ni les petites entreprises. Les dix détections les plus fréquentes dans les petites et moyennes entreprises incluent « Opération SharePoint suspecte Office 365 », « Recherche eDiscovery suspecte Office 365 » et « Opération Azure AD suspecte », ce qui n'est pas le cas dans les grandes entreprises.

Le stockage d'applications dans le cloud permet aux cybercriminels de remplacer ou d'injecter des DLL et des exécutables malveillants dans des partages régulièrement utilisés.

Analyse : nous pouvons en conclure que les utilisateurs qui accèdent aux applications stockées sur OneDrive ou SharePoint sont plus nombreux dans les grandes entreprises. Le stockage d'applications dans le cloud permet aux cybercriminels de remplacer ou d'injecter des DLL et des exécutables malveillants dans des partages régulièrement utilisés, ce qui se traduit par un accès plus fréquent à ces types de fichiers. Plus discrète, cette technique est nettement plus efficace pour les attaquants.

Détection des compromissions

Le fait que la détection « Recherche eDiscovery suspecte Office 365 » n'apparaisse pas dans le classement des dix détections les plus fréquentes dans les grandes entreprises, mais que la détection « Exfiltration eDiscovery suspecte Office 365 » y figure, indique que les utilisateurs qui effectuent ces types de recherches dans les grandes

entreprises ont recours à eDiscovery plus régulièrement et extraient des données de ces recherches plus fréquemment que dans les entreprises de plus petite taille. Une détection « Exfiltration eDiscovery suspecte Office 365 » est déclenchée à chaque fois qu'un compte prévisualise ou exporte des données à partir d'une recherche eDiscovery. L'accès à eDiscovery accorde aux cybercriminels un accès presque libre à tous les composants d'Office 365, ce qui leur permet d'effectuer des recherches et d'obtenir des informations en toute simplicité. Vectra a relevé un cas où eDiscovery était utilisé par un cybercriminel pour surveiller la réponse de l'équipe d'un centre SOC à sa présence sur le réseau interne. Sans Vectra, l'entreprise ne se serait pas rendu compte qu'un compte Office 365 était compromis et que le cybercriminel pouvait s'en servir pour infiltrer à nouveau le réseau après la correction de la compromission initiale.

La détection « Opération Azure AD suspecte » arrive respectivement en deuxième et troisième position du classement des détections les plus fréquentes dans les petites et moyennes entreprises.

Opération Azure AD suspecte : dans le trio de tête des détections de menaces les plus fréquentes dans les petites et moyennes entreprises

Résultat : la détection « Opération Azure AD suspecte » arrive respectivement en deuxième et troisième position du classement des détections de menaces les plus fréquentes dans les petites et moyennes entreprises. Elle désigne les modifications apportées à l'environnement qui peuvent être attribuées à un cybercriminel prenant le contrôle d'un compte et élevant les privilèges de ce dernier.

Analyse : cette détection ne figure pas dans le classement des dix détections de menaces les plus fréquentes dans les grandes entreprises, ce qui peut indiquer que l'administration d'Azure AD doit être plus régulière dans les grandes entreprises que dans celles de plus petite taille. Les entreprises de plus petite taille doivent donc examiner attentivement les alertes afin de s'assurer que les comportements inhabituels ne reflètent pas une action administrative malveillante suite à la prise de contrôle d'un compte d'utilisateur et à l'élévation de ses privilèges.

Opération d'échange risquée O365 : en tête du classement

Résultat : la détection « Opération d'échange risquée Office 365 » arrive en haut (si ce n'est en première place) du classement, quelle que soit la taille de l'entreprise.

Analyse : cette détection de menace est déclenchée par une activité préoccupante, qui peut aller de la collecte et de l'exfiltration d'informations sensibles à l'exécution de scripts, en passant par la mise en place d'un backdoor (porte dérobée). Comme nous l'avons vu dans une récente attaque majeure de la chaîne logistique, les cybercriminels ont l'habitude de cibler la messagerie des entreprises pour accéder à des informations sensibles. Le déclenchement de cette détection de menace indique qu'il est inhabituel pour le compte d'effectuer l'activité en question. Cela indique qu'un administrateur exécute occasionnellement ce genre de tâches ou qu'un cybercriminel manipule Exchange dans le service cloud pour accéder à des données ou permettre à une attaque de poursuivre sa progression.

Correspondance entre surfaces d'attaque et attaques de la chaîne logistique

Intéressons-nous à une récente attaque de la chaîne logistique et examinons comment les actions courantes ayant été exécutées par les cybercriminels dans l'environnement Azure AD sont détectées par Vectra. Dans cet exemple d'attaque, l'attaquant a exploité l'accès au produit largement déployé d'un éditeur pour infiltrer les réseaux locaux de nombreuses entreprises.

Les attaques de la chaîne logistique ont démontré qu'elles parvenaient à échapper aux contrôles préventifs faisant intervenir des sandbox réseau, l'analyse des terminaux et l'authentification multifacteur, notamment par les moyens suivants :

- Vérifications approfondies permettant aux cybercriminels de s'assurer qu'ils ne se trouvent pas dans une sandbox ou tout autre environnement d'analyse des malwares
- Utilisation de la signature de code et de processus légitimes pour échapper aux contrôles courants des terminaux
- Déploiement d'un nouvel injecteur en mémoire permettant d'échapper à l'analyse basée sur les fichiers lors de la distribution de la balise de commande et de contrôle (C&C)
- Contournement de l'authentification multifacteur à l'aide de clés de signature de session SAML (Security Assertion Markup Language) volées

Les compétences et la précision nécessaires pour contourner les contrôles des terminaux témoignent des récents progrès réalisés dans le domaine de la détection et de l'aide à la résolution des incidents (EDR). Il s'agit également d'une bonne piqûre de rappel : un cybercriminel déterminé et sophistiqué trouvera toujours un moyen de contourner les contrôles préventifs et l'analyse des terminaux.

Les attaques de la chaîne logistique ont démontré qu'elles parvenaient à échapper aux contrôles préventifs faisant intervenir des sandbox réseau, l'analyse des terminaux et l'authentification multifacteur.

Pour en savoir plus sur les attaques de la chaîne logistique, regardez cette vidéo qui étudie en détail une récente compromission.

Stratégies de contournement

Cette attaque spécifique de la chaîne logistique met en lumière une surface d'attaque que les entreprises ne sont pas en mesure de défendre.

Attaque de la chaîne logistique / Progression de SolarFlare du réseau jusqu'au cloud

1 Utilisation du backdoor (porte dérobée) SolarWinds (SUNBURST)

- Activation d'un mécanisme C&C initial avec une réponse DNS
- Téléchargement et mise en place d'un mécanisme C&C complet (Cobalt Strike)

2 Obtention d'un accès administrateur au domaine

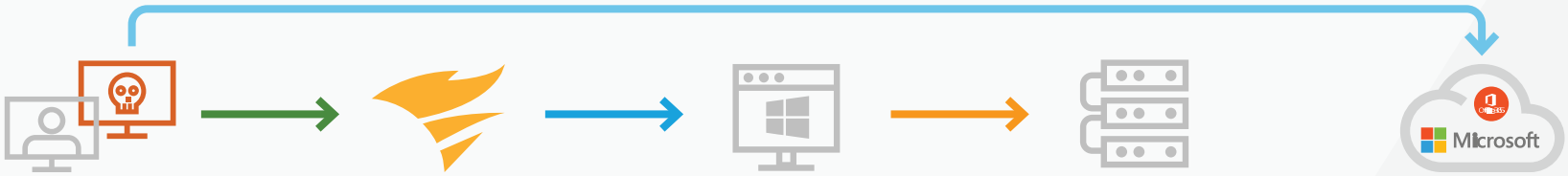
- Reconnaissance du réseau pour trouver des identifiants du domaine
- Déplacement latéral basé sur des identifiants à partir de SolarWinds

3 Vol d'un certificat de signature SAML

- Utilisation des identifiants administrateur du domaine pour accéder aux services ADFS

4 Accès à Microsoft Azure AD et à Office 365.

- Accès administrateur à Azure AD avec un ticket falsifié
- Établissement d'une persistance grâce à la modification des configurations et des autorisations
- Accès à la messagerie via des outils natifs



Analyse de l'étape 3 : Falsification de jetons pour accéder à Microsoft Azure AD et à Office 365

Dans de nombreux cas, le pirate a exploité cet accès pour infiltrer le service cloud de l'entreprise dans le but d'accéder à ses e-mails et à ses documents. Le déplacement latéral depuis l'environnement sur site vers le cloud est peu commun. En effet, les cybercriminels ont plutôt tendance à se déplacer dans la direction opposée. À l'instar d'un attaquant opérant sur le réseau local, le pirate a exécuté plusieurs actions qui relèvent de l'une des catégories suivantes : « Commande et contrôle (C&C) », « Déplacement latéral » ou « Exfiltration ».

L'une des premières opérations effectuées par ce cybercriminel a été de compromettre ou de modifier l'infrastructure d'authentification, ce qui lui a permis de falsifier des jetons SAML et d'accéder à l'environnement Azure AD et Office 365 en contournant l'authentification multifacteur et d'autres vérifications du niveau de sécurité. L'utilisation de jetons falsifiés pour se connecter déclenche la **détection « Connexion suspecte Azure AD »** par Vectra, qui entre dans la catégorie « Commande et contrôle (C&C) ». Cette détection de menace alerte les entreprises en cas de connexion inhabituelle par rapport à l'activité normale du compte. Dans notre analyse, cette détection ne figure pas dans le classement des dix détections de menaces les plus fréquentes.

Il apparaît donc qu'un accès inhabituel à l'environnement n'est pas fréquemment observé chez la plupart de nos clients et doit faire l'objet d'un examen encore plus approfondi en cas de détection. Enfin, la visibilité n'est pas seulement une question de données, mais aussi de contexte. Vous devez identifier les comportements à la fois suspects et bénéfiques aux cybercriminels, ce qui exige une compréhension des événements attendus et du schéma d'une attaque en cours.

Méthode alternative pour l'étape 3 : Modification de la relation de confiance

Pour contourner l'authentification, le cybercriminel peut également modifier la relation de confiance. Cette action implique de compromettre un compte disposant des droits requis ou d'attribuer ces droits à un compte déjà compromis. Dans ce dernier cas de figure, l'ajout des droits administrateur requis à un compte déclenche la **détection « Création d'un accès redondant Azure AD »**, qui entre également dans la catégorie « Commande et contrôle (C&C) ». La modification de la relation de confiance via un compte à privilèges déclenche la **détection « Opération Azure AD suspecte »**, qui entre dans la catégorie « Déplacement latéral ». Notre analyse montre que cette détection de menace figure dans le classement des dix détections les plus fréquentes, quelle que soit la taille de l'entreprise.

> Les actions mises en œuvre par le cybercriminel pointent vers un objectif commun : accéder aux informations contenues dans les e-mails et les documents.

Analyse de l'étape 4 : Accès aux informations contenues dans les e-mails

Les actions mises en œuvre par le cybercriminel pointent vers un objectif commun : accéder aux informations contenues dans les e-mails et les documents. Une fois l'accès établi, le pirate doit effectuer d'autres actions qui pourraient être considérées comme un déplacement latéral. Il semblerait que le cybercriminel ajoute les identifiants d'un compte compromis à des applications ou des principes de service existants. Cette action déclenche la **détection « Opération Azure AD suspecte »** que nous avons déjà évoquée.

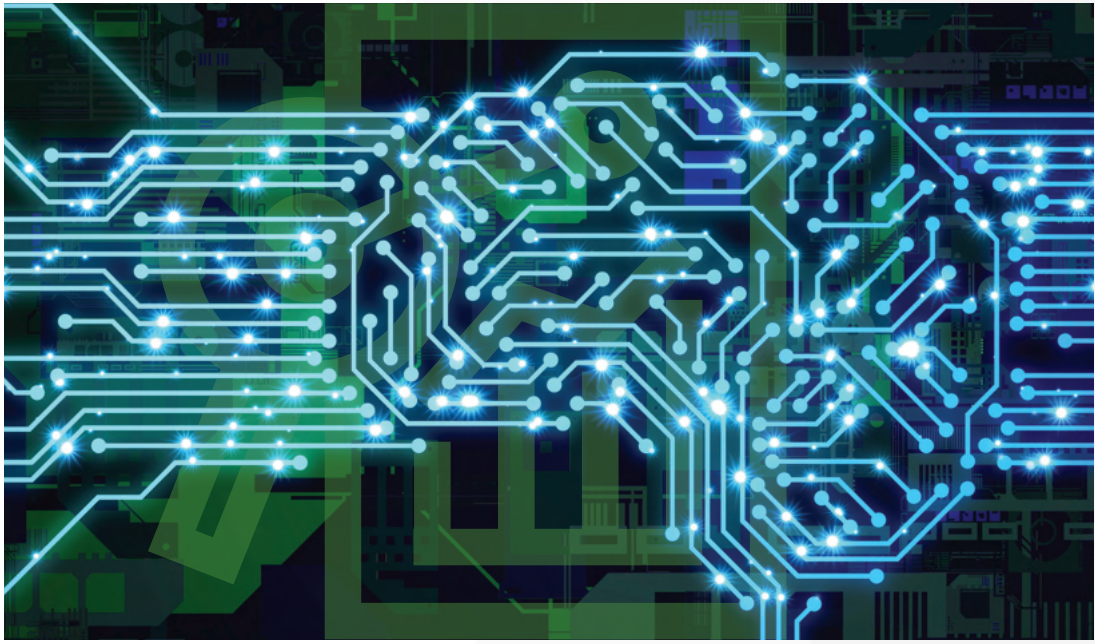
Dans certains cas, le pirate ajoute de nouvelles applications ou de nouveaux principes de service, ce qui accorde des autorisations aux applications souhaitées. Ce dernier cas de figure déclenche la **détection « Application OAuth suspecte Azure AD »**. Ces dernières activités mettent en lumière deux autres surfaces d'attaque qui doivent être surveillées de près par les clients afin d'obtenir une idée précise des modifications attendues et autorisées, et de celles qui ne le sont pas.

L'importance de connaître le comportement de vos comptes

Le scénario ci-dessus est devenu une réalité pour bon nombre d'entreprises qui ne savent pas faire la différence entre le comportement d'un attaquant et l'utilisation d'un compte à privilèges. La distinction entre les deux n'est pas évidente. C'est la principale raison pour laquelle 30 % des entreprises subissent des prises de contrôle de comptes d'utilisateur tous les mois. Comme nous l'avons mentionné précédemment, il s'agit également d'une bonne piqûre de rappel : un cybercriminel déterminé trouvera toujours le moyen de contourner les contrôles préventifs et l'analyse des terminaux. Encore une fois, l'essentiel est d'allier vision et visibilité : savoir reconnaître une utilisation autorisée et identifier les comportements que les pirates ont tendance à adopter. La bonne nouvelle, c'est que cette tâche n'est pas forcément aussi ardue qu'il n'y paraît.

Une technologie d'intelligence artificielle sophistiquée peut vous aider à combler les failles de vos comptes Azure AD et Office 365 afin que vous disposiez des données appropriées pour détecter tout comportement sortant de l'ordinaire. Réfléchissez aux dix détections de menaces les plus fréquentes que nous avons évoquées : recevez-vous une alerte en cas de téléchargement ou de transfert d'une pièce jointe suspecte, ou lorsqu'une opération risquée ou suspecte survient dans votre cloud ? Si la réponse est non, vous pouvez probablement optimiser votre stratégie.

Pour savoir comment détecter tout comportement sortant de l'ordinaire dans votre environnement Azure AD ou Office 365, consultez la page dédiée à Cognito Detect pour Office 365.



Une technologie d'intelligence artificielle sophistiquée peut vous aider à combler les failles de vos comptes Azure AD et Office 365 afin que vous disposiez des données appropriées pour détecter tout comportement sortant de l'ordinaire.

E-mail : info_france@vectra.ai vectra.ai