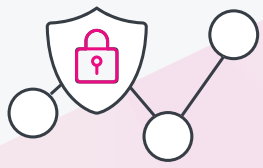
Les principales détections de menaces de cybersécurité avec **Splunk et MITRE ATT&CK**

Classez, identifiez et évaluez les menaces avec MITRE ATT&CK, supervisez et répondez avec Splunk



splunk>

Sommaire

Avant-propos

La migration vers le cloud et la transformation numérique sont deux tendances en plein essor. Face à ces évolutions, les responsables de la sécurité doivent adopter une approche orientée données pour sécuriser leur organisation.

Dans ce monde complexe et imprévisible, Splunk est essentiel pour assurer la sécurité et la résilience des entreprises comme la vôtre. Splunk vous permet en effet de détecter et répondre plus rapidement aux menaces, évolue avec vos besoins et soutient votre innovation. La sécurité et la résilience de votre organisation repose sur deux choses : la communication entre vos réseaux et vos outils de sécurité, qui doivent analyser toutes vos données et fournir des informations utiles.

Pour être résilient, nous pensons que vous devez avoir une visibilité sur l'intégralité de votre infrastructure et sur toutes ses données, avec une fidélité parfaite. Vous devez disposer d'opérations de sécurité suffisamment flexibles pour vous adapter aux nouvelles menaces, aux technologies émergentes et aux volumes de données en constante augmentation.

Vous avez besoin de techniques de détection et de réponse plus rapides. Vous pouvez le faire en exploitant toutes vos données, en automatisant des processus pour identifier les nouvelles menaces en un temps record et en donnant à votre équipe les moyens de se concentrer sur ses vraies priorités.

C'est ainsi que nous améliorons notre cyber-résilience, qui nous permet d'accélérer la croissance de l'entreprise, d'assurer la confidentialité et la conformité, et de continuer à innover.

Nous sommes déterminés à résoudre les défis des clients dans ce monde changeant en renforçant nos offres de sécurité et d'observabilité. C'est pourquoi nous avons créé cette liste de tactiques MITRE ATT&CK, accompagnées des détections correspondantes et de scénarios analytiques de l'équipe Splunk de recherche sur les menaces (STRT). L'objectif : lutter contre les dernières menaces, afin que vous puissiez faire preuve de résilience face à la complexité et à l'incertitude.

Patrick Coughlin
VP, Stratégie et spécialisation GTM

Les technologies évoluent et les cybercriminels sont, eux aussi, plus sophistiqués qu'auparavant. Les acteurs malveillants font constamment évoluer leur approche : du chiffrement et exfiltration des données à la double extorsion, lors de laquelle ils divulguent des données confidentielles si leurs demandes ne sont pas satisfaites.

Si ça ne suffisait pas, la cybercriminalité à motivation financière est également en hausse ; elle devance même les activités soutenues par des États-nations et représente plus de 80 % des intrusions. Cette vague d'assauts devrait coûter aux organisations 10 500 milliards de dollars par an d'ici 2025. Les attaquants profitent également de vulnérabilités dans les chaînes d'approvisionnement, ciblent les faiblesses opérationnelles des organisations et exploitent les nouvelles surfaces d'attaque créées par les services cloud.

Pour nous protéger contre ces cybermenaces, nous devons repenser et renforcer nos défenses de sécurité, et faire preuve de résilience face aux menaces en constante évolution. Dans cet e-book, nous examinons une sélection de tactiques et techniques de menaces définies par le framework MITRE ATT&CK. Nous allons voir comment les équipes de sécurité peuvent être mieux préparées (et équipées) grâce à Splunk.

Découvrez MITRE ATT&CK

MITRE ATT&CK est une base de connaissances sur les tactiques, techniques et procédures (TTP) courantes employées par les acteurs malveillants. Elle représente un véritable manuel des TTP vues et signalées dans le monde réel. Les organisations se réfèrent à MITRE ATT&CK pour classer les attaques, évaluer les risques et améliorer leur posture de sécurité globale. Cela leur permet de mieux comprendre le comportement des adversaires, afin d'identifier et mettre en œuvre des mécanismes de détection pertinents.

Essentiellement, ATT&CK est un langage standard, facile d'accès et mondialement reconnu auquel les spécialistes de la sécurité peuvent se référer pour obtenir de la threat intelligence et renforcer leur posture de sécurité.

Le cadre MITRE ATT&CK peut également aider à :

- informer le centre des opérations de sécurité (SOC) pour mieux hiérarchiser les alertes et les détections ;
- identifier et évaluer les risques, maîtriser les écarts et l'exposition acceptable ;
- fournir un cadre pour la gouvernance et la maturité de la sécurité ;
- recommander de nouvelles sources de données basées sur une réduction quantifiable des risques ;
- mieux visualiser les chemins d'attaque, améliorer les connaissances et les compétences d'une équipe de sécurité.

La solution idéale : ATT&CK + Splunk

Quand les menaces évoluent, le framework ATT&CK évolue également. Pour faire face aux menaces nouvelles et émergentes, les équipes de sécurité doivent adapter et mettre à jour leurs capacités de détection et de réponse au même rythme que leurs adversaires. Splunk Enterprise Security (ES), Splunk Security Essentials (SSE), et les Splunk Enterprise Security Content Updates (ESCU) aident les organisations à se préparer aux menaces. Ces solutions associent le framework MITRE ATT&CK à des scénarios analytiques Splunk : des guides de sécurité qui fournissent du contexte sur les techniques d'attaque et les menaces, accompagnés de recherches Splunk, d'outils de machine learning et de playbooks SOAR (orchestration, automatisation et réponse de sécurité).

Ces composants puissants fonctionnent de concert pour vous aider à détecter, analyser et prendre en charge les signes de menaces dans votre environnement. Des mises à jour périodiques vous aident à améliorer continuellement vos défenses. Les scénarios analytiques complètent les indicateurs de compromission (IOC) traditionnels, qui sont à la traîne et souvent éphémères. Au moment où vous les détectez, les attaquants ont généralement modifié leurs URL, leurs adresses IP et autres artefacts, rendant les IOC obsolètes. En revanche, les ESCU vous aident à superviser les tactiques et techniques habituelles et constantes de l'adversaire. Une fois que vous avez identifié les signes de ces menaces dans votre environnement, des recherches et des playbooks vous aident à décider s'il faut investiguer davantage.

Cas d'utilisation de MITRE ATT&CK

Différentes applications de la taxonomie MITRE ATT&CK dans Splunk

Vous trouverez ci-dessous quelques exemples d'exploitation du framework ATT&CK dans Splunk :

- **Cartographie des contrôles de défense**
  Les équipes de sécurité peuvent acquérir une vision claire des outils, systèmes et stratégies de défense lorsqu'ils sont référencés selon les tactiques et techniques ATT&CK et les menaces qui leur sont associées. Il est très facile d'ajouter des mots-clés MITRE ATT&CK aux recherches de corrélation de Splunk Enterprise Security pour annoter les événements et mieux les comprendre.

- **Traque des menaces**
  Les équipes de sécurité peuvent planifier leurs défenses selon le modèle ATT&CK pour identifier les lacunes critiques de leur infrastructure de sécurité et ainsi détecter des activités menaçantes précédemment négligées. Avec Splunk Security Essentials et le framework MITRE ATT&CK, les chasseurs de menaces peuvent identifier les lacunes dans la couverture afin d'orienter le développement de détections, ou imaginer de nouvelles recherches et scénarios d'utilisation afin de combler les lacunes existantes.

- **Investigation**
  La réponse aux incidents peut se référer au framework ATT&CK pour mieux traiter les vulnérabilités potentielles et valider certaines mesures tout en détectant les erreurs de configuration et autres défauts opérationnels.

- **Identification des acteurs et des groupes de menaces**
  Les équipes de sécurité peuvent rapprocher les comportements documentés des acteurs et groupes malveillants.

Découvrez l'équipe Splunk de recherche sur les menaces

Rien de tout cela ne serait possible sans l'équipe Splunk de recherche sur les menaces, qui travaille sans relâche pour améliorer les offres de sécurité de Splunk en créant des scénarios d'utilisation, des recherches de détection et des playbooks prêts à l'emploi. Toutes les deux semaines, leurs recherches sont regroupées et partagées avec la communauté Splunk. Ce contenu varié, qui comprend aussi bien des détections de menaces que des instructions étape par étape, est accessible dans Splunk. L'époque où il fallait rédiger des recherches personnalisées et tester de nouvelles détections est révolue. Désormais, les équipes peuvent mettre en œuvre des détections prêtes à l'emploi pour accélérer les investigations. Ces recherches jouent un rôle central dans le confinement et la résolution rapides d'une menace, et le temps qu'elles font gagner aux équipes de sécurité leur permet de se consacrer à des tâches essentielles.

En conclusion ? Les recherches sur les menaces de Splunk aident les équipes de sécurité à exploiter tout le potentiel de leur investissement Splunk. Elles intègrent le framework MITRE ATT&CK de façon transparente en le traduisant en détections de menaces pour une plus grande couverture de sécurité, et elles enrichissent certaines capacités de sécurité avec des connaissances et des recherches d'experts sur les dernières menaces et tendances de sécurité.

L'objectif final de l'utilisation de MITRE ATT&CK dans votre environnement Splunk est d'apporter des informations et une valeur supplémentaires à votre déploiement dans le contexte du framework ATT&CK. Face à l'évolution constante des besoins et des détections de sécurité, ce cadre permet d'appuyer les travaux actuels et futurs sur des applications pertinentes et réelles.

Tactiques MITRE ATT&CK

Vous souhaitez améliorer votre réponse aux menaces ?
Nous décrivons ci-dessous les principales tactiques et techniques de menaces MITRE ATT&CK, accompagnées d'exemples d'approches de réponse utilisant Splunk.

Reconnaissance (TA0043)

Tactique : recueillir des informations

Pourquoi ces menaces existent-elles ?

La reconnaissance porte très bien son nom : c'est une attaque axée sur la collecte et la recherche d'informations utiles sur une cible, ses systèmes et/ou son organisation. Elle peut impliquer toute une série de techniques – ingénierie sociale, infiltration du réseau et supervision physique. Les informations obtenues concernent généralement l'infrastructure de l'organisation et les membres clés de son personnel. Ces informations sont exploitées par le malfaiteur pour faciliter d'autres phases de la cyber kill-chain.
La cyber kill-chain, outil normalisé comparable à MITRE ATT&CK, décrit les étapes d'une attaque de la reconnaissance à l'exfiltration de données. Elle a été élaborée par la société de sécurité internationale Lockheed Martin.

Comment ces menaces sont-elles exécutées ?

L'objectif est l'acquisition d'informations sur l'identité de la victime et sur ses réseaux, de données administratives et de détails concernant les opérations de l'organisation.

Pour y parvenir, les malfaiteurs interagissent souvent directement avec le système grâce à des techniques telles que le balayage de ports, le reniflage de paquets et le balayage par ping. C'est ce qu'on appelle la « reconnaissance active ». Elle est généralement plus rapide et plus précise qu'une approche « passive », dans laquelle l'attaquant recherche des informations sur Internet, à l'aide de services d'information publics comme « Whois », d'outils comme Wireshark et Shodan, ou de méthodes comme l'identification des systèmes d'exploitation par fingerprinting.

Décomposons les étapes potentielles de cette tactique : les techniques identifiées par le framework MITRE ATT&CK incluent la collecte initiale d'informations, l'évaluation de la portée du réseau de la cible, la recherche de points d'accès et de ports ouverts, ainsi que la cartographie du réseau de l'organisation. Toutes ces étapes assurent la collecte d'informations visant à renseigner l'adversaire et à l'aider à sélectionner ou identifier sa cible.

Détecter et répondre avec Splunk

Détection de menace Splunk :
Présence d'outils malveillants sur le terminal

- **Scénario analytique Splunk**
  Supervision des logiciels non autorisés, XMRig, Ransomware SamSam, Processus inhabituels
- **Tactiques MITRE ATT&CK**
  Reconnaissance, accès aux identifiants, évitement des mécanismes de défense
- **Techniques MITRE ATT&CK**
  Imitation d'un nom ou d'un emplacement légitime, usurpation d'identité, déversement d'identifiants du système d'exploitation, scan actif
- **Phase de la kill-chain**
  Installation, commande et contrôle, actions sur les objectifs
- **Fonctionnement**
  Cette détection de menace recherche l'exécution d'outils d'attaque couramment utilisés sur un terminal.

Exécution (TA0002)

Tactique de menace : exécution d'un code malveillant

Pourquoi ces menaces existent-elles ?

L'exécution des menaces désigne les techniques utilisées par un attaquant pour exécuter ou contrôler un code malveillant sur un système local ou distant. Les techniques qui exécutent du code malveillant sont souvent associées à d'autres tactiques, comme l'infiltration d'un réseau ou le vol de données. Par exemple, un adversaire peut utiliser un outil d'accès à distance pour exécuter un script PowerShell qui effectue la découverte du système à distance.

Comment ces menaces sont-elles exécutées ?

Les adversaires peuvent exploiter les interpréteurs de commandes et des scripts pour exécuter des commandes, comme PowerShell, AppleScript, Unix, Windows et Python. Ces interfaces et langages permettent aux utilisateurs d'interagir avec les systèmes informatiques et sont communs à de nombreuses plateformes différentes. Les attaquants peuvent les utiliser pour découvrir des informations, exécuter du code, ouvrir des fenêtres, envoyer des frappes au clavier et interagir avec toutes les applications ouvertes ou presque, localement ou à distance. Certaines commandes shell offrent aux adversaires un accès complet à quasiment tous les aspects du système de la cible.

Les malfaiteurs peuvent également exploiter les conteneurs pour exécuter du code et des systèmes de contrôle. En abusant du service d'administration des conteneurs d'un environnement, ils peuvent les contrôler à distance. Une fois un conteneur déployé dans un environnement, ils peuvent ensuite exécuter du code et échapper aux défenses de l'intérieur.

Une autre tactique d'exécution consiste à abuser de la planification des tâches pour faciliter l'exécution initiale ou récurrente de code malveillant à une date et une heure définies. Les pirates peuvent également déployer des charges utiles malveillantes via des modules partagés ou accéder à des suites logicielles tierces installées au sein d'un réseau d'entreprise. Ils vont également exploiter des services système ou des daemons pour exécuter des commandes ou des programmes, et recourir à l'ingénierie sociale pour inciter un utilisateur à effectuer des actions spécifiques, comme cliquer sur un faux lien ou télécharger un fichier malveillant.

Détecter et répondre avec Splunk

Détection de menace Splunk : Linux – décodage Base64 en shell

- **Scénario analytique Splunk**
  Linux hors territoire
- **Tactiques MITRE ATT&CK**
  Évitement des mécanismes de défense, exécution
- **Techniques de MITRE ATT&CK**
  Fichiers ou informations obscurcis, shell Unix
- **Phase de la kill-chain**
  Livraison, exploitation
- **Fonctionnement**
  Cette identification de menace recherche le code base64 décodé et transmis à un shell Linux. L'encodage base64 est souvent exploité pour transporter des charges utiles malveillantes déguisées en code légitime.

Persistance (TA0003)

Tactique de menace : maintien de l'emprise

Pourquoi ces menaces existent-elles ?

Une fois qu'un acteur malveillant pénètre dans les systèmes d'une cible, la persistance est invariablement payante ; elle éclipse presque toutes les autres tactiques du playbook de l'attaquant. Pour maintenir son emprise, il doit anticiper un certain nombre d'interruptions pouvant le priver de son accès, comme les redémarrages du système ou la modification des identifiants. Cette tactique couvre les modifications d'accès, d'action ou de configuration qui permettent à l'auteur de se déplacer latéralement (et, surtout, discrètement) au sein du compte ou du système compromis, en remplaçant ou en détournant le code légitime avec le sien.

Comment ces menaces sont-elles exécutées ?

Les adversaires recourent souvent à la manipulation de comptes pour conserver leur accès. Ils peuvent modifier les identifiants ou les groupes d'autorisations, puis effectuer des mises à jour itératives des mots de passe pour contourner les politiques de renouvellement obligatoire. Ils peuvent également ajouter des identifiants de compte, modifier des clés SSH (Secure Socket Shell) autorisées ou enregistrer des appareils sur des comptes qu'ils contrôlent.

Ils déposent des scripts qui sont automatiquement exécutés au démarrage ou à l'initialisation de la connexion pour établir la persistance. Les scripts d'initialisation peuvent servir à exécuter des fonctions administratives, qui vont ensuite exécuter d'autres programmes ou envoyer des informations à un serveur de journalisation interne. Ces scripts varient en fonction du système d'exploitation et selon leur application locale ou à distance.

Les pirates peuvent également créer un nouveau compte pour conserver l'accès aux systèmes victimes, qu'il s'agisse d'un compte local, de domaine ou cloud. Ils modifient les processus au niveau du système pour exécuter des charges utiles malveillantes de façon répétée, à l'aide d'agents de lancement, de services système, de services Windows et de daemons de lancement.

Détecter et répondre avec Splunk

Détection de menace Splunk :
O365 Ajout d'un principal de service

- **Scénarios analytiques Splunk**
  Détections Office 365, Abus d'identifiants cloud fédérés
- **Tactiques MITRE ATT&CK**
  Persistance
- **Techniques MITRE ATT&CK**
  Compte cloud, création de compte
- **Phase de la kill-chain**
  Exploitation
- **Fonctionnement**
  Cette détection identifie la création d'un nouveau paramètre en signalant un événement corrélé spécifique. Bien que la création d'une nouvelle fédération ne soit pas nécessairement malveillante, l'événement doit être suivi de près, car il peut trahir un abus d'identifiants.

Acquisition de privilèges (TA0004)

Tactique de menace : obtention d'autorisations de niveau supérieur

Pourquoi ces menaces existent-elles ?

Quand des malfaiteurs infiltrent et parcourent un réseau avec un accès non privilégié, ils doivent parfois acquérir des autorisations supérieures pour atteindre leurs objectifs. Les techniques qu'ils utilisent pour obtenir ces autorisations sont regroupées sous l'intitulé d'acquisition de privilèges. Les approches courantes consistent à tirer parti des faiblesses du système, des erreurs de configuration et des vulnérabilités.

Comment ces menaces sont-elles exécutées ?

En tirant parti de vulnérabilités présentes dans le système de la cible, les adversaires peuvent obtenir un accès élevé tel que le niveau SYSTEM/root ou le statut d'administrateur local, un compte disposant d'un accès de type administrateur ou un compte ayant accès à un système spécifique ou remplissant une fonction précise. Les techniques utilisées pour obtenir des autorisations de niveau supérieur recoupent souvent les techniques de persistance, car les fonctionnalités qui permettent à un pirate de persister peuvent également s'exécuter à des fins d'acquisition.

Les auteurs de menaces contournent les mécanismes conçus pour contrôler l'acquisition de privilèges en utilisant diverses méthodes qui exploitent les mécanismes de contrôle intégrés. Quelques méthodes : abus des configurations dans lesquelles une application définit l'identité de l'utilisateur et du groupe afin d'exécuter du code dans un contexte d'utilisateur différent (et potentiellement plus privilégié), contournement des mécanismes de contrôle de compte d'utilisateur (UAC) et mise en cache sudo et/ou utilisation du fichier sudoers.

Les adversaires peuvent encore modifier les jetons d'accès pour qu'ils opèrent sous un autre utilisateur ou contexte de sécurité système, afin d'accomplir des actions et de contourner les contrôles d'accès. En configurant les paramètres système, ils peuvent exécuter automatiquement un programme au démarrage ou à l'ouverture de session pour maintenir la persistance ou obtenir des privilèges de niveau supérieur. D'autres techniques consistent à falsifier des processus au niveau du système pour exécuter à plusieurs reprises des charges utiles malveillantes, à modifier des paramètres de configuration d'un domaine et à utiliser des mécanismes système qui déclenchent l'exécution en fonction d'événements spécifiques.

Détecter et répondre avec Splunk

Détection de menace Splunk :
Authentification PowerShell réussie d'Azure AD

- **Scénarios analytiques Splunk**
  Acquisition de compte Azure Active Directory
- **Tactiques MITRE ATT&CK**
  Évitement des mécanismes de défense, persistance, acquisition de privilèges, accès initial
- **Techniques MITRE ATT&CK**
  Comptes valides, Comptes cloud
- **Phase de la kill-chain**
  Exploitation
- **Fonctionnement**
  Cette détection de menace identifie un événement d'authentification réussi auprès d'un locataire Azure AD à l'aide de commandlets PowerShell. Ce comportement est rare chez les utilisateurs non administrateurs. Après avoir compromis un compte dans Azure AD, les adversaires et les red teams exécutent des techniques d'énumération et de découverte. Pour ce faire, ils peuvent, par exemple, tirer parti des modules PowerShell natifs.

Évitement des mécanismes de défense (TA0005)

Tactique de menace : éviter d'être détecté

Pourquoi ces menaces existent-elles ?

L'évitement des mécanismes de défense est une tactique visant à éviter la détection à travers les différentes étapes d'une attaque. Elle couvre un large éventail de techniques, comme la désinstallation ou la désactivation des logiciels de sécurité de la cible, et l'obscurcissement ou le chiffrement des données et des scripts. Pour échapper à la détection, les acteurs de la menace vont également exploiter des processus de confiance pour cacher et dissimuler leurs logiciels malveillants.

Comment ces menaces sont-elles exécutées ?

Les acteurs malveillants essaient d'échapper à la détection de différentes manières, selon le type d'attaque et son stade. Ils exploitent toutes les vulnérabilités de l'environnement de la victime, abusent des informations d'identification, modifient les autorisations et les attributs, détournent les systèmes d'exploitation, injectent du code et entravent ou désactivent les outils de sécurité et autres mécanismes de défense. En cours de route, ils font tout ce qu'ils peuvent pour dissimuler et supprimer les preuves de leur présence et de leur comportement dans l'environnement de la cible.

Pour échapper aux défenses, les adversaires modifient les paramètres, les accès et autres éléments de l'environnement de la victime. En modifiant les paramètres de configuration d'un domaine, ils acquièrent un outil centralisé pour gérer les opérations et les interactions des machines et des comptes sur le réseau. En modifiant les jetons d'accès, ils peuvent opérer sous un autre utilisateur ou dans un contexte de sécurité système, afin d'accomplir des actions et de contourner les contrôles d'accès. Ils modifient et altèrent également les mécanismes défensifs – pare-feux et protections antivirus – et les détections qui pourraient révéler leur activité.

En plus de modifier les autorisations et les attributs, les adversaires tentent de dissimuler les preuves de leur comportement en abusant des fonctionnalités des systèmes d'exploitation et en manipulant les caractéristiques de leurs artefacts pour arborer un visage légitime. Les acteurs malveillants peuvent également abuser des utilitaires d'exécution de commandes afin de contourner les restrictions de sécurité et d'exécuter leurs propres charges utiles malveillantes en détournant la façon dont les systèmes d'exploitation exécutent les programmes – et ce n'est qu'un début.

Détecter et répondre avec Splunk

Détection de menace Splunk :
Circle CI – Désactivation de tâche de sécurité

- **Scénario analytique Splunk**
  Dev Sec Ops
- **Tactiques MITRE ATT&CK**
  Persistance
- **Techniques MITRE ATT&CK**
  Binaire de logiciel client compromis
- **Phase de la kill-chain**
  Actions sur les objectifs
- **Fonctionnement**
  Cette détection de menace recherche les tâches CircleCI qui ont été désactivées à la phase de compilation et fournit à l'analyste le nom de la tâche et l'utilisateur qui l'a désactivée. Cette action peut avoir pour but d'éviter les défenses ou de perturber les services.

Accès aux identifiants (TA0006)

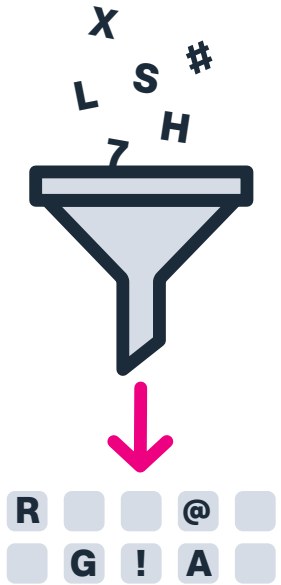
Tactique de menace : vol des détails du compte

Pourquoi ces menaces existent-elles ?

L'accès aux identifiants comprend différentes techniques visant à voler des informations de compte (noms d'utilisateur et mots de passe). De nombreuses techniques permettent d'obtenir des informations d'identification, comme l'enregistrement de frappe et le déversement d'identifiants. En plus d'être extrêmement efficace, ce type d'attaque est beaucoup plus difficile à repérer que d'autres techniques d'accès initial, car il apparaît comme une utilisation légitime de compte d'utilisateur. C'est aussi une attaque extrêmement rentable et efficace pour accéder aux comptes d'utilisateurs et aux informations.

Comment ces menaces sont-elles exécutées ?

Lors d'une attaque d'injection d'identifiants à grande échelle, l'attaquant met en place un bot capable de se connecter automatiquement et simultanément à plusieurs comptes d'utilisateurs, tout en simulant des adresses IP différentes. Les informations d'identification volées sont ensuite testées sur une longue liste de sites web, pour repérer les connexions réussies et obtenir des informations personnellement identifiables, des données de cartes de crédit ou autres données précieuses. En exécutant ce processus en parallèle sur plusieurs canaux, l'adversaire évite de devoir se connecter à plusieurs reprises au même service. Les informations de compte sont également conservées pour être réutilisées, par exemple dans le cadre d'attaques par phishing ou d'autres transactions permises par le service compromis.



Détecter et répondre avec Splunk

Détection de menace Splunk : 0365 Désactivation de la MFA

- **Scénario analytique Splunk**
  Détections Office 365
- **Tactiques MITRE ATT&CK**
  Accès aux identifiants, évitement des mécanismes de défense, persistance
- **Techniques MITRE ATT&CK**
  Modification du processus d'authentification
- **Phase de la kill-chain**
  Exploitation
- **Fonctionnement**
  Cette détection de menace repère la désactivation de l'authentification multifacteurs. Elle sait à quel moment cela s'est produit, quelle entité en est l'autrice et quel utilisateur était visé.

Découverte (TA0007)

Tactique de menace : compréhension de votre environnement

Pourquoi ces menaces existent-elles ?

La découverte comprend des techniques visant à acquérir des connaissances sur le système et le réseau interne de la cible. Ces techniques aident les pirates à observer l'environnement et à s'orienter avant de décider comment agir. Elles leur permettent également d'établir leur champ de contrôle et l'environnement de leur point d'entrée pour le mettre au service de leur objectif. Les outils natifs du système d'exploitation sont souvent exploités pour atteindre cet objectif de collecte d'informations post-compromission.

Comment ces menaces sont-elles exécutées ?

Les pirates sont plus performants que jamais quand il s'agit d'infiltrer les systèmes. Et une fois qu'ils ont accès au réseau d'une entreprise, les pirates restent souvent dans l'ombre pour effectuer des opérations de reconnaissance. Ils observent et apprennent en silence comment exploiter les failles de sécurité (les réglages par défaut, notamment) pour atteindre leurs objectifs par surprise. Dans le framework MITRE ATT&CK, cette traque numérique est connue sous le nom de « découverte ».

Les entreprises intelligentes peuvent atténuer l'impact d'une violation en empêchant les intrus de s'orienter. De nombreux dirigeants connaissent les méthodes des attaquants pour violer les systèmes. En comprenant la phase de découverte d'une cyberattaque, vous pouvez mieux vous préparer à contrer ces activités et leurs conséquences en aval. Les actions à entreprendre sont tactiques mais elles peuvent faire toute la différence en permettant à l'entreprise de maintenir leur stratégie et leurs opérations.

Détecter et répondre avec Splunk

Détection de menace Splunk : Windows AdFind Exe

- **Scénario analytique Splunk**
  Groupe NOBELIUM, Découverte d'approbation de domaine
- **Tactiques MITRE ATT&CK**
  Découverte
- **Techniques MITRE ATT&CK**
  Découverte de système à distance
- **Phase de la kill-chain**
  Exploitation
- **Fonctionnement**
  Cette détection de menace recherche l'exécution d'adfind.exe avec les arguments de ligne de commande qu'elle utilise par défaut. Elle cible en particulier les fonctions de filtrage ou de recherche.

Collecte (TA0009)

Tactique de menace : obtention de données pertinentes sur la cible

Pourquoi ces menaces existent-elles ?

Peu importe la ruse, les acteurs malveillants ne peuvent pas agir seuls ; pour réussir une attaque, ils doivent puiser dans – ou, plus précisément, collecter – des informations clés au cours de leur campagne. Cette tactique est connue sous le nom de « collecte » et implique plusieurs techniques axées sur la recherche d'informations sensibles et/ou propriétaires. En bout de ligne, les données collectées sont exfiltrées et exploitées par l'attaquant lors d'autres phases de l'attaque. Les cibles courantes incluent les disques, les navigateurs, les contenus audio et vidéo et les e-mails. Quant aux méthodes de collecte, elles vont des captures d'écran à la saisie au clavier.

Comment ces menaces sont-elles exécutées ?

Un malfaiteur dispose d'une myriade de moyens pour collecter des informations numériques (ou physiques) sensibles et personnelles pour assister ses opérations. Il peut espionner les navigateurs et les périphériques audio, pirater des comptes de messagerie, voler les identifiants de connexion et plus encore. Une fois qu'il a obtenu l'accès au système de la cible, il peut ensuite cibler des vulnérabilités et se déplacer latéralement sur le réseau afin de collecter et de transférer des données entre le système compromis et le sien.

Détecter et répondre avec Splunk

Détection de menace Splunk : Utilisation anormale de 7zip

- **Scénario analytique Splunk**
  Cobalt Strike, Groupe NOBELIUM
- **Tactiques MITRE ATT&CK**
  Collecte
- **Techniques MITRE ATT&CK**
  Archivage via l'utilitaire, archivage des données collectées
- **Phase de la kill-chain**
  Exploitation
- **Fonctionnement**
  La détection des menaces identifie la génération d'un 7z.exe à partir de Rundll32.exe ou Dllhost.exe. On suppose que l'adversaire a introduit 7z.exe et 7z.dll. Une couverture supplémentaire peut être nécessaire pour identifier le comportement des instances renommées de 7z.exe.

Déplacement latéral (TA0008)

Tactique de menace : déplacement dans votre environnement

Pourquoi ces menaces existent-elles ?

À ce stade, l'auteur de la menace tente de se déplacer rapidement (mais de façon systématique) dans votre environnement. Et il vise à couvrir un maximum de terrain par tous les moyens possibles une fois qu'il a infiltré le réseau.

Pour mener à bien leur mission, les acteurs malveillants doivent inspecter le réseau pour localiser leur cible et y accéder. À ce stade, ils appliquent de nombreuses techniques visant à entrer dans des systèmes distants et à les contrôler. Cela implique souvent de parcourir plusieurs systèmes et comptes par déplacement latéral pour installer des outils d'accès à distance. Pour y parvenir, ils utilisent souvent des identifiants légitimes et des outils natifs du réseau et du système d'exploitation pour couvrir furtivement leurs allées et venues.

Comment ces menaces sont-elles exécutées ?

Les malfaiteurs s'appuient sur une variété de techniques pour se déplacer furtivement dans un environnement. Une fois qu'ils ont infiltré un réseau, ils peuvent exploiter une vulnérabilité logicielle – souvent une faille dans un programme, un service ou dans le système d'exploitation lui-même – pour obtenir un accès non autorisé à d'autres systèmes internes.

Les adversaires peuvent également utiliser des techniques de harponnage interne pour accéder à des informations supplémentaires ou exploiter des utilisateurs ayant déjà accès à des comptes ou à des systèmes dans l'environnement. Ils essaient souvent d'inciter une personne peu méfiante à cliquer sur un lien malveillant ou à télécharger une pièce jointe infectée, qui servira de tremplin pour un mouvement latéral vers d'autres parties du réseau.

Les acteurs malveillants peuvent également détourner les sessions préexistantes des utilisateurs pour se déplacer latéralement sur un réseau. Ils utilisent ensuite des informations d'identification valides pour se connecter à un service spécialement conçu pour accepter les connexions à distance. Ils peuvent également utiliser d'autres éléments d'authentification – hachages de mots de passe, tickets Kerberos ou jetons d'accès aux applications – pour contourner les contrôles d'accès normaux au système et se déplacer latéralement.

Détecter et répondre avec Splunk

Détection de menace Splunk : Paramètres de la ligne de commande PassTheTicket Mimikatz

- **Scénario analytique Splunk**
  Attaques Kerberos Active Directory
- **Tactiques MITRE ATT&CK**
  Évitement des mécanismes de défense, Déplacement latéral
- **Techniques MITRE ATT&CK**
  Utilisation de moyen d'authentification alternatif, Pass the Ticket
- **Phase de la kill-chain**
  Exploitation
- **Fonctionnement**
  L'analyse suivante recherche l'utilisation des paramètres de ligne de commande Mimikatz, employés pour exécuter les attaques « PassTheTicket ». Les red teams et les adversaires peuvent utiliser la technique Pass the ticket afin d'exploiter des tickets Kerberos volés pour se déplacer latéralement dans un environnement, en contournant les contrôles d'accès normaux au système.

Commande et contrôle (TA0011)

Tactique de menace : contrôle des systèmes compromis

Pourquoi ces menaces existent-elles ?

Dans la phase de commande et de contrôle, les adversaires tentent de communiquer avec les systèmes qu'ils ont infectés et compromis. Leur objectif est de prendre le contrôle total de leur cible et de les utiliser à des fins néfastes, souvent via des attaques par phishing, des logiciels vulnérables ou des failles de sécurité dans les plug-ins de navigateur.

Une fois qu'ils ont infecté un appareil ou un système sur le réseau, ils utilisent une série de techniques pour communiquer avec les systèmes compromis au sein d'un réseau victime. Lors de cette phase, il n'est pas non plus rare que les adversaires imitent des niveaux de trafic normaux en utilisant des protocoles de couche d'application pour éviter de déclencher des alertes de sécurité, échapper au filtrage du réseau et, globalement, esquiver tout autre examen indésirable.

Comment ces menaces sont-elles exécutées ?

Le but de cette phase est d'établir une communication entre la machine infectée et le serveur des pirates, pour envoyer un ensemble d'instructions visant à prendre le contrôle complet de l'ensemble du réseau ou du système. Une fois qu'ils ont réussi à compromettre un appareil, l'ordinateur infecté exécute les commandes du serveur malveillant pour se connecter à autant d'appareils que possible.

Toutefois, comme ils infectent tout un réseau, les adversaires doivent aussi brouiller les pistes. Ils sont donc contraints d'utiliser une foule de techniques furtives pour dissimuler les activités de commande et de contrôle. L'une d'elles consiste à intégrer des commandes dans le trafic entre le client et le serveur des protocoles de la couche application – Web, transfert de fichier, protocoles de messagerie ou DNS – pour se fondre dans le trafic existant. Une autre consiste à communiquer via un support amovible : les adversaires peuvent alors exécuter des fonctions de commande et de contrôle sur des réseaux potentiellement déconnectés à l'aide de simples clés USB pour transférer des commandes entre des systèmes compromis.

Les adversaires peuvent également prendre discrètement le contrôle d'un réseau en ajoutant simplement des données indésirables au trafic de protocole, en utilisant la stéganographie ou en se faisant passer pour des protocoles légitimes. D'autre part, plutôt que de compter sur des protections inhérentes, ils peuvent utiliser un algorithme de chiffrement connu pour dissimuler le trafic de commande et de contrôle.

Détecter et répondre avec Splunk

Détection de menace Splunk : Trafic TOR

- **Scénario analytique Splunk**
  Trafic interdit autorisé ou incompatibilité de protocole, Ransomware, Commande et contrôle
- **Tactiques MITRE ATT&CK**
  Commande et contrôle
- **Techniques MITRE ATT&CK**
  Protocole de la couche application, protocoles web
- **Phase de la kill-chain**
  Commande et contrôle
- **Fonctionnement**
  Cette détection de menace recherche le trafic réseau TOR (The Onion Router), un réseau d'anonymat bénin qui peut être exploité par des attaquants malveillants à diverses fins néfastes.

Exfiltration (TA0010)

Tactique de menace : vol de données propriétaires

Pourquoi ces menaces existent-elles ?

Au stade de l'exfiltration, les adversaires utilisent une variété de méthodes sophistiquées pour voler des données de votre réseau. Une fois qu'ils ont collecté toutes les données souhaitées, ils trouvent souvent des moyens créatifs de les packager furtivement, notamment par compression et chiffrement, pour éviter toute détection lors de leur exfiltration du réseau. Pour s'enfuir avec des données en toute discrétion, certains les transfèrent sur leurs canaux de commande et contrôle ou limitent la taille des paquets transmis.

Comment ces menaces sont-elles exécutées ?

Les adversaires possèdent d'innombrables ruses pour exfiltrer des données sensibles d'une organisation. Ils peuvent notamment utiliser des processus automatisés pour transférer les données après la phase de « collecte ». Les malfaiteurs peuvent également déplacer les données en paquets de taille définie, inférieure à un certain seuil, plutôt qu'exfiltrer des fichiers entiers, afin d'éviter de déclencher diverses alertes de transfert réseau et de sécurité.

Les acteurs malveillants peuvent encore s'appuyer sur des services web externes légitimes pour exfiltrer des données. Ces services populaires peuvent offrir une excellente couverture, tout simplement parce que l'organisation ciblée les utilisait probablement déjà avant l'attaque.

Les adversaires peuvent également tenter d'exfiltrer des données via un support physique, comme une clé USB amovible, un disque dur externe, un téléphone portable, un lecteur MP3 ou autre périphérique de stockage courant, qui devient alors le point d'exfiltration final avant la suppression complète des données sur le système ciblé. Ils peuvent également voler des données via des transferts planifiés à des moments spécifiques de la journée ou à certains intervalles. En se fondant dans les tendances de trafic habituelles, ces transferts bénéficient d'une couverture parfaite.

Détecter et répondre avec Splunk

Détection de menace Splunk : Windows PowerShell se connecte à Internet avec une fenêtre masquée

- **Scénario analytique Splunk**
  Log4Shell CVE-2021-44228, PowerShell malveillant, Groupe HAFNIUM
- **Tactiques MITRE ATT&CK**
  Exfiltration
- **Techniques MITRE ATT&CK**
  Exfiltration automatisée
- **Phase de la kill-chain**
  Exploitation
- **Fonctionnement**
  Cette détection de menace identifie les commandes PowerShell qui utilisent le paramètre WindowStyle pour masquer la fenêtre sur le terminal compromis. Cette combinaison d'options de ligne de commande est suspecte, car elle remplace la stratégie d'exécution PowerShell par défaut, tente de masquer son activité à l'utilisateur et se connecte à Internet.

Impact (TA0040)

Tactique de menace : manipuler, interrompre ou détruire vos systèmes et vos données

Pourquoi ces menaces existent-elles ?

Lors de cette phase, l'adversaire essaie activement de manipuler, d'interrompre ou de détruire les systèmes et les données ciblés. La phase d'impact comprend des techniques visant à perturber la disponibilité ou compromettre l'intégrité en manipulant les processus commerciaux et opérationnels. Les techniques utilisées pour l'impact comprennent la destruction ou la falsification des données. Dans certains cas, les processus métier peuvent sembler intacts et fonctionner correctement en surface. Mais en réalité, ils peuvent avoir été secrètement modifiés pour consulter, voler ou compromettre des données, mener des opérations de cyberespionnage, et faire des ravages sur les systèmes ciblés.

Comment ces menaces sont-elles exécutées ?

La phase d'impact consiste en un large éventail de techniques visant à perturber, compromettre, détruire et manipuler l'intégrité et la disponibilité des opérations, des processus, des systèmes, des appareils et des données du réseau, ainsi que leur environnement. Ces techniques sont particulièrement dangereuses car elles peuvent perturber instantanément les processus et entraîner des dommages à plus long terme pour l'environnement ou les systèmes.

Les pirates peuvent, par exemple, interrompre les ressources système et réseau en bloquant, supprimant ou verrouillant l'accès aux comptes, ou en manipulant les identifiants pour obtenir un accès non autorisé et interdire l'accès des utilisateurs légitimes.

Les adversaires peuvent également chercher à détruire des données et des fichiers – sur des systèmes spécifiques ou en masse – dans le but de perturber les systèmes, les services et les ressources réseau, d'écraser des fichiers sur des disques locaux et distants et de rendre les données stockées irrécupérables. Les manipulations de données consistent notamment à insérer, supprimer ou modifier des informations pour influencer des résultats externes, masquer une activité ou influer sur un processus métier ou une décision.

Les malfaiteurs peuvent également chercher à altérer des contenus internes et externes et des ressources web, avec diverses conséquences pour la cible : perte de revenus, de crédibilité commerciale et dégradation de la réputation. Les attaques par déni de service sont particulièrement prisées pour dégrader ou interrompre complètement la disponibilité des sites web, des services de messagerie, des DNS et des applications web en étouffant le système avec du trafic.

Détecter et répondre avec Splunk

Détection de menace Splunk :
Création en masse de notes de ransomware

- **Scénario analytique Splunk**
  Ransomware Clop, Ransomware DarkSide, Ransomware BlackMatter
- **Tactiques MITRE ATT&CK**
  Impact
- **Techniques MITRE ATT&CK**
  Chiffrement des données à des fins d'impact
- **Phase de la kill-chain**
  Exploitation
- **Fonctionnement**
  Cette détection de menace repère la présence d'un grand nombre de notes de rançon sur la machine infectée. Ce comportement offre une bonne indication quand le nom de fichier de la note de rançon n'est pas connu du secteur de la sécurité ou ne figure pas dans votre table de recherche de ransomware.

Vous voulez donner un coup d'accélérateur à vos opérations de sécurité ?

Découvrez Splunk Security Essentials, et commencez à résoudre gratuitement des centaines de problèmes de sécurité différents.

En savoir plus

splunk>

22-26440-Splunk-Cybersecurity Threat Detections with Splunk _ Mitre ATT_CK_SS-107