ANOMALI

Cas pratique

ATTÉNUER LES ATTAQUES BASÉES SUR LES IDENTIFIANTS COMPROMIS GRÂCE AU FRAMEWORK MITRE ATT&CK®

Les usurpations d'identifiants, capture de noms d'utilisateur et de mots de passe par un acteur malveillant, constituent aujourd'hui la toute première menace pour les entreprises. Pour les équipes de sécurité, ces attaques exploitant des identifiants compromis posent un problème bien spécifique : les cybercriminels, se faisant passer pour un utilisateur légitime, accèdent à des systèmes et à des données sensibles à l'insu des outils de sécurité standard, comme les antivirus ou les anti-malwares.

COMPROMISSION D'IDENTIFIANTS : UN COÛT ÉLEVÉ

Selon IBM et le Ponemon Institute, le coût moyen d'une violation de données approche les 10 millions de dollars, mais les derniers incidents notoires basés sur des identifiants compromis le montrent : les pertes ne sont pas que financières.

- **Colonial Pipeline (2021) :** Les assaillants ont utilisé un mot de passe de VPN compromis pour exfiltrer plus de 100 Go de données et déployer un ransomware sur les systèmes de leur victime. L'entreprise a dû mettre à l'arrêt son pipeline long de 9 000 km, entraînant des pénuries de carburant et une explosion des prix dans tout le pays. Elle a aussi consenti à verser une rançon de 5 millions de dollars, à laquelle s'ajoutent des conséquences opérationnelles majeures et un impact tragique sur sa réputation.
- **Okta (2024) :** Leader des solutions de gestion des identités et des accès (IAM), Okta a été plongée dans l'embarras par une fuite de données d'envergure. Les attaquants s'étaient servi des données d'identification enregistrées par un employé dans son espace personnel Google. Cette violation a affecté certains clients de premier plan, dont Cloudflare et BeyondTrust, ce qui n'a fait qu'empirer l'atteinte à la réputation d'Okta.
- **Norton (2023) :** Sur le dark web, des cybercriminels ont mis la main sur des identifiants issus d'une violation antérieure et les ont utilisés pour infiltrer le réseau de cet acteur historique de la cybersécurité. Plus de 925 000 clients ont été touchés, dont certains avaient enregistré leurs mots de passe dans le gestionnaire de mots de passe de l'éditeur d'antivirus.
- **23andMe (2023) :** Ciblant des données à caractère personnel très sensibles, les criminels ont d'abord utilisé des identifiants compromis pour accéder à 14 000 comptes, puis, dans un deuxième temps, se sont servi des informations génétiques et familiales de ceux-ci pour exposer les données de 6,9 millions de personnes. L'entreprise a subi de sévères critiques et a consenti à un règlement amiable d'un montant de 30 millions de dollars.

Heureusement, le framework MITRE ATT&CK est là pour vous aider à comprendre et à développer des stratégies permettant de gérer ce type de vulnérabilités.

LE FRAMEWORK MITRE ATT&CK : DÉFINITION

MITRE ATT&CK est une base de connaissances reconnue dans le monde entier et qui peut être utilisée comme un socle d'amélioration de la sécurité par n'importe quelle personne ou organisation. ATT&CK est l'acronyme d'Adversarial Tactics, Techniques & Common Knowledge (« tactiques et techniques adverses et connaissances communes »). Ce référentiel se compose d'une liste exhaustive et constamment mise à jour de tactiques et de techniques utilisées par les cybercriminels pour infiltrer les réseaux ou les systèmes.

MITRE ATT&CK fournit aux entreprises divers moyens de mieux lutter contre ces adversaires :

- Informations sur l'ensemble des techniques adverses
- Détails sur les groupes associés à ces techniques
- Méthodes de détection et de neutralisation de ces tactiques et techniques

Par « tactiques », on entend ce que l'agresseur essaie de faire lors d'une phase précise de l'attaque, tandis que les « techniques » désignent les approches qui ont déjà permis à des criminels d'infiltrer des entreprises.

LES IDENTIFIANTS COMPROMIS ÉCHAPPENT À TOUTE DÉTECTION

De toutes les techniques d'attaque, celles usurpant des identifiants sont exceptionnellement difficiles à neutraliser.

- **Légitimité apparente :** Les identifiants compromis permettent de se faire passer pour des utilisateurs autorisés. Pour les outils de sécurité traditionnels, les activités qui y sont associées paraissent donc légitimes. Résultat : les criminels arrivent souvent à opérer longtemps au sein des réseaux cibles. Ils s'approprient des privilèges supérieurs et se déplacent latéralement sans éveiller les soupçons.
- **Techniques d'attaque évolutives :** Les cybercriminels développent en permanence de nouvelles méthodes afin de récupérer et d'exploiter des identifiants — phishing sophistiqué, ingénierie sociale, ou encore attaques basées sur l'accoutumance à la MFA (authentification multifacteur), dans lesquelles les attaquants sapent le système d'authentification multifacteur en inondant de requêtes MFA l'e-mail, le téléphone ou d'autres appareils de leur victime.
- **Volume et complexité des données :** Dans les réseaux modernes, le volume d'événements d'authentification et d'activité des utilisateurs constitue en soi un obstacle à la détection des signaux faibles de la compromission d'identifiants. Confrontées aux immenses volumes de données et d'alertes produits par les environnements d'entreprise complexes, les équipes de sécurité peinent à distinguer les véritables menaces des faux positifs.

TACTIQUES D'ENTREPRISE MITRE ATT&CK

Les 14 tactiques distinctes suivent les différentes étapes d'une cyberattaque. La compromission d'identifiants correspond à la catégorie MITRE ATT&CK TA0006 : Accès aux informations d'identification.

ID	Tactique	Description
TA0043	Reconnaissance	Collecte des informations en vue de planifier des opérations
TA0042	Développement de ressources	Définit les ressources qu'il est possible d'exploiter
TA0001	Accès initial	Tente d'infiltrer le réseau
TA0002	Exécution	Tente d'exécuter du code malveillant
TA0003	Persistance	Tente de maintenir sa présence dans les systèmes
TA0004	Élévation des privilèges	Tente de s'approprier des permissions supérieures
TA0005	Contournement des défenses	Tente d'échapper à la détection
TA0006	Accès aux identifiants	Tente de voler des noms de compte et des mots de passe
TA0007	Découverte	Tente de cartographier un environnement
TA0008	Latéralisation	Tente de se déplacer à l'intérieur de l'environnement
TA0009	Collecte	Tente de collecter des données pertinentes pour un objectif donné
TA0011	Commande et contrôle	Tente de communiquer avec les systèmes compromis en vue d'en prendre le contrôle
TA0010	Exfiltration	Tente d'exfiltrer des données
TA0040	Impact	Tente de manipuler, d'interrompre ou de détruire des systèmes et des données

Le framework ATT&CK recense diverses techniques dans la catégorie TA0006 : Accès aux informations d'identification.

ID	Technique	Description
T1110	Force brute	• Approche par tâtonnements qui cherche à deviner de façon méthodique le mot de passe en utilisant un outil répétitif ou itératif jusqu'à trouver la bonne combinaison. • Dépend de la puissance de calcul.
T1557	Adversary-in-the-Middle	• Installe un serveur entre la cible et un site authentique. • Redirige l'utilisateur vers le serveur au lieu du site réel. • Intercepte et modifie les informations échangées.
T1555	Identifiants issus de magasins de mots de passe	• Recherche les emplacements où les mots de passe sont couramment stockés en vue de s'approprier des identifiants d'utilisateur.
T1212	Exploitation de l'accès aux informations d'identification	• Tire profit d'une erreur de programmation dans un programme, un service ou le système d'exploitation en vue d'exécuter du code.
T1187	Authentification forcée	• Ex. : Envoi d'une pièce jointe à un e-mail d'hameçonnage ciblé (spearfishing) contenant un lien ou un fichier empoisonné conçu sur mesure. • À l'instant où la cible ouvre le document ou clique sur le lien, tente de s'authentifier et transmet via SMB diverses informations, notamment le hachage des identifiants de l'utilisateur, au serveur contrôlé par l'attaquant.
T1606	Falsification d'identifiants web	• Crée de fausses informations d'identification utilisables pour accéder à des applications ou des services sur Internet. • Cette technique est spécifique en ce que les identifiants sont nouveaux et faux, ils sont créés et non volés.
T1056	Capture de saisie de données	• Exploite diverses méthodes pour capturer la saisie de l'utilisateur en vue de récupérer des identifiants ou des informations. S'appuie sur des moyens transparents ou incite l'utilisateur à renseigner des informations auprès d'un service qu'il pense légitime.
T1556	Modification du processus d'authentification	• Modifie les processus et mécanismes d'authentification en vue d'accéder aux identifiants de l'utilisateur ou de faciliter l'accès illégitime à divers comptes. • L'acteur malveillant peut ainsi s'authentifier auprès d'un service ou d'un système sans compte valide.
T1111	Interception de l'authentification multifacteur (MFA)	• Cible les systèmes de MFA pour accéder aux identifiants. • Ces techniques visent à intercepter et à contourner les outils de MFA.
T1621	Génération de demandes d'authentification multifacteur	• Crée des requêtes de MFA et les envoie aux utilisateurs, par exemple en exploitant la génération automatique de notifications push pour les services de MFA tels que Duo Push, Microsoft Authenticator, Okta, etc.
T1040	Reniflage/analyse réseau	• Utilise l'interface réseau d'un système pour surveiller ou capturer les informations transmises par connexion filaire ou sans fil. • Analyse de manière passive le trafic réseau afin d'accéder aux données ou utilise les ports SPAN pour capturer de grands volumes de données.
T1003	Extraction d'identifiants depuis l'OS	• Extrait en masse les identifiants en vue de récupérer des informations de connexion et d'identification, habituellement sous forme de hachages ou de mots de passe en clair.
T1528	Vol de jeton d'accès aux applications	• Vole les jetons qui permettent de se connecter à des systèmes et à des ressources à distance. • Les adversaires dérobent les jetons d'API d'environnements cloud ou conteneurisés dans le but d'accéder à des données et d'exécuter diverses actions en se servant des permissions associées aux comptes piratés.
T1649	Vol ou falsification de certificats d'authentification	• Les certificats numériques sont souvent utilisés pour signer et chiffrer les messages ou les fichiers, ou servent de support d'authentification. • Vole ou falsifie ces certificats afin de s'authentifier et d'accéder à des systèmes et à des ressources à distance.
T1558	Vol ou falsification de tickets Kerberos	• Kerberos est un protocole d'authentification très répandu dans les environnements modernes de domaines Windows. • Cette technique manipule l'authentification Kerberos en volant ou en falsifiant des tickets du protocole sans avoir accès à un mot de passe.
T1539	Vol de cookie de session web	• Les applications et services web utilisent souvent des cookies de session comme jetons d'authentification une fois que l'utilisateur s'est authentifié une première fois sur un site web. Ces cookies sont généralement valides longtemps, même si l'application web n'est plus utilisée activement. • Cette technique vole les cookies de session des applications ou services web et s'en sert pour accéder au compte d'un utilisateur authentifié sans les identifiants.
T1552	Identifiants non sécurisés	• Les identifiants peuvent être stockés ou égarés dans de nombreux recoins du système. • Cette technique fouille les systèmes compromis à la recherche de ceux stockés de façon non sécurisée.

INDICATEURS DE COMPROMISSION DES IDENTIFIANTS UTILISATEUR

Les acteurs malveillants mettent en œuvre tous les outils à leur disposition pour échapper à la détection. Les organisations comme les utilisateurs doivent impérativement surveiller en continu leurs systèmes afin de détecter les comptes compromis. Les indicateurs de compromissions prennent différentes formes :

- **Trafic sortant inhabituel :** Activité réseau présentant un comportement inhabituel et dans le cadre de laquelle un système ou un réseau envoie de grands volumes de données vers l'extérieur.
- **Horaires et emplacements de connexion inhabituels :** Tentatives de connexion émanant d'un emplacement ou effectuées à une heure qui diffèrent beaucoup des habitudes de l'utilisateur.
- **Déplacement impossible :** Connexions provenant de deux lieux distincts dans un laps de temps suspect.
- **Échecs de connexion multiples :** Plusieurs erreurs de connexion consécutives provenant du même compte au cours d'une très courte période.
- **Accès irrégulier à des données sensibles :** Accès non autorisé ou inhabituel à des informations confidentielles sans permission adéquate.
- **Modifications de configuration suspectes :** Changements inattendus ou non autorisés des stratégies de paramètres système.

STRATÉGIES DE DÉTECTION DES IDENTIFIANTS COMPROMIS

Si les entreprises ne peuvent pas totalement empêcher l'utilisation détournée d'identifiants (la moindre erreur suffit pour récupérer un identifiant valide), certaines stratégies atténuent toutefois le risque associé :

- **Activer la MFA :** La MFA, ou double authentification, impose aux utilisateurs de fournir plusieurs formes d'identification pour se connecter à leur compte. Si les mots de passe protègent les actifs numériques, la MFA ajoute une couche de sécurité qui empêche les utilisateurs non autorisés d'accéder à ces comptes, même lorsqu'ils disposent du bon mot de passe.
- **Établir un profil des menaces :** Cherchez à comprendre l'ennemi et ses tactiques en relevant ses motivations et les capacités techniques spécifiques à votre organisation. En créant un profil pour chacun de vos adversaires, vous identifiez des points communs qui vous aideront à adapter vos défenses, à prioriser les ressources et à mettre en place des mesures proactives. ATT&CK met à jour en continu les tactiques et techniques des cybercriminels connus et émergents afin de fournir aux entreprises des renseignements en temps réel sur leurs adversaires.
- **Déployer l'analyse comportementale des utilisateurs et des entités (UEBA) :** Cette stratégie collecte des informations provenant d'un ensemble de systèmes, applications, réseaux et dispositifs pour définir un modèle comportemental standard. Elle s'appuie sur le machine learning et des analyses avancées pour repérer les comportements inhabituels indicateurs d'une cyberattaque sophistiquée. Cette approche aide les organisations à détecter les techniques de compromission d'identifiants du framework ATT&CK plus rapidement qu'avec des règles.
- **Surveiller la surface d'attaque en continu :** Scrutez activement et en continu vos ressources numériques pour y rechercher des vulnérabilités potentielles (logiciel obsolète, erreurs de configuration) ou des données sensibles mal protégées. Vous identifierez plus facilement les menaces émergentes et les nouveaux points d'entrée. Alignez la catégorisation des vulnérabilités sur le framework ATT&CK pour mieux repérer les lacunes de vos contrôles opérationnels face à certains acteurs.
- **Accélérer la chasse aux menaces :** Traquez activement les activités malveillantes en combinant l'expertise humaine et les analyses avancées pour décortiquer les journaux et les données au lieu de simplement réagir aux alertes. Les analystes peuvent ainsi débusquer les menaces furtives qui ont échappé aux mécanismes de sécurité traditionnels et déjà établi une présence dans le réseau interne.
- **Enrichir votre renseignement stratégique :** ATT&CK fournit des détails sur presque 70 acteurs et groupes malveillants, ainsi que sur les techniques et les tactiques qu'ils emploient pour s'infiltrer dans les réseaux. Exploitez les flux de renseignement stratégique sur les menaces pour mettre au jour les indicateurs de compromission (IoC) potentiels, comme les identifiants compromis, avant qu'une attaque se produise. Cette vision proactive détecte les menaces dans votre environnement en suivant les TTP définies par ATT&CK, les acteurs malveillants, les campagnes de malwares, les bulletins de sécurité et les vulnérabilités émergentes.

DÉTECTION DES IDENTIFIANTS COMPROMIS AVEC LA PLATEFORME ANOMALI

Les entreprises qui s'approprient le framework MITRE ATT&CK comprennent les tactiques, techniques et procédures de leurs adversaires. À l'image de la solution proposée par Anomali, les bons outils s'appuient sur des connaissances éprouvées pour aider les entreprises à passer à l'action.

La plateforme de SOC agentique intelligence-native d'Anomali associe une compréhension et une intégration en profondeur du framework MITRE ATT&CK à un accès inégalé au renseignement d'intérêt cyber pour détecter les comportements inhabituels. Elle orchestre la réponse de manière rapide et efficace afin d'empêcher les acteurs malveillants, même entièrement authentifiés, de nuire à vos systèmes, à vos données et à votre activité.

ANOMALI : LE FUTUR DU SIEM

Anomali est une plateforme novatrice de SOC agentique intelligence-native qui associe une visibilité totale, une agilité sans pareille et des fonctions d'IA à une cyberveille de premier plan au sein d'une même plateforme intégrée. Anomali combine un lac de données entièrement sécurisé, le renseignement d'intérêt cyber et l'IA agentique pour consolider votre stack technologique et donner à vos équipes les moyens d'en faire plus avec moins.

UNE TECHNOLOGIE INNOVANTE ET EFFICACE

Des solutions de cybersécurité pour les organisations de toutes tailles. Des solutions basées sur le renseignement et augmentées par l'IA, pour un monde plus sûr. Voilà comment définir Anomali.

Découvrez comment Anomali vous aide à stopper les compromissions d'identifiants dans votre organisation — réservez une démonstration.

VOIR ANOMALI EN ACTION

Demander une démo