Prevention First

Menaces par email :

Pourquoi la protection native de Microsoft 365 et de Google Workspace n'est pas suffisante

Digital Security
Progress. Protected.

Protection insuffisante de la messagerie

Les entreprises font partie des 3 milliards d'utilisateurs de Google Workspace (dont 1,8 milliard d'utilisateurs actifs de Gmail), 400 millions d'utilisateurs d'Outlook, ou des 320 millions d'utilisateurs de l'application de collaboration Microsoft Teams, qui sont tous des outils professionnels numériques essentiels afin de répondre aux nouvelles habitude de travail.

Après un déploiement réussi et la mise en place de certaines règles de sécurité, les équipes des entreprises devraient idéalement se concentrer sur les tâches critiques tout en travaillant dans des environnements de collaboration sécurisés.

Ce n'est pas nécessairement le cas. **De nombreux auteurs de menaces détournent des applications cloud légitimes** mais il existe bien heureusement une solution à ce problème. Les responsables informatiques doivent mettre en place des couches de sécurité supplémentaires.

Avec les bons outils, les administrateurs peuvent minimiser la surface d'attaque de leurs services cloud, en adoptant une approche de prévention qui protège les applications de collaboration et la messagerie de l'entreprise contre les menaces avant qu'elles ne s'exécutent.

Les menaces liées à la messagerie sont les principaux grands défis auxquels les entreprises sont confrontées pour la protection des applications dans le cloud :

HAMEÇONNAGE

Les attaquants utilisent des méthodes innovantes, notamment des QR Code et des homoglyphes, pour tromper leurs cibles et les inciter à scanner et/ou à cliquer sur des liens apparemment légitimes.

USURPATION DES IDENTITÉS ET DE LA MESSAGERIE PROFESSIONNELLE

Des emails tentent de tromper leurs destinataires en leur faisant croire qu'un expéditeur légitime communique avec eux. Ces emails s'améliorent de jour en jour, en particulier avec l'utilisation croissante des technologies d'IA.

FACTEUR HUMAIN

Les collaborateurs commettent des erreurs, ce qui rend les passerelles de messagerie particulièrement attrayantes pour les attaquants. Les formations à la cybersécurité sont toujours d'actualité car le facteur humain reste le maillon le plus faible de la chaîne et aucune technologie ne peut fonctionner à 100 % si elle n'est pas utilisée correctement.

MENACES ZERO-DAY

L'IA permet également aux adversaires de créer plus facilement de nouvelles menaces inédites.

Messagerie : le terrain de jeu préféré des criminels

La messagerie reste le principal vecteur de cybermenaces. Ces dernières années, ESET a détecté et bloqué des millions de menaces qui ont réussi à contourner la protection native de Microsoft 365 et de la suite Google Workspace dans le cloud.

La majorité des menaces bloquées étaient des messages d'hameçonnage et de spam. Selon Verizon, le temps moyen nécessaire aux utilisateurs pour se faire piéger par des emails d'hameçonnage était inférieur à 60 secondes. Son rapport d'enquête de 2024 sur les failles de sécurité des données affirme que l'ingénierie sociale sophistiquée est l'une des techniques d'attaque les plus utilisées. Son nombre a presque doublé entre 2022 et 2023 et, aujourd'hui, l' ingénierie sociale sophistiquée est impliquée dans environ 20 % de toutes les attaques à but lucratif. La majorité des incidents d' ingénierie sociale sophistiquée se sont traduits par une compromission des emails d'entreprise (BEC), avec un montant moyen de transactions d'environ 50 000 $, selon l'ensemble de données IC3 du FBI. Les toutes dernières données montrent que cette tendance n'est pas près de diminuer.

Selon le rapport d'ESET sur les menaces du second semestre 2024, la détection des spams a augmenté de 19 %, et les fichiers HTML malveillants qui renvoient les victimes vers des sites d'hameçonnage (HTML/Phishing.Agent trojan) restent de loin la menace la plus répandue pour la messagerie. Dans l'ensemble, ces **attaques par email représentent près d'un quart (23,8 %) de toutes les cybermenaces** détectées par ESET. Différents types de malwares, tels que les portes dérobées, les logiciels espions, les infostealers et les downloaders font partie des autres menaces détectées par la télémétrie ESET.

Manque de protection

Bien que Microsoft et Google aient intégré une sécurité directement dans leurs applications dans le cloud, qui sont toutes deux protégées et régulièrement mises à jour, cela ne signifie pas qu'elles sont à l'abri de toutes les menaces existantes.

Des exemples concrets montrent que des applications et des services cloud légitimes peuvent être détournés pour diffuser des malwares, dissimuler des processus malveillants et permettre l'accès à distance aux appareils d'entreprise :

- Les chercheurs d'ESET ont remarqué de nouvelles campagnes d'hameçonnage par email menées par un acteur inconnu et ciblant des entreprises dans les pays européens au cours des dernières années. Les emails contenaient des pièces jointes malveillantes s'appuyant sur AceCryptor, un malware de chiffrement sous forme de services conçu pour dissimuler d'autres malwares. S'ils parviennent à échapper aux outils de cybersécurité, les attaquants peuvent déployer l'outil d'accès à distance de Rescoms (également appelé Remcos) et espionner leurs victimes.

- Dans la seconde moitié de 2024, **Formbook, un infostealer** découvert pour la première fois en 2016, a connu une résurgence significative, avec des taux de détection augmentant de plus de 200 %. Ce malware collecte entre autres les données du presse-papiers, les frappes au clavier, des captures d'écran et les données du navigateur mises en cache. Il s'agit d'un malware sous forme de services (MaaS), vendu sur des forums clandestins, qui se propage via des pièces jointes malveillantes dans des emails d'hameçonnage. Les produits ESET ont protégé près de 34 000 utilisateurs contre ce malware, principalement en Europe centrale et de l'Est, ainsi qu'au Japon, au Canada et en Espagne.

- Heureusement, dans la plupart des cas, les professionnels de la cybersécurité découvrent les vulnérabilités plus tôt que les auteurs de menaces. En juin 2023, la Red Team de Jumpsec, un prestataire de services de sécurité basé au Royaume-Uni, a découvert et démontré un moyen de diffuser des malwares à l'aide de Microsoft Teams via un compte situé en dehors de l'organisation cible. L'équipe de Jumpsec **a contourné la protection intégrée** et a réussi à faire croire au système qu'un utilisateur externe était en fait un compte interne.

ESET, l'un des principaux fournisseurs de cybersécurité, utilise ESET Cloud Office Security pour protéger les environnements de collaboration dans le cloud.

Cette solution avancée renforce les fonctions de sécurité intégrées de Microsoft 365 et de Google Workspace en effectuant des analyses après que les produits de bureautique dans le cloud aient marqué les emails ou les fichiers comme étant « sains ».

Les données suivantes* d'ESET montrent combien de menaces sont parvenues à franchir les défenses natives.

920 000

menaces détectées contre la messagerie

813 000

emails d'hameçonnage bloqués

110 000

menaces hors messagerie provenaient de OneDrive, SharePoint, Teams et Google Drive

75 820 000

emails de spam capturés

*Données ESET janv-nov 2024

Comment améliorer les défenses du cloud

Il est clair que la sécurité native des applications dans le cloud ne suffit pas. Pour minimiser cette surface d'attaque croissante, prévenir et atténuer les attaques avant qu'elles ne fassent des dégâts, les entreprises devraient envisager d'améliorer les contrôles intégrés de Microsoft ou de Google en y ajoutant des **couches de protection supplémentaires** :

Filtrage antispam

Les messages de spam représentaient plus de 46,8 % des 362 milliards d'emails échangés quotidiennement dans le monde en 2024. Avec la bonne solution de filtrage, les entreprises peuvent faire gagner beaucoup de temps à leurs collaborateurs et éviter les problèmes liés aux spams malveillants.

Anti-hameçonnage

En 2024, l'hameçonnage a été identifié comme le vecteur d'attaque initial dans 22 % des cyberattaques auxquelles les entreprises américaines étaient confrontées. Il est absolument essentiel de disposer d'un outil automatisé qui reconnaisse les liens d'hameçonnage joints aux emails.

Analyse anti-malwares

Une bonne solution de sécurité pour le cloud devrait automatiquement rechercher tout fichier nouveau ou modifié dans le stockage partagé afin d'empêcher les malwares de s'exécuter ou de se propager.

Sandbox et analyse comportementale

Avec l'apparition constante de nouvelles menaces, les outils automatisés de cybersécurité doivent être préparés à des attaques inédites. Cela peut se faire grâce à une analyse approfondie des comportements des échantillons suspects dans une sandbox isolée et sécurisée.

Antispoofing et moteur de règles

Il est nécessaire de stopper les emails indésirables qui masquent leur propre identité et se font passer pour un expéditeur légitime. Grâce à ce contrôle, seuls les emails provenant de sources fiables sont réellement légitimes et autorisés.

Protection contre les homoglyphes

Les attaquants utilisent des caractères ressemblants pour créer des adresses emails ou des domaines trompeurs qui semblent légitimes. La détection et le blocage de ces attaques homoglyphes permettent de prévenir l'hameçonnage et d'autres activités malveillantes, garantissant ainsi la sécurité des communications de votre organisation.

Récupération des emails

Cette fonction renforce la sécurité en permettant aux administrateurs de mettre en quarantaine des emails directement à partir du journal des analyses. Ce faisant, les emails sont transférés hors de la boîte mail des destinataires, ce qui permet une action immédiate en cas d'attaque présumée, notamment d'hameçonnage.

Comment ESET vous aide

Disposer d'un grand nombre d'outils et gérer un système de sécurité robuste peut ressembler à n'importe quel autre défi, mais la mise en place d'une sécurité supplémentaire ne doit pas nécessairement accroître la complexité du travail d'un administrateur informatique.

ESET Cloud Office Security offre une protection préventive avancée pour les applications Microsoft 365 et Google Workspace avec toutes les fonctionnalités mentionnées ci-dessus. Il améliore la posture de sécurité d'une organisation grâce à une protection avancée contre les menaces, ainsi qu'à la visibilité et au contrôle de la messagerie, du partage de fichiers et des outils de données et de collaboration dans le cloud. En plus de rationaliser les opérations et renforcer la sécurité, ESET Cloud Office Security contribue à **réduire la complexité en centralisant et en automatisant les processus de routine** tels que :

- Les nouveaux utilisateurs dans l'environnement professionnel n'ont pas besoin d'être ajoutés manuellement par un administrateur dans une console ; ils sont automatiquement protégés après la création de leur compte.
- Les administrateurs peuvent définir des intervalles de notification pour éviter la lassitude associée aux alertes tout en veillant à ce qu'ils reçoivent les notifications les plus importants.
- Les fichiers suspects peuvent être facilement gérés dans une quarantaine centralisée avec la possibilité de les libérer/supprimer ou de les examiner plus en détail séparément au besoin.

- La solution permet une gestion multi-tenant couvrant des dizaines de milliers d'utilisateurs de comptes créés dans les deux plateformes les plus utilisées : Microsoft 365 et Google Workspace.

Avec un focus sur la prévention et la protection des utilisateurs et de leurs appareils, ESET Cloud Office Security garantit des niveaux élevés de protection contre les menaces en minimisant la surface d'attaque du cloud, allégeant ainsi la charge pour les administrateurs grâce à une console d'administration cloud facile d'emploi.

Proposé en tant que solution autonome ou intégrée à la plateforme ESET PROTECT, ESET Cloud Office Security protège les organisations contre les infections, minimise les interruptions de travail dues aux messages non sollicités et bloque les attaques ciblées ainsi que des types de menaces jamais vus auparavant, en particulier des ransomwares.

INTÉGRATION

Enfin, **ESET LiveGuard Advanced**, une technologie cloud qui utilise l'analyse avancée, l'IA, le sandboxing cloud et l'analyse approfondie des comportements pour prévenir les attaques ciblées ainsi que les menaces nouvelles ou inconnues, notamment les ransomwares, est gratuitement intégré à ESET Cloud Office Security.

À propos d'ESET

Défense proactive.
Notre activité consiste à minimiser la surface d'attaque.

Prenez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre approche préventive reposant sur l'IA et l'expertise humaine.

Bénéficiez d'une protection de haut niveau grâce à notre Threat Intelligence interne, compilée et examinée depuis plus de 30 ans, qui alimente notre vaste réseau de R&D dirigée par des chercheurs reconnus. ESET protège votre organisation afin qu'elle puisse maximiser le potentiel de la technologie.

EN SAVOIR PLUS

Prévention multicouche

IA de pointe associée à une expertise humaine

Threat Intelligence de renommée mondiale

Support hyperlocal et personnalisé

eset®
Digital Security
Progress. Protected.