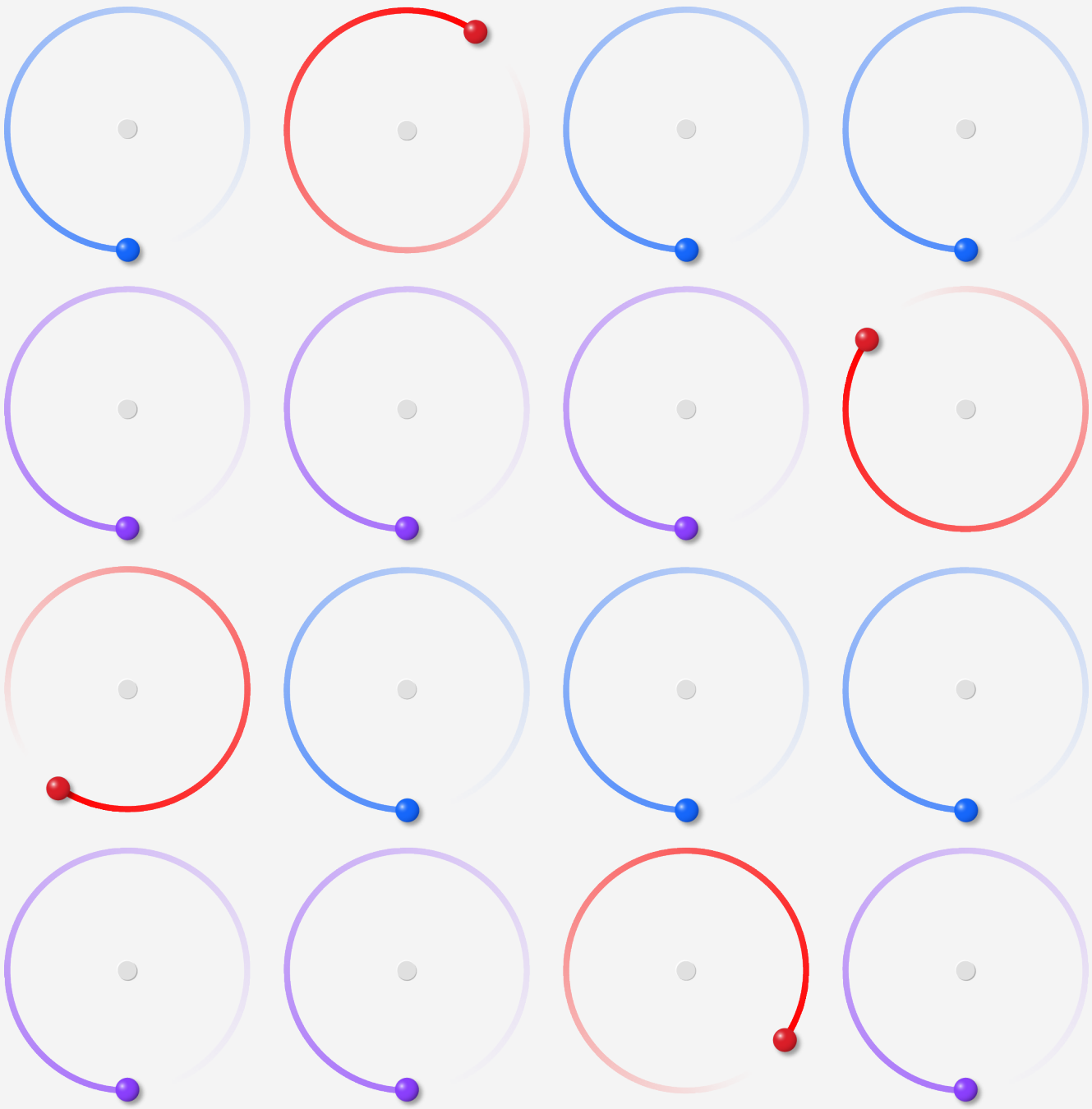
X-Force Cloud Threat Landscape Report 2024



IBM

Table des matières

Introduction

Alors que le marché du cloud computing devrait atteindre environ 600 milliards de dollars en 2024, l'adoption de l'infrastructure cloud continue de progresser. Les entreprises déplacent de plus en plus de données critiques d'un environnement sur site vers l'infrastructure et les services cloud, motivant le besoin de mesures défensives appropriées et la nécessité de sécuriser les données dans le cloud. Les entreprises cherchent également à maximiser la valeur de leurs investissements dans le cloud et à tirer parti du potentiel de l'IA. Pour y parvenir, elles doivent donc adopter une approche intentionnelle.

Pour les organisations opérant une migration vers le cloud, la transformation est un processus en plusieurs étapes qui demande du temps, de l'énergie et des ressources. Le Rapport 2024 sur le coût d'une violation de données a révélé qu'environ 40 % de toutes les violations impliquaient des données distribuées dans des environnements multiples, tels que les clouds publics, les clouds privés et les environnements sur site. Par conséquent, dans le cadre du processus de migration, il est essentiel que les organisations élaborent et mettent en œuvre des stratégies de sécurité appropriées et de bonnes pratiques pour protéger leurs actifs clés.

Comprendre le paysage des menaces liées au cloud et ses impacts potentiels sur les activités est essentiel tant pour le service informatique que pour la direction. Cet éclairage permet de prendre des mesures proactives pour limiter l'exposition et protéger les informations et les ressources critiques de l'entreprise, garantissant ainsi un parcours de transformation cloud fluide et sûr, ainsi que la réussite des futures mises en œuvre.

L'équipe d'IBM X-Force est bien placée dans le domaine de la sécurité pour fournir aux organisations des bonnes pratiques et des stratégies sectorielles pour les accompagner dans leur parcours cloud. Pour sa cinquième édition, le rapport X-Force Cloud Threat Landscape offre une perspective mondiale intersectorielle sur la manière dont les acteurs de la menace compromettent les environnements cloud, les activités malveillantes qu'ils mènent une fois dans les réseaux compromis et l'impact que celles-ci ont sur les organisations.

Pour produire ce rapport, X-Force a rassemblé et analysé des données compilées de juin 2022 à juin 2024 à partir des sources suivantes :[1]

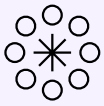
- IBM X-Force Threat Intelligence
- Tests de pénétration IBM X-Force Red, services de simulation d'adversaires et de gestion des vulnérabilités
- Engagements de réponse aux incidents (IR) IBM X-Force
- Red Hat Insights
- Analyse du dark web par X-Force avec des données fournies par le contributeur du rapport Cybersixgill

Points essentiels à retenir

Lors de la collecte et de l'analyse des données, X-Force a révélé les risques de sécurité les plus courants pesant sur les organisations de la part d'acteurs de la menace au cours de leur parcours cloud. Voici les points essentiels à retenir.

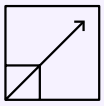
Le cross-site scripting (XSS) arrive en tête des vulnérabilités et expositions courantes (CVE) les plus importantes

- Les vulnérabilités XSS représentent 27 % des CVE nouvellement découvertes au cours de la période étudiée, ce qui pourrait permettre aux acteurs de la menace de dérober des jetons de session ou de rediriger les utilisateurs vers des pages Web malveillantes.



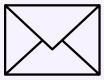
La demande d'identifiants cloud se maintient sur le dark web malgré la saturation du marché

- Bien que les mentions globales de plateformes SaaS sur les places de marché du dark web aient diminué d'environ 20 % par rapport à 2023, l'obtention d'un accès à l'aide d'identifiants cloud compromis est le deuxième vecteur d'attaque initiale le plus courant.
- Le prix moyen des identifiants d'accès au cloud compromis a connu une baisse constante, passant de 11,74 USD en 2022 à 10,23 USD en 2024, soit une baisse globale de 12,8 % sur une période de trois ans.



L'utilisation de services d'hébergement de fichiers basés sur le cloud à des fins d'activités malveillantes est en hausse

- Les acteurs de la menace exploitent de plus en plus les services de confiance basés sur le cloud, tels que Dropbox, OneDrive et Google Drive, pour les communications de commande et de contrôle et la distribution de logiciels malveillants.
- Des groupes parrainés par l'État nord-coréen, dont APT43 et APT37, ont mené des attaques en plusieurs étapes contre des services basés sur le cloud afin de distribuer des chevaux de Troie d'accès à distance (RAT).



Le phishing est le principal vecteur d'accès initial

– L'hameçonnage représente 33 % de tous les incidents liés au cloud auxquels X-Force a répondu au cours des deux dernières années, les attaquants utilisant souvent le phishing pour collecter des identifiants par le biais d'attaques AITM (adversary-in-the-middle).

Les identifiants valides sont fréquemment exploités

– 28 % des incidents liés au cloud ont impliqué l'utilisation d'identifiants vérifiés pour pénétrer dans l'environnement des victimes. Souvent, ces comptes sont sur-privilégiés, les utilisateurs ayant plus de privilèges que nécessaire pour mener à bien leurs tâches, posant ainsi un problème de sécurité majeur pour les organisations.

La compromission des e-mails professionnels (BEC) cible les identifiants

– Les attaques BEC, où les attaquants usurpent des comptes de messagerie électronique en se faisant passer pour une personne de l'organisation victime ou d'une autre organisation de confiance, représentent 39 % des incidents au cours des deux dernières années. Les acteurs de la menace tirent généralement parti des identifiants récoltés lors d'attaques de phishing pour s'emparer de comptes de messagerie et mener d'autres activités malveillantes.

Les défauts de conformité nuisent à la sécurité des environnements cloud des clients

– La première règle de sécurité à ne pas avoir été respectée dans les environnements 100 % cloud concerne la mauvaise configuration des paramètres essentiels de sécurité et de gestion dans les systèmes Linux.

– La première règle de sécurité à ne pas avoir été respectée dans les environnements qui comportent au moins 50 % de systèmes basés dans le cloud concerne l'absence de pratiques d'authentification et de cryptographie cohérentes et sûres.

Vulnérabilités liées au cloud

À la suite de l'analyse de l'année dernière, X-Force a classé les nouvelles CVE en fonction de l'impact potentiel qu'elles auraient si elles étaient exploitées avec succès. X-Force a ainsi observé que le recueil d'informations, l'obtention d'un accès et l'acquisition de privilèges constituent les trois principaux impacts des CVE découvertes au cours de la précédente période étudiée. Cette année, le XSS, l'obtention d'un accès et le recueil d'informations représentent les trois principaux impacts des CVE découvertes. Cette comparaison d'une année sur l'autre met en évidence un changement dans les types de vulnérabilités révélées, le XSS apparaissant comme une menace potentiellement importante. Voir la figure 1.

L'exploitation des vulnérabilités est l'un des principaux vecteurs d'accès initial pour les attaquants. Par exemple, le XSS peut être utilisé pour dérober des jetons de session ou rediriger les utilisateurs vers des pages Web malveillantes, tandis que l'obtention d'un accès peut conduire à d'autres exploitations des ressources cloud. En fin de compte, cette exploitation peut entraîner le déploiement de cryptomineurs, d'infostealers, de ransomwares et d'autres types de logiciels malveillants permettant d'atteindre des objectifs malintentionnés.

Impact des CVE

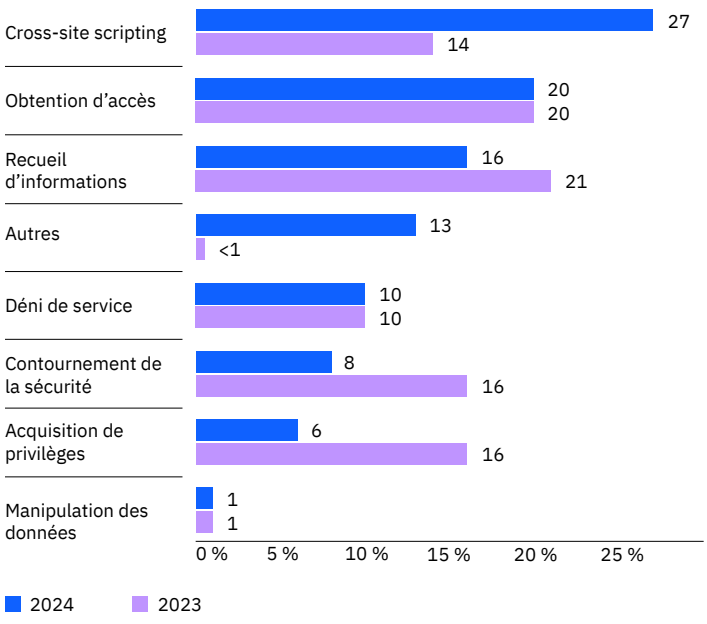


Figure 1. Le XSS est le premier impact des CVE. Source : X-Force

Cloud et dark web

Pour le rapport de cette année, les chercheurs de X-Force se sont à nouveau associés à Cybersixgill pour comprendre comment les cybercriminels exploitent les environnements et les infrastructures cloud sur le dark web. Pour ce faire, X-Force a analysé les données de Cybersixgill, extraites de divers forums et places de marché du dark web entre juin 2023 et juin 2024, afin d'éclairer l'analyse suivante.

X-Force a observé une baisse constante du prix moyen des identifiants d'accès au cloud sur le dark web, passant de 11,74 USD en 2022 à 10,68 USD en 2023 et 10,23 USD en 2024, soit une baisse globale de 12,8 % depuis 2022. Voir la figure 2.

Cette tendance pourrait indiquer que le marché des identifiants cloud compromis connaît une sursaturation, entraînant une dévaluation des identifiants. Les organisations se tournent de plus en plus vers le cloud, ce qui signifie que davantage d'identifiants sont susceptibles d'être dérobés ou compromis, augmentant ainsi le volume global d'identifiants d'accès au cloud à vendre. En outre, chaque année, les mesures de sécurité défensives pour l'infrastructure cloud s'améliorent, notamment la vitesse de détection et les capacités de réponse, rendant ces identifiants moins efficaces et, par conséquent, moins précieux.

Prix moyen des identifiants d'accès au cloud

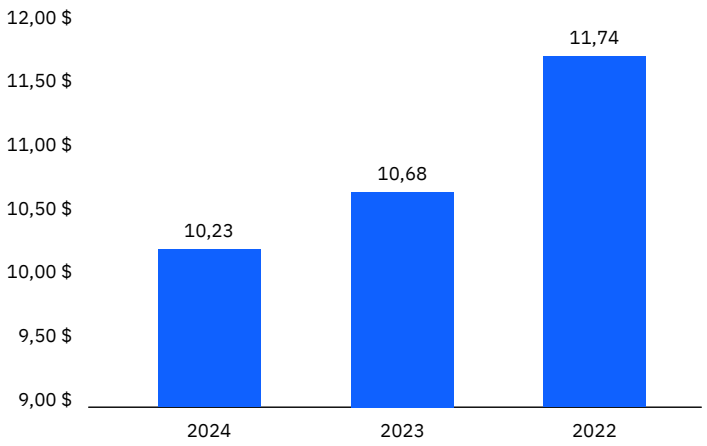


Figure 2. Depuis 2022, le prix des identifiants d'accès au cloud a baissé de 12,8 %. En dollars américains. Source : Cybersixgill

Alors que l'accès aux identifiants cloud compromis continue d'être un actif à vendre populaire sur les places de marché du dark web, en particulier en ce qui concerne les solutions SaaS basées sur cloud, les mentions globales des plateformes SaaS sur les places de marché du dark web ont diminué en moyenne de 20,4 % par rapport à 2023. Voir la figure 3.

La diminution des mentions de ces solutions SaaS sur le dark web suggère une tendance positive du point de vue de la sécurité défensive. Cette baisse s'explique probablement par les mesures prises par les autorités ainsi que par les perturbations des places de marché du dark web, qui peuvent avoir un impact considérable sur la disponibilité d'identifiants dérobés et d'autres annonces. Des démantèlements très médiatisés, comme celui de la place de marché Nemesis, mettent en évidence cette conséquence. En outre, à mesure que la sécurité des solutions SaaS s'améliore, les attaquants sont susceptibles de commencer à chercher des alternatives plus faibles pour réaliser des profits et mener des activités malveillantes. Les organisations doivent continuer à donner la priorité à la sécurité, à investir dans des technologies de pointe et à favoriser une culture de sensibilisation et de préparation à la sécurité pour préserver cette évolution.

- Les recherches menées par X-Force indiquent que Microsoft Outlook est la solution SaaS la plus fréquemment mentionnée sur les places de marché du dark web, avec 68 %, loin devant Zoom avec 7 %.

- Le nombre global de mentions pour chaque plateforme SaaS sur les places de marché du dark web a considérablement diminué par rapport à 2023, à l'exception de Microsoft TeamViewer, qui a augmenté de 9 %. Malgré cette légère augmentation, elle ne représente que 1,8 % du total des discussions concernant les solutions SaaS.

- Notamment, la diminution la plus importante des discussions sur la place de marché concerne Wordpress-Admin (98 %), suivi de Microsoft Active Directory (44 %) et de ServiceNow (38 %).

Plusieurs facteurs peuvent expliquer la baisse significative des mentions des plateformes SaaS précédemment citées sur le dark web. L'évolution des tactiques, techniques et procédures (TTP) des acteurs de la menace, l'absence potentielle de retour sur investissement (ROI) et les mesures de sécurité renforcées prises par les entreprises, telles que la mise en œuvre d'un chiffrement avancé, d'une authentification par étapes (MFA) et d'une gestion robuste des correctifs, ont considérablement réduit les vulnérabilités et l'exploitabilité de ces solutions.

Les solutions SaaS les plus mentionnées sur le dark web

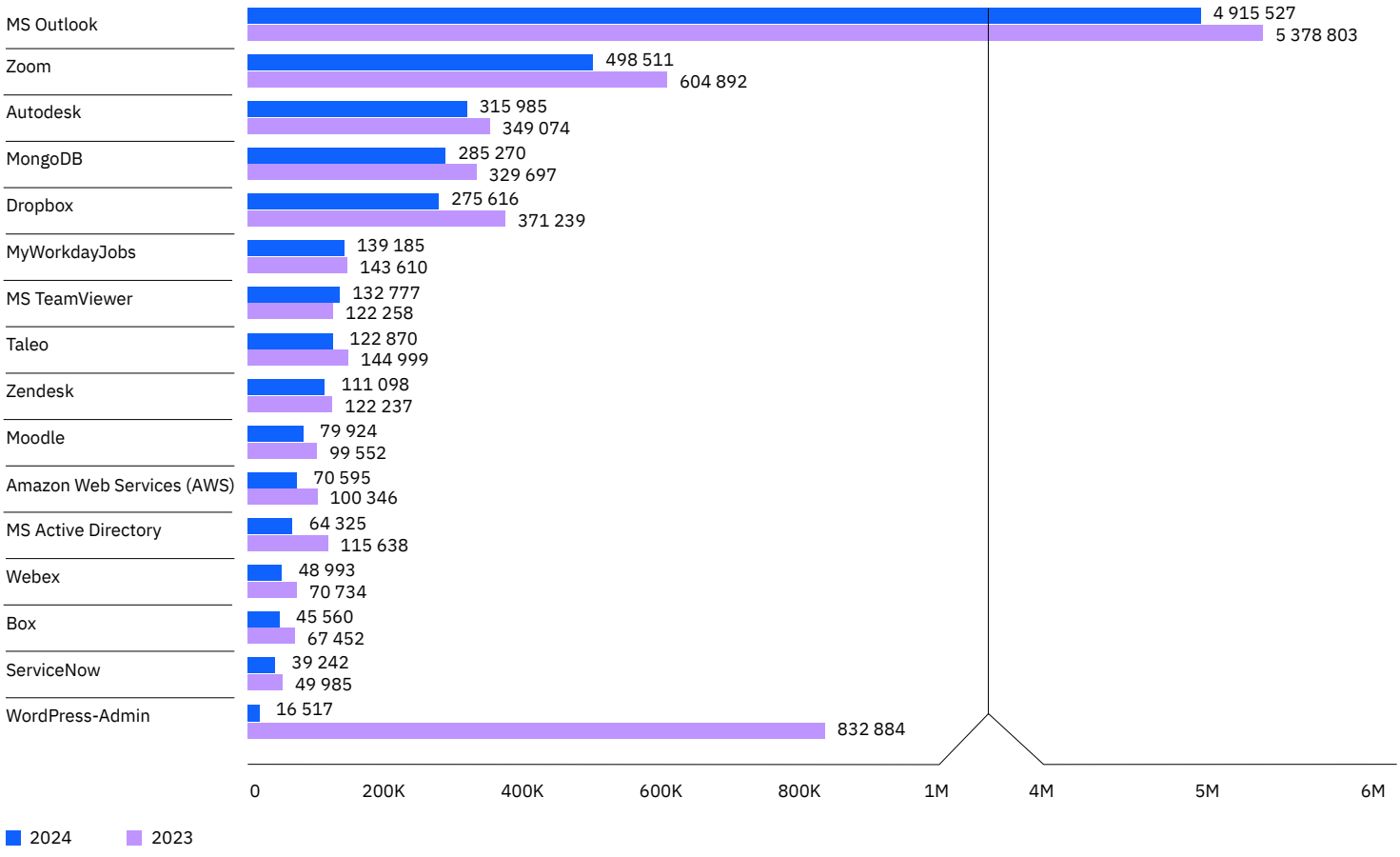


Figure 3. Les solutions SaaS les plus mentionnées sont basées sur les discussions de la place de marché du dark web. Source : Cybersixgill

Les infostealers les plus mentionnés sur le dark web

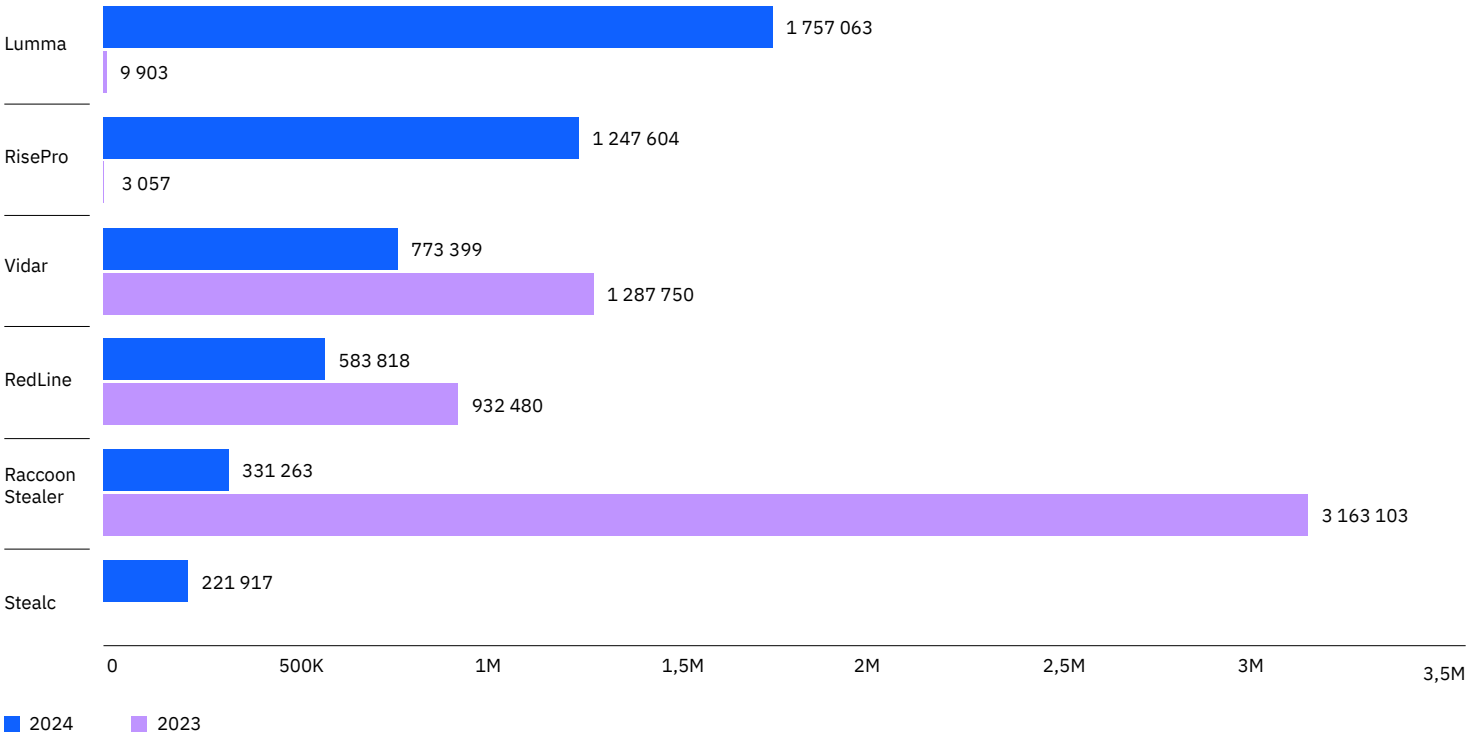


Figure 4. Les infostealers les plus mentionnés sont basés sur les discussions de la place de marché du dark web. Source : Cybersixgill

X-Force a constaté que Lumma, RisePro et Vidar étaient les infostealers les plus populaires vendus sur le dark web en 2024. En comparaison, les principaux infostealers en 2023 étaient Raccoon Stealer, Vidar et RedLine. Plus particulièrement, Lumma et RisePro n'ont eu que peu ou pas d'activité sur le dark web en 2023, tandis que Vidar était le deuxième infostealer le plus populaire cette année-là. En outre, Raccoon Stealer était de loin l'infostealer le plus populaire avec plus de 3 millions de mentions en 2023, mais ce chiffre a chuté de manière drastique en 2024 pour atteindre seulement 300 000 mentions. Voir la figure 4.

Au cours de l'année écoulée, la collaboration internationale entre les services répressifs a permis de démanteler d'importants réseaux cybercriminels distribuant Raccoon Stealer. En outre, l'émergence de nouveaux infostealers tels que Lumma et RisePro a détourné l'attention des acteurs de la menace, réduisant ainsi la popularité de Raccoon Stealer.

Plus particulièrement, alors que Lumma et RisePro n'avaient que peu ou pas d'activité sur le dark web en 2023, ils sont devenus les deux infostealers les plus vendus sur le dark web en 2024.

Cibler les services, les plateformes et les SaaS d'hébergement de fichiers basés sur le cloud

L'analyse de plusieurs simulations d'adversaires menées par X-Force Red a révélé une utilisation croissante des services basés sur le cloud pour les communications de type commande et contrôle, une hausse qui s'explique par la confiance accordée par les organisations à ces services et par le fait que ces derniers se fondent parfaitement dans le trafic habituel de l'entreprise. Les adversaires reconfigurent les ressources basées sur le cloud pour faciliter la réalisation de leurs objectifs et s'octroyer des privilèges élevés.

En outre, X-Force a observé que les services basés sur le cloud étaient ciblés de deux manières :

Services d'hébergement de fichiers dans le cloud : distribution de logiciels malveillants

X-Force a continué à suivre les acteurs de la menace et à observer qu'ils utilisent largement les services d'hébergement de fichiers basés dans le cloud, tels que Dropbox, OneDrive et Google Drive, pour distribuer des logiciels malveillants qui semblent légitimes.

Trois campagnes notables de logiciel malveillant dont deux émanant de groupes soutenus par l'État nord-coréen :

- APT43, qui utilise Dropbox pour faciliter une campagne d'attaque en plusieurs étapes impliquant un logiciel malveillant connu sous le nom de TutorialRAT.
- APT37, qui a mené une vaste campagne de phishing en utilisant OneDrive pour distribuer RokRAT, un logiciel malveillant.

La troisième campagne notable est une campagne de spam par e-mail utilisant OneDrive pour héberger et distribuer le logiciel malveillant Bumblebee. Ces campagnes sont parvenues à exploiter la nature fiable des services de cloud public en contournant les mesures de sécurité traditionnelles et en distribuant efficacement des logiciels malveillants à des utilisateurs peu méfiants.

Services et plateformes cloud : infostealers, cryptomineurs et ransomware

On observe en 2024 une tendance constante des vols d'identifiants par des infostealers spécialement conçus pour exfiltrer les identifiants des services cloud. De nombreux infostealers populaires, tels que RedLine, Raccoon Stealer, Vidar, Lumma, MetaStealer et Stealc, ainsi que différents outils de piratage, tels que FBot, AlienFox et Legion, ont ciblé les plateformes cloud. Ces plateformes comprennent AWS, Microsoft Azure, Google cloud et d'autres solutions SaaS, telles qu'Office 365, Google Workspace (anciennement G suite) et Salesforce.

Ces infostealers et outils de piratage ont été utilisés pour dérober des identifiants spécifiques à des plateformes et à des services, notamment :

- Les **identifiants d'infrastructure cloud**, comme AWS Identity and Access Management (IAM), Microsoft Azure Active Directory, Google cloud IAM et Snowflake, contrôlent l'accès aux ressources cloud, telles que les machines virtuelles, le stockage et les bases de données.
- Les **identifiants de stockage cloud**, comme Dropbox, Box et Microsoft OneDrive, permettent aux pirates d'exfiltrer des fichiers et des documents sensibles.
- Les **services de messagerie électronique basés sur le cloud**, comme Office 365 et Gmail, contiennent des données de communication précieuses et peuvent être utilisés pour les procédures de réinitialisation des mots de passe pour d'autres services cloud.
- Les **identifiants d'outils de collaboration basés sur le cloud** sur des plateformes comme Microsoft Teams, Slack ou Google Workspace, où des informations sensibles sont souvent partagées entre les membres d'équipe, sont souvent ciblés.
- Les **plateformes de développement basées sur le cloud**, comme Wordpress, GitHub, GitLab et Bitbucket, sont utilisées pour voler des identifiants permettant d'accéder à des référentiels de code source, ce qui peut permettre d'obtenir du code propriétaire ou des informations de développement sensibles.
- Les **systèmes de gestion de la relation client (CRM) basés sur le cloud**, comme Salesforce, contiennent une multitude de données client. Des identifiants dérobés peuvent permettre un accès non autorisé à des informations précieuses sur les clients.

On observe une tendance constante des vols d'identifiants par des infostealers spécialement conçus pour exfiltrer les identifiants des services cloud.

Les chercheurs X-Force ont également observé que des cryptomineurs étaient déployés dans des environnements cloud, soulignant ainsi le besoin critique de mesures de sécurité robustes pour le cloud. Kinsing, un ensemble de logiciels malveillants notoire, cible de plus en plus les environnements clouds, lançant contre eux des cryptomineurs. Par exemple, Kinsing se cache sous la forme d'un fichier système, en particulier un fichier de manuel ou *man page*, pour éviter d'être détecté tout en exploitant les vulnérabilités des conteneurs cloud pour déployer des opérations de cryptominage sur les serveurs cloud.

En outre, les ransomwares sont devenus une menace prévalente ces dernières années, faisant fréquemment la une des journaux en raison des attaques menées contre diverses organisations du monde entier. L'impact sur les environnements cloud passe cependant souvent inaperçu. Un incident impliquant CloudNordic, une société danoise d'hébergement dans le cloud, illustre parfaitement ce problème croissant. L'attaque par ransomware qui a été signalée a entraîné la perte totale de toutes les données des clients. Elle a exploité une vulnérabilité lors de la migration d'un centre de données, chiffrant tous les serveurs et les systèmes de sauvegarde. Malgré les mesures de sécurité existantes, l'entreprise n'a pas pu récupérer ses données et a choisi de ne pas payer la rançon. Cet incident démontre les lourdes conséquences des ransomwares sur les environnements cloud, soulignant la nécessité de bonnes pratiques de sécurité, de stratégies d'atténuation et de plans de reprise après sinistre efficaces.

Vecteurs d’accès initial

Les techniques employées par les acteurs de la menace pour obtenir un accès initial sont présentées ci-après, dans l’ordre des vecteurs les plus utilisés.

Campagnes de phishing

Malgré la multitude de tactiques et de techniques utilisées par les acteurs de la menace pour obtenir un accès initial aux réseaux des victimes, le phishing a été la principale tactique de choix, utilisée dans 33 % de tous les incidents liés au cloud pour lesquels X-Force est intervenu au cours des deux dernières années. Plus précisément, les attaquants utilisent le phishing comme point de départ d’attaques AITM dans le cadre desquelles ils recueillent les identifiants du destinataire d’un e-mail de phishing après l’avoir incité à saisir des informations de connexion sur une page de connexion contrôlée par l’attaquant.

Utilisation d’identifiants valides

L’utilisation d’identifiants valides a été le deuxième vecteur d’infection initiale dans les attaques où l’infrastructure cloud était une cible potentielle dans la surface d’attaque. Au cours des deux dernières années, 28 % des incidents ont impliqué l’utilisation d’identifiants vérifiés comme vecteur d’accès initial. Les organisations font encore face à la difficulté de trouver un équilibre entre les niveaux d’accès des utilisateurs et les risques de sécurité. Cette problématique se manifeste le plus clairement dans les situations où les attaquants obtiennent l’accès à des comptes d’utilisateurs ou de services surprivilégiés et peuvent causer davantage de dégâts dans l’environnement.

> Le phishing a été la principale tactique, utilisée dans 33 % des incidents liés au cloud.

Exploitation des applications publiques

Le troisième vecteur le plus courant est l'exploitation des vulnérabilités dans les applications publiques. Il s'agit d'une méthode fiable permettant aux acteurs de la menace d'accéder aux environnements cloud et sur site. Cette exploitation représente 22 % des incidents liés au cloud. Voir la figure 5.

La gestion des applications cloud et de leur accès représente un défi de taille pour les organisations, d'autant plus que la hausse du nombre d'applications et de services se poursuit dans les environnements modernes de cloud ou de cloud hybride. L'absence de mise en œuvre correcte pose le risque de passer à côté d'applications non corrigées fonctionnant dans le cloud ou, pire encore, de ne pas savoir qu'elles existent et qu'elles sont en cours d'exécution.

De nombreuses vulnérabilités soulignent le besoin critique de mesures de sécurité robustes et de processus de correction appropriés dans les environnements cloud. Voici deux exemples notables révélés cette année :

Tout d'abord, en mai 2024, une vulnérabilité critique d'exécution de code à distance de Microsoft Outlook (CVE-2024-21413) est apparue comme une menace importante pour les environnements cloud. Des acteurs malveillants peuvent exploiter cette vulnérabilité par le biais d'e-mails de phishing et, s'ils parviennent à leurs fins, peuvent saisir et manipuler les communications, compromettant ainsi les services de messagerie électronique basés sur le cloud et d'autres ressources cloud sensibles.

Puis, en juillet 2024, une vulnérabilité critique a été divulguée dans les serveurs OpenSSH contenant des SSHD sur les systèmes Linux basés sur glibc. Cette vulnérabilité, connue sous le nom de *regreSSHion* et répertoriée sous la référence CVE-2024-6387, peut permettre à un attaquant non authentifié d'exécuter du code à distance sur un système vulnérable avec des privilèges root. OpenSSH est un outil de connectivité largement déployé dans les environnements cloud pour la connexion à distance avec le protocole Secure Shell (SSH).

Principaux vecteurs d'accès initial

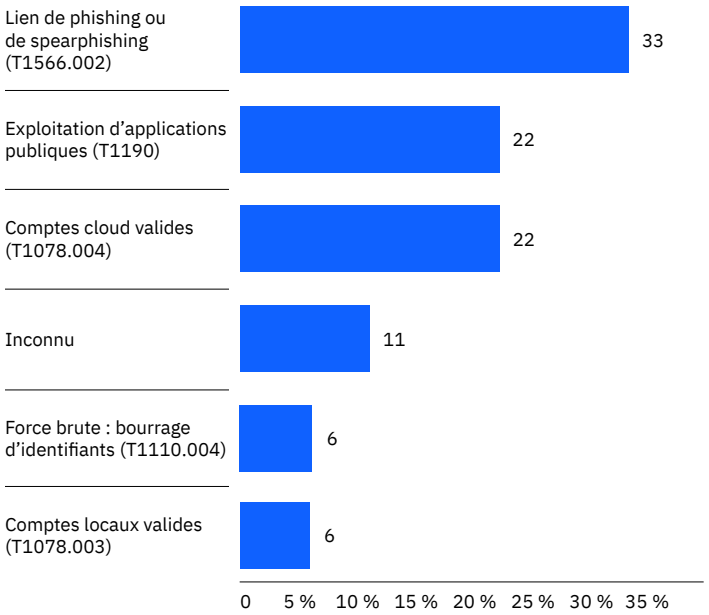


Figure 5. Principaux vecteurs d'accès initial observés par X-Force dans les environnements cloud. Sources : X-Force et MITRE ATT&CK Matrix for Enterprise Framework.[2]

L'exploitation des vulnérabilités dans les applications publiques reste une méthode fiable permettant aux acteurs de la menace d'accéder aux environnements cloud et sur site.

Actions sur l’objectif

Les acteurs de la menace ont utilisé plusieurs moyens d’accès pour atteindre leurs objectifs. X-Force a constaté que les actions sur l’objectif les plus populaires étaient les suivantes.

Compromission des e-mails professionnels

X-Force a observé à plusieurs reprises que des acteurs de la menace abusaient des serveurs hébergés dans le cloud par Active Directory pour mener des attaques de compromission par e-mail dans les environnements des victimes. Cette activité a représenté 39 % des missions de réponse aux incidents au cours des deux dernières années, ce qui en fait la principale action sur l’objectif. Plus précisément, les acteurs de la menace utilisent fréquemment des tactiques de phishing AITM pour contourner l’authentification à étapes de l’utilisateur.

Dans ce scénario, les attaquants utilisent un serveur proxy pour intercepter le processus d’authentification entre la cible et un service légitime. Cette stratégie permet à l’attaquant de collecter les identifiants de la cible *et le* jeton généré lorsque la cible entre son MFA, ce qui permet de maintenir une session authentifiée que l’attaquant peut utiliser. Voir la figure 6.

Si l'attaque réussit, l'acteur de la menace s'authentifie à l'aide des identifiants de la victime et peut effectuer n'importe quelle action à l'intérieur de l'application. Dans la plupart des cas, l'attaquant peut envoyer des e-mails de phishing à partir du compte compromis, ajouter des règles de transfert d'e-mails ou même se connecter à d'autres ressources cloud qui possèdent les mêmes identifiants de connexion d'entreprise.

Cryptominage

Représentant 22 % des incidents survenus au cours des deux dernières années, le cryptominage était la deuxième action sur l'objectif la plus fréquente, restant populaire parmi les acteurs de la menace, en particulier dans les environnements cloud. Parce qu'elle est extrêmement gourmande en ressources, une infrastructure cloud puissante est l'endroit idéal pour déployer un logiciel malveillant de cryptominage. En outre, les utilisateurs sont moins susceptibles de remarquer l'effet de ce logiciel malveillant lorsqu'il n'est pas exécuté localement sur leur point de terminaison. Voir la figure 7.

Collecte d'identifiants

La collecte d'identifiants est l'une des nombreuses techniques employées par les acteurs de la menace pour dérober les identifiants d'authentification des utilisateurs afin de mener d'autres activités malveillantes, généralement par le biais d'attaques de type phishing, keylogging (enregistrement de frappes), watering hole (attaque du point d'eau) et force brute. Les attaques par collecte d'identifiants ont été la troisième action sur l'objectif la plus fréquente, représentant 11 % des incidents. Il est courant que des identifiants dérobés soient mis en vente et achetés sur les places de marché du dark web ou utilisés pour compromettre d'autres comptes. Voir la figure 7.

Étapes d'une attaque BEC

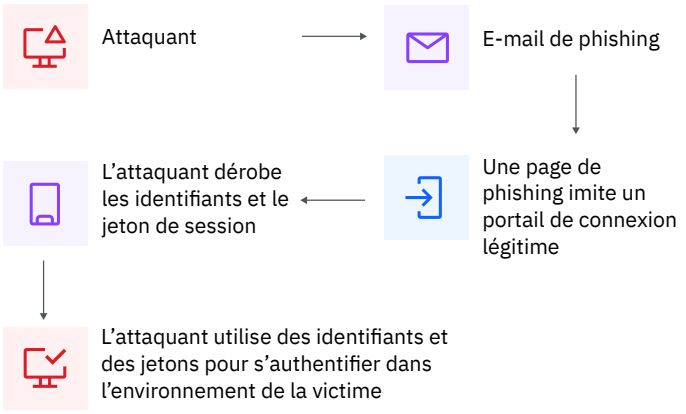


Figure 6. Une page Web contrôlée par un attaquant dérobe les identifiants de la victime au cours d'une attaque AITM, qui est le scénario de menace le plus courant observé par X-Force dans les environnements cloud.

Actions sur l'objectif

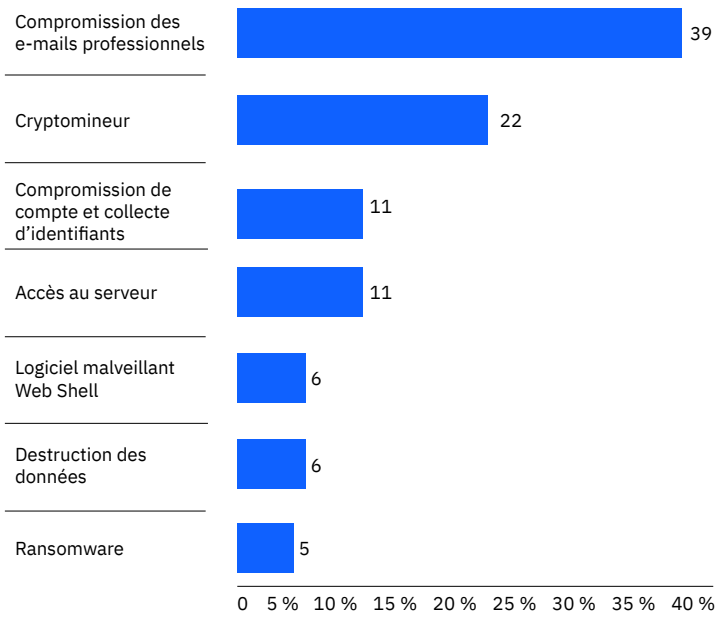


Figure 7. Principales actions sur l'objectif observées par X-Force dans les environnements cloud. Les incidents peuvent avoir plus d'une action principale sur l'objectif observé.

Défaillances des règles de sécurité dans les environnements basés sur le cloud

Dans le cadre du partenariat entre IBM et Red Hat Insights, X-Force a analysé deux jeux de données provenant d'une centaine de clients des services de conformité de Red Hat Insights du monde entier. Le premier jeu de données concernait des clients opérant dans des environnements 100 % cloud, tandis que le second jeu incluait des clients dont au moins 50 % des systèmes se trouvaient dans le cloud. X-Force a évalué les règles de sécurité pour leurs environnements respectifs. Ces manquements aux règles de sécurité ou à la conformité donnent des informations essentielles sur la manière dont les organisations peuvent atténuer les risques pour leurs environnements cloud.

Les organisations opérant dans des environnements cloud totalement ou partiellement intégrés ont souvent rencontré des difficultés majeures pour maintenir une posture de sécurité robuste, comme en témoignent les manquements répétés aux règles de sécurité clés dans les environnements des clients Red Hat Insights. Ces manquements sont souvent dus à la complexité de la configuration et de l'application systématique des politiques de sécurité dans des infrastructures cloud dynamiques et étendues. La configuration des zones de pare-feu, l'isolement des systèmes de fichiers et l'application d'options de montage sécurisé nécessitent des connaissances spécialisées et une surveillance assidue, ce qui peut s'avérer difficile pour les équipes informatiques et de sécurité.

En outre, le recours à des pratiques obsolètes, à des configurations manuelles et à des outils d'automatisation insuffisants peut exacerber ces problèmes, entraînant une augmentation des erreurs de configuration liée à la sécurité et des vulnérabilités.

Dans un contexte plus large, ces problèmes techniques dans l'infrastructure cloud devraient indiquer des risques conséquents pour les organisations, y compris une plus forte probabilité de cyberattaques, de défaut de conformité aux normes réglementaires et de déficiences opérationnelles. À mesure que le développement et l'évolution des environnements cloud se poursuivent, il devient vital pour les organisations d'adopter des mesures de sécurité, des stratégies et des bonnes pratiques globales. Ces mesures leur permettent de tirer pleinement parti des avantages liés à la technologie cloud tout en protégeant les actifs critiques et en préservant la réussite des opérations et la conformité réglementaire.

> Les manquements aux règles de l'infrastructure cloud indiquent des risques conséquents pour les organisations.

Les 5 principales règles à ne pas avoir été respectées pour les environnements 100 % cloud

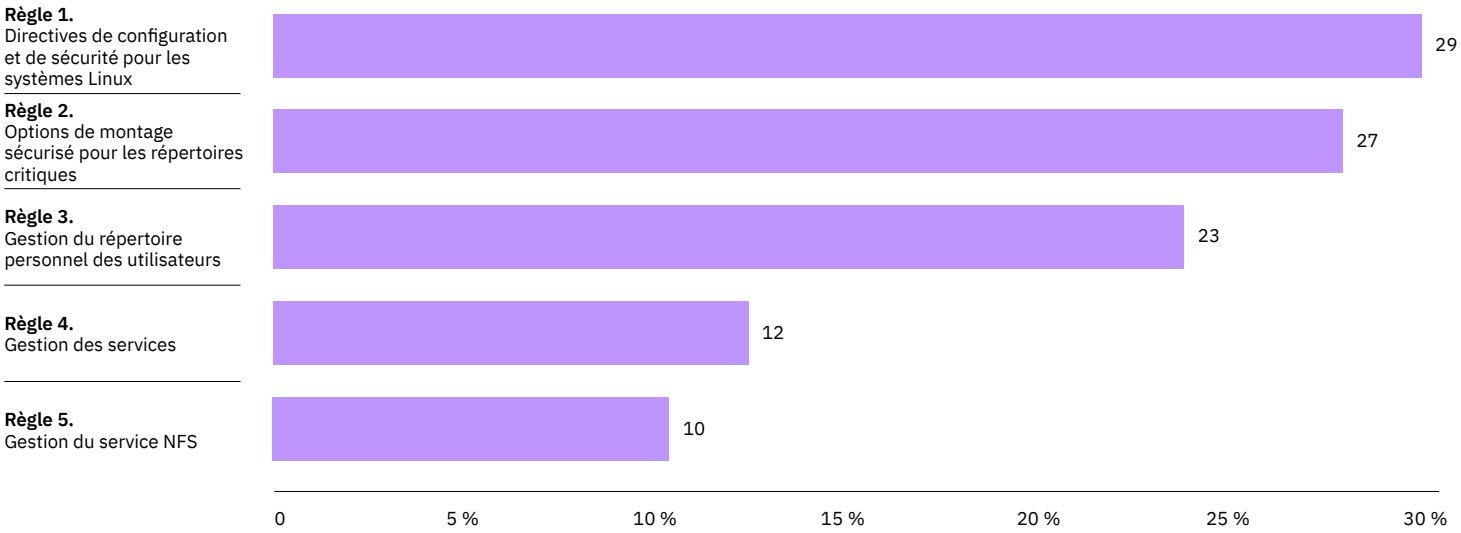


Figure 8. Nombre des cinq principales règles à ne pas avoir été respectées pour les environnements 100 % cloud, par ordre d'importance. Source : Red Hat Insights

Les 5 principales règles à ne pas avoir été respectées pour les environnements 100 % cloud

À partir des données Red Hat Insights analysées par X-Force, vous trouverez ci-dessous les cinq règles de sécurité qui ont le plus souvent fait défaut dans les environnements 100 % cloud, ainsi que les recommandations pour y remédier. Voir la figure 8.

Règle 1. Directives de configuration et de sécurité pour les systèmes Linux (29 %)
Cet ensemble de règles se concentre sur la configuration des paramètres essentiels de sécurité et de gestion dans les systèmes Linux, y compris la définition de la zone par défaut pour firewalld et l'isolement du répertoire /tmp sur une partition distincte pour renforcer la sécurité et gérer efficacement l'espace disque. Pour atténuer les risques :

- Configurez la zone par défaut pour le service firewalld afin de garantir des configurations de sécurité réseau correctes dans les systèmes basés sur Red Hat.
- Isolez le répertoire /tmp sur une partition distincte pour renforcer la sécurité et gérer efficacement l'espace disque afin d'éviter les attaques par déni de service et d'améliorer les performances du système.

Règle 2. Options de montage sécurisé pour les répertoires critiques (27 %)
Cet ensemble de règles met l'accent sur la configuration d'options de montage sécurisées pour les répertoires critiques en empêchant l'exécution de binaires, la création de fichiers spéciaux et l'exécution de programmes setUID et setGID afin de renforcer la sécurité et d'imposer une utilisation correcte des répertoires. Pour atténuer les risques, empêchez les actions suivantes :

- Exécution de binaires dans le répertoire /var/log
- Création de fichiers spéciaux dans le répertoire /var/log
- Exécution des programmes setUID et setGID dans le répertoire /var/log/audit
- Création de fichiers spéciaux dans le répertoire /home
- Création de fichiers spéciaux dans le répertoire /var
- Exécution des programmes setUID et setGID dans le répertoire /var/log
- Création de fichiers spéciaux dans le répertoire /var/log/audit
- Exécution des programmes setUID et setGID dans le répertoire /var
- Exécution de binaires dans le répertoire /var/log/audit
- Exécution des programmes setUID et setGID dans le répertoire /home

Règle 3. Gestion du répertoire personnel des utilisateurs (23 %)
Cet ensemble de règles garantit la propriété et les autorisations appropriées des répertoires personnels des utilisateurs, ce qui renforce la sécurité en empêchant les accès non autorisés et en maintenant une structure de système de fichiers cohérente et organisée. Pour atténuer les risques :

- Veillez à ce que tous les répertoires personnels des utilisateurs interactifs soient détenus par le groupe de l'utilisateur principal afin de préserver la propriété, les contrôles d'accès et la cohérence de l'organisation.

Règle 4. Gestion des services (12 %)
Cet ensemble de règles consiste à désactiver les services inutiles, tels que rpcbind et Network File System (NFS), afin de réduire la surface d'attaque, de renforcer la sécurité et de libérer des ressources système. Pour atténuer les risques :

- Désactivez le service rpcbind.
- Désactivez le service NFS.

Règle 5. Gestion du service NFS (10 %)
Cet ensemble de règles est exclusivement dédié à la gestion du service NFS et met l'accent sur son rôle spécifique dans le partage de fichiers en réseau et sur les implications d'ordre sécuritaire liées à l'activation inutile de ce service. Pour atténuer les risques :

- Désactivez le service NFS pour réduire la surface d'attaque, renforcer la sécurité et libérer des ressources du système. NFS permet le partage de fichiers entre systèmes sur un réseau mais, s'il n'est pas nécessaire, sa désactivation peut améliorer la sécurité et les performances.

Les 5 principales règles à ne pas avoir été respectées pour les environnements 50 % cloud

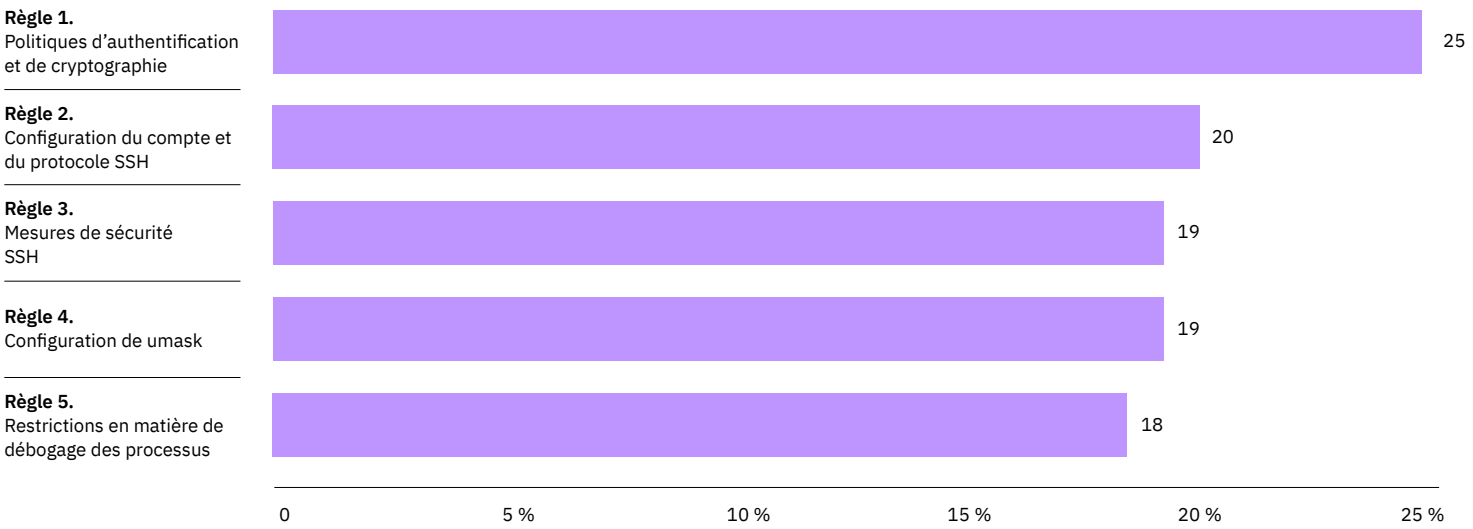


Figure 9. Nombre des cinq principales règles à ne pas avoir été respectées pour les environnements 50 % cloud, par ordre d'importance. Source : Red Hat Insights

Les 5 principales règles à ne pas avoir été respectées pour les environnements 50 % cloud ou plus

À partir des données Red Hat Insights analysées par X-Force, vous trouverez ci-dessous les cinq règles de sécurité qui ont le plus souvent fait défaut dans les environnements 50 % cloud ou plus, ainsi que les recommandations pour y remédier. Voir la figure 9.

Règle 1. Politiques d'authentification et de cryptographie (25 %)
Cet ensemble de règles se concentre sur la normalisation et la sécurisation des mécanismes d'authentification et des politiques cryptographiques afin de garantir des pratiques de sécurité cohérentes et fortes dans l'ensemble du système.
Pour atténuer les risques :

- Utilisez authselect pour normaliser et simplifier la gestion des paramètres d'authentification, afin de garantir la cohérence et de renforcer la sécurité.
- Définissez des politiques cryptographiques à l'échelle du système pour garantir l'utilisation d'algorithmes et de protocoles cryptographiques solides et sûrs, afin d'améliorer la sécurité et la conformité.

Règle 2. Configuration du compte et du protocole SSH (20 %)
Cet ensemble de règles concerne la gestion de l'inactivité des comptes d'utilisateurs, les limites des sessions SSH, la propriété des fichiers et l'expiration des mots de passe afin de renforcer la sécurité, de réduire les risques et de se conformer aux exigences réglementaires. Pour atténuer les risques :

- Désactivez automatiquement les comptes d'utilisateurs après une période d'inactivité donnée afin de réduire les risques de sécurité associés aux comptes dormants.
- Définissez SSH ClientAliveCountMax pour vous assurer de mettre fin aux connexions inactives ou qui ne répondent pas et ainsi renforcer la sécurité et libérer des ressources.
- Veillez à ce que tous les fichiers appartiennent à un utilisateur valide en recherchant et en corrigeant tout fichier sans propriétaire afin de maintenir la propriété et la sécurité des fichiers.
- Fixez une durée de vie maximum pour les mots de passe pour garantir leur changement régulier et ainsi renforcer la sécurité et la conformité.

Règle 3. Mesures de sécurité SSH (19 %)
Cet ensemble de règles renforce la sécurité SSH en désactivant les accès et encourage les bonnes pratiques de sécurité. Pour atténuer les risques :

- Désactivez l'accès SSH via des mots de passe vides pour empêcher les accès non autorisés et atténuer les attaques par force brute.
- Désactivez la connexion root SSH pour empêcher l'accès root direct et ainsi réduire le risque d'accès administratif non autorisé.

Règle 4. Configuration de umask (19 %)
Cet ensemble de règles consiste à configurer les valeurs umask par défaut afin de garantir la sécurité des autorisations des nouveaux fichiers et répertoires et ainsi de renforcer la sécurité et d'assurer la régularité. Pour atténuer les risques :

- Définissez les valeurs umask appropriées dans le répertoire /etc/profile pour vous assurer que les nouveaux fichiers et répertoires disposent d'autorisations sécurisées par défaut.
- Définissez les valeurs umask appropriées dans le répertoire /etc/bashrc pour vous assurer que les nouveaux fichiers et répertoires disposent d'autorisations sécurisées par défaut.

Règle 5. Restrictions en matière de débogage des processus (18 %)
Cet ensemble de règles limite le débogage et l'inspection des processus aux seuls processus descendants afin de renforcer la sécurité en empêchant l'accès et la manipulation non autorisés des processus. Pour atténuer les risques :

- Restreignez l'utilisation de ptrace aux processus descendants pour renforcer la sécurité en limitant les capacités de débogage et d'inspection des processus afin de réduire le risque d'utilisation malveillante.

Cloud et IA

Bien que les cybercriminels et les acteurs de la menace commandités par des États aient mené des campagnes mondiales de phishing et de spam pour diffuser divers logiciels malveillants par le biais des services cloud, la menace à court terme des attaques générées par l'IA et ciblant les environnements cloud reste modérément faible. Il est cependant possible que les acteurs de la menace aient déjà recours à l'IA pour mener des activités malveillantes contre les environnements cloud. Une étude X-Force a montré que l'IA peut être utilisée pour développer des prompts d'ingénierie sociale sophistiqués et des campagnes de phishing en bien moins de temps qu'il n'en faut à un humain pour créer un e-mail de phishing convaincant.

En outre, X-Force a remarqué que Hive0137, un distributeur de logiciels malveillants extrêmement actif depuis au moins octobre 2023, utilise probablement de grands modèles de langage (LLM) pour aider au développement de scripts, ainsi qu'à la création d'e-mails de phishing authentiques et uniques. Bien que les outils d'IA donnent aux attaquants les moyens de rendre leurs appâts plus authentiques, permettant ainsi aux acteurs de la menace d'échapper plus facilement à la détection, l'utilisation de la technologie d'IA dans le cadre d'activités malveillantes entame tout juste sa courbe de maturité.

Les attaques ciblant les plateformes IA, qu'elles soient déployées dans le cloud ou sur site, s'accompagnent d'un obstacle majeur et, en l'état actuel des choses, le retour sur investissement immédiat n'en vaut pas la peine. Cependant, à mesure que le marché de l'IA mûrit et s'intègre de plus en plus dans les opérations métier de tous les secteurs, la surface d'attaque peut s'étendre et les acteurs de la menace peuvent être davantage incités à mener des attaques. Selon les prévisions de X-Force, lorsqu'une seule technologie d'IA générative approchera 50 % de part du marché ou lorsque le marché se résumera à trois technologies maximum, alors des attaques à l'échelle seront susceptibles d'être déclenchées contre ces plateformes. Les organisations sont encouragées à se référer aux recommandations de ce rapport, qui peuvent contribuer à atténuer le risque de cybermenaces, qu'elles émanent ou non de l'utilisation de l'IA.

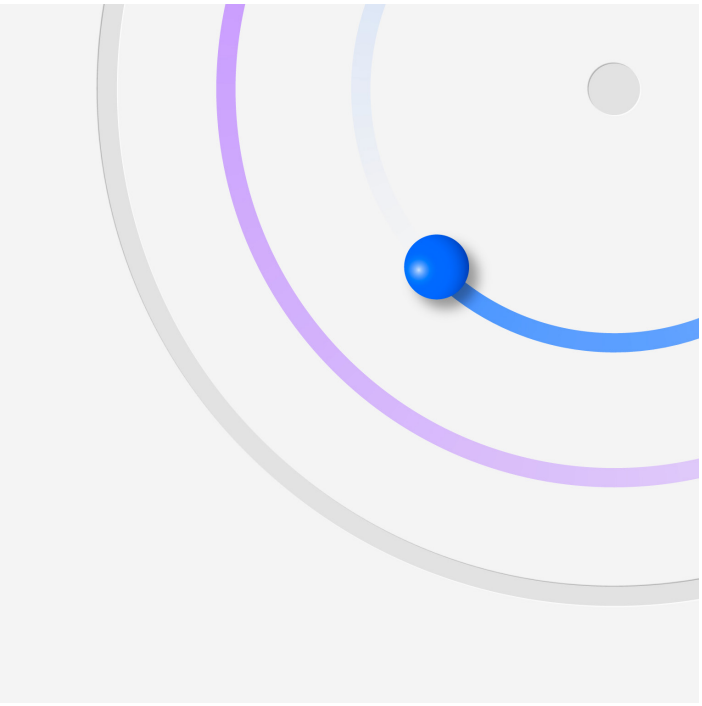
> Les acteurs de la menace sont déjà susceptibles de tirer parti de l'IA pour mener des activités malveillantes contre les environnements cloud.

Recommandations

Compte tenu de l'évolution de l'environnement des menaces liées au cloud, les organisations doivent continuellement surveiller, adapter et améliorer leurs stratégies de sécurité pour protéger les environnements cloud et SaaS.

X-Force a constaté que les organisations amélioraient la sécurité cloud en renforçant les protections des messageries électroniques et en exigeant l'utilisation du MFA pour accéder au cloud, ce qui rend les attaques par phishing plus difficiles. Cependant, la protection de l'identité et des données dans les environnements cloud et SaaS nécessite des ajustements continus pour faire face à l'évolution des menaces.

Voici quelques recommandations pour contribuer à l'élaboration d'un cadre d'exigences robuste visant à améliorer la sécurité cloud.



Effectuer une préparation globale et des tests complets

Une approche proactive et holistique de la sécurité est primordiale dans l'environnement cloud. Intégrez la sécurité tout au long du développement grâce à un DevOps sécurisé, à la modélisation des menaces et à des tests rigoureux pour renforcer la résilience. L'automatisation minimise l'erreur humaine et contribue à garantir une conformité continue, permettant ainsi aux organisations de faire face à l'évolution des menaces en toute confiance.

Renforcer les capacités de réponse aux incidents

Dans l'environnement dynamique des menaces d'aujourd'hui, une réponse rapide et efficace aux incidents peut faire toute la différence. Tirez parti des renseignements sur les menaces pour comprendre les motivations des attaquants et réagir plus rapidement. Pendant les enquêtes, préserver les preuves légales en redéployant les machines affectées (plutôt qu'en les restaurant) permet d'assurer la conservation des données critiques. Des tests réguliers des procédures de reprise après sinistre et de sauvegarde sont également essentiels pour assurer la continuité des activités et la résilience.

Protéger vos données grâce à des mesures de sécurité robustes

La protection des données reste la pierre angulaire d'une stratégie de sécurité cloud globale. Chiffrez les données lors du stockage, de l'utilisation et du transit, et gérez les clés en toute sécurité afin de garantir la protection des informations sensibles. Les organisations doivent minimiser l'exposition des données en réduisant le nombre de données sensibles stockées et en limitant strictement l'accès au personnel nécessaire. L'automatisation des privilèges des groupes de sécurité et la désactivation des comptes dormants renforcent davantage la sécurité en adhérant au principe du moindre privilège et en empêchant les compromissions potentielles de comptes.

Renforcer la posture de sécurité des identités

Avoir une stratégie de gestion des identités rationalisée n'est plus un luxe, mais une nécessité. Simplifiez les politiques d'identité pour trouver un équilibre entre sécurité robuste et expériences conviviales. Adoptez des méthodes d'authentification modernes, telles que le protocole MFA, et explorez des options sans mot de passe, telles qu'un code QR ou l'authentification FIDO2, pour renforcer les défenses contre les accès non autorisés.

Concevoir des stratégies IA sécurisées pour garder une longueur d'avance sur les menaces liées au cloud

Exploiter la puissance de l'IA est crucial pour garder une longueur d'avance sur les menaces en constante évolution liées au cloud. L'IA offre le potentiel de révolutionner l'authentification et l'identification, en améliorant à la fois l'efficacité et la sécurité de ces processus critiques. Alors que l'IA générative continue de progresser, protégez l'intégrité des données et des modèles avec un chiffrement robuste et des contrôles d'accès.

Les organisations doivent gérer de manière proactive les risques associés au shadow AI et à l'utilisation non autorisée d'outils d'IA sur le lieu de travail afin de contribuer à garantir la transparence et le contrôle des initiatives d'IA. En outre, les organisations doivent se préparer à l'impact potentiel que les menaces basées sur la technologie quantique pourraient avoir sur la sécurité à long terme des projets d'IA.

À propos

IBM X-Force
IBM X-Force est une équipe de hackers, d'intervenants, de chercheurs et d'analystes spécialisés dans les menaces. Notre portefeuille comprend des produits et services offensifs et défensifs, alimentés par une vision des menaces à 360 degrés.

Grâce à une compréhension approfondie de la façon dont les cybercriminels pensent, élaborent des stratégies et frappent, X-Force Threat Intelligence vous aide à prévenir, détecter, répondre et récupérer après des incidents et à vous concentrer sur les priorités de votre entreprise.

Si votre organisation souhaite obtenir de l'aide pour renforcer sa posture de sécurité, prenez rendez-vous pour un entretien individuel avec un expert IBM X-Force.

IBM
IBM, l'un des principaux fournisseurs mondiaux de cloud hybride, d'IA et de services métier, aide ses clients dans plus de 175 pays à tirer parti des informations issues de leurs données, à rationaliser les processus métier, à réduire leurs coûts et à obtenir un avantage concurrentiel dans leurs secteurs. Ces capacités s'appuient sur l'engagement légendaire d'IBM en faveur de la confiance, de la transparence, de la responsabilité, de l'inclusion et du service. Pour plus d'informations, rendez-vous sur www.ibm.com/fr-fr.

Planifier une séance d'information →

Contributeurs
Austin Zeizel
Christopher Caridi
David McMillen
Michelle Alvarez
Agnes Ramos-Beauchamp
Christopher Bedell
Johnny Shaieb
Scott Lohr
Scott Moore
Sophie Cunningham
Cybersixgill
Red Hat Insights

1. Toutes les données recueillies et analysées dans le rapport, à l'exception des données relatives à l'engagement de réponse aux incidents, ont été collectées entre juin 2023 et juin 2024. X-Force a étendu la période de collecte des données d'engagement de réponse aux incidents de juin 2022 à juin 2024 afin de fournir le vecteur d'accès initial global sur deux ans ainsi que les actions sur les tendances des objectifs.
2. MITRE ATT&CK Matrix, The MITRE Corporation, 19 juin 2019.