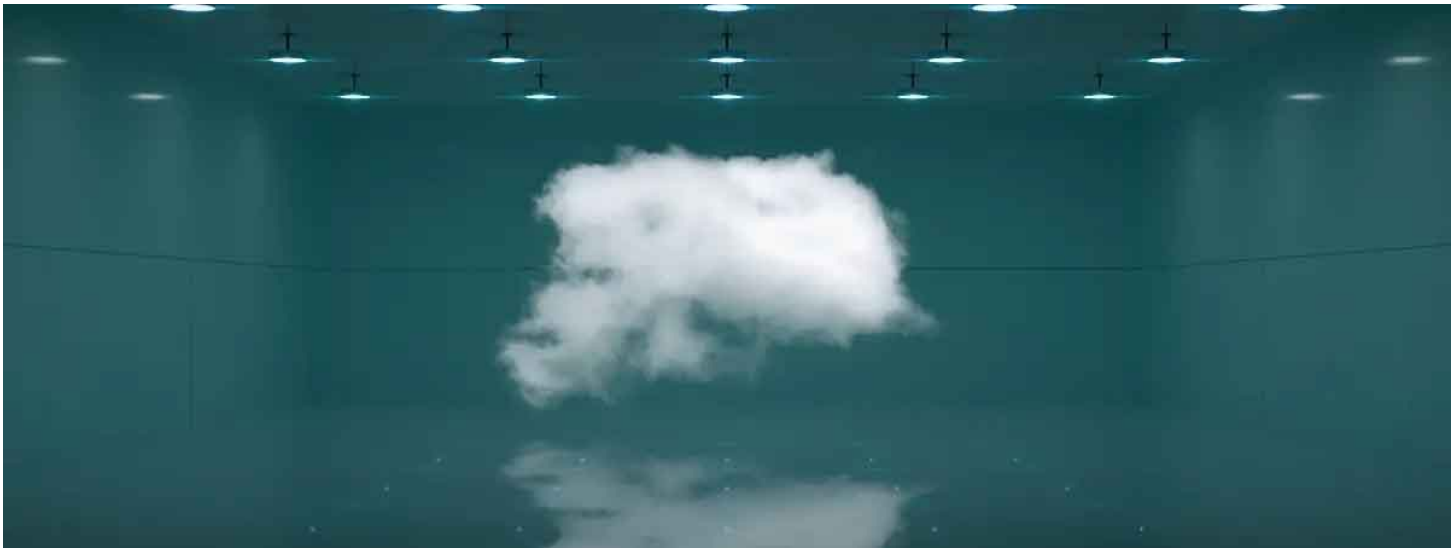
Communiqués de presse

« Autorisés » à s'infiltrer : les attaquants utilisent des informations d'identification valides pour compromettre les environnements Cloud

Des informations d'identification à hauts privilèges laissées en clair dans 33 % des simulations d’attaques réalisées par X-Force



Les attaquants cherchent constamment à améliorer leurs marges de productivité, mais de nouvelles données d'IBM X-Force suggèrent qu'ils ne s'appuient pas exclusivement sur la sophistication pour y parvenir. Les tactiques simples mais fiables qui offrent une facilité d'utilisation et souvent un accès direct aux environnements privilégiés sont encore très utilisées. X-Force a publié aujourd'hui le rapport 2023 sur le paysage des menaces dans le Cloud (2023 Cloud Threat Landscape Report), qui détaille les tendances courantes et les principales menaces observées contre les environnements Cloud au cours de l'année écoulée. L'utilisation inappropriée des informations d'identification constitue la principale cause de compromission du Cloud à laquelle X-Force a répondu au cours de l'année écoulée, ce qui réaffirme la nécessité pour les entreprises de redoubler d'efforts pour renforcer leurs pratiques en matière de gestion des informations d'identification.

Basé sur des informations provenant de X-Force threat intelligence, de tests d’intrusion, des missions de réponse aux incidents, d’information provenant de Red Hat Insights et de données fournies par le contributeur du rapport Cybersixgill, entre juin 2022 et juin 2023, certains des points clés issus du rapport sont les suivants :

- **Des informations d'identification qui valent une douzaine de beignets** - Plus de 35 % des incidents de sécurité dans le Cloud résultent de l'utilisation par des attaquants d'informations d'identification valides mais compromises. Représentant près de 90 % des actifs mis en vente sur les places de marché du dark web, la popularité des informations d'identification auprès des cybercriminels est évidente, avec une moyenne de 10 dollars par liste, soit l'équivalent d'une douzaine de beignets. Les identifiants Microsoft Outlook Cloud ont fait l'objet de plus de 5 millions de mentions sur les places de marché illicites, ce qui en fait de loin le type d'identifiants le plus populaire à la vente.

- **Clouds "non entretenus"** - X-Force a observé une augmentation de près de 200% des nouvelles vulnérabilités et expositions communes (CVE) liées au Cloud par rapport à l'année précédente, suivant désormais près de 3 900 vulnérabilités liées au Cloud, un nombre qui a doublé depuis 2019. Les attaquants peuvent faire progresser leurs objectifs de manière significative en exploitant un grand nombre de ces vulnérabilités, plus de 40 % des nouvelles CVE liées au Cloud leur permettant d'obtenir soit des informations, soit un accès, ce qui indique que les attaquants peuvent s'implanter solidement grâce à ces points d'entrée.

- **Prévisions pour l'Europe** – 64 % des incidents liés au Cloud qu'X-Force a traités au cours de la période couverte par le rapport concernaient des organisations européennes. En fait, sur l'ensemble des logiciels malveillants observés par Red Hat Insights, 87 % ont été identifiés dans des organisations européennes, ce qui souligne leur attrait pour les attaquants. Il est possible que les tensions croissantes dans la région et l'augmentation du déploiement de portes dérobées - qui ont été signalées dans le rapport 2023 X-Force Threat Intelligence Index - soient liées au fait que les environnements Cloud européens figurent en tête des cibles observées.

Les informations d'identification ne sont plus des authentificateurs crédibles

Les attaquants continuent de miser sur une mauvaise hygiène des informations d'identification dans les entreprises pour mener à bien leurs attaques. Les missions d'X-Force révèlent que, souvent, les informations d'identification avec un accès privilégié sont laissées exposées sur les terminaux des utilisateurs en texte clair, créant ainsi une opportunité pour les attaquants d'établir un point de pivot pour pénétrer plus profondément dans l'environnement ou accéder à des informations hautement sensibles. Plus précisément, des informations d'identification en clair ont été trouvées sur les terminaux des utilisateurs dans 33 % des simulations d'attaques de X-Force Red qui impliquaient des environnements Cloud au cours de la période considérée. Cette tendance à la hausse de l'utilisation des informations d'identification comme vecteur d'accès initial - représentant 36 % des incidents liés au Cloud en 2023 contre 9 % en 2022 - souligne la nécessité pour les organisations d'aller au-delà des « authentifications humaines » et de donner la priorité aux garde-fous technologiques capables de sécuriser la gestion de l'identité et de l'accès des utilisateurs.

Alors que l'accès à davantage de données dans un plus grand nombre d'environnements devient un besoin récurrent, l'erreur humaine continue de représenter un défi en matière de sécurité. Le besoin croissant d'une gestion des identités et des accès plus dynamique et adaptative peut être satisfait grâce aux capacités d'IA avancées disponibles sur le marché aujourd'hui. Par exemple, les clients d'IBM Security Verify constatent une amélioration substantielle en s'appuyant sur des processus d'authentification plus intuitifs pour calculer le score de risque en fonction des habitudes de connexion, de l'emplacement de l'appareil, de l'analyse du comportement et d'autres contextes, puis pour adapter automatiquement le processus de connexion et la vérification en conséquence.

Les organisations minimisent leur surface d'attaque - Il est essentiel de soumettre leur sécurité à

des tests de résistance

La capacité à gérer l'ensemble de la surface d'attaque des organisations est essentielle à l'établissement d'une cyber-résilience. Cependant, les organisations ont tendance à être plus exposées qu'elles ne le pensent, sous-estimant souvent les cibles potentielles au sein de leur environnement qui peuvent servir les objectifs des attaquants. Le Shadow IT et une dette de vulnérabilité ingérable rendent de plus en plus difficile pour les organisations de savoir où elles sont le plus exposées.

Selon le rapport X-Force, près de 60 % des vulnérabilités récemment divulguées pourraient, si elles étaient exploitées, permettre aux attaquants d'obtenir des informations, un accès ou des privilèges qui leur permettraient de se déplacer latéralement dans le réseau. Qu'il s'agisse de fournir aux attaquants des informations sur la façon dont les environnements sont configurés ou d'obtenir une authentification non autorisée leur permettant d'obtenir des autorisations supplémentaires, il est essentiel pour les organisations de savoir quels risques doivent être prioritaires, en particulier lorsqu'elles disposent de ressources limitées. Pour aider les organisations à relever ce défi, X-Force Red utilise l'IA pour évaluer les risques liés aux codes d'exploitation dotés de charges actives - en s'appuyant sur le moteur de classement automatisé conçu par notre équipe de hackers pour enrichir et hiérarchiser les résultats en fonction des codes d'exploitation et des principaux facteurs de risque tels que la valeur et l'exposition des actifs.

Alors que les organisations s'efforcent de mieux comprendre leur posture en matière de risques liés au Cloud, il est important qu'elles associent ces connaissances à la préparation de la réponse en s'engageant dans des exercices de simulation d'attaques utilisant des scénarios basés sur le Cloud afin de s'entraîner et de mettre en pratique une réponse efficace aux incidents liés à cette technologie. De cette manière, elles peuvent non seulement se faire une idée des voies d'attaque et des objectifs qu'un attaquant pourrait poursuivre, mais aussi mieux mesurer leur capacité à répondre à une telle attaque et à en limiter l'impact potentiel.

Si vous souhaitez lire l'intégralité du rapport 2023 X-Force Cloud Threat Report, vous pouvez le consulter ici.

Vous pouvez vous inscrire ici au webinaire " Cloud Threat Landscape Report : Explorer les tendances pour garder une longueur d'avance sur les menaces" qui aura lieu le mercredi **20 septembre à 17h00**.

Pour en savoir plus sur les recherches de X-Force en matière de sécurité, les renseignements sur les menaces et les informations fournies par les attaquants, vous pouvez consulter le X-Force Research Hub.

Si vous souhaitez organiser un échange avec l'équipe IBM X-Force, cliquez ici.

Contacts Presse :

IBM
Gaëlle Dussutour
Tél. : + 33 (0)6 74 98 26 92
dusga@fr.ibm.com

Weber Shandwick pour IBM

Louise Weber

Tél. : + 33 (0)6 89 59 12 54

ibmfrance@webershandwick.com