ARTICLE DE RECHERCHE SUR LES MENACES

Attaques par réutilisation des identifiants dans les environnements connectés au cloud

splunk> turn data into doing™

L'équipe de recherche Splunk a mis au point un nouveau scénario analytique abordant la récente campagne SolarWinds, au cours de laquelle des TTP (Golden SAML) ont ciblé l'extraction d'identifiants dans des environnements cloud fédérés. Des technologies de fédération comme Active Directory Federation Services (ADFS) structurent ces environnements. Ces fédérations peuvent se trouver à l'intérieur du périmètre ou entre différents fournisseurs de cloud.

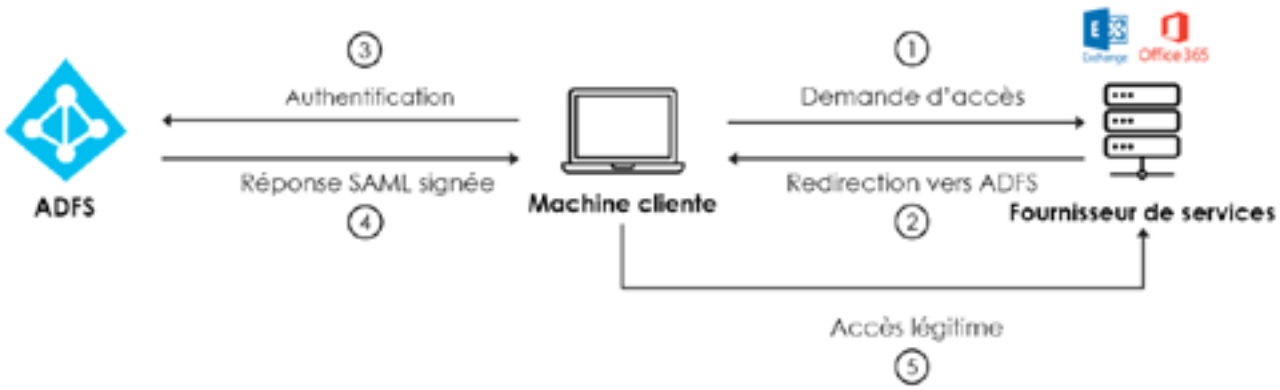
Une récente alerte de l'Agence de la cybersécurité et de la sécurité des infrastructures signale de nouveaux vecteurs d'attaque qui exploitent la réutilisation d'identifiants pour viser les infrastructures connectées au cloud. Avec la généralisation des technologies cloud, de nombreuses entreprises administrent désormais des environnements où la frontière entre le périmètre et Internet est floue. Ces environnements permettent aux applications et aux utilisateurs locaux d'interagir avec les services cloud. Ces interactions se font généralement via les points de terminaison API REST et doivent être simples, rapides et efficaces afin de fournir une bonne expérience utilisateur et d'utiliser efficacement la puissance de traitement. L'interaction constante de ces services nécessite des normes d'authentification, d'autorisation et de validation de la confiance entre les utilisateurs, les applications à l'intérieur du périmètre et les services cloud connectés. Deux protocoles populaires permettent d'atteindre cet objectif : OAuth2 et le langage de balisage des assertions de sécurité (SAML). Ces protocoles partagent le même but : autoriser les utilisateurs ou les applications à accéder à plusieurs environnements de manière transparente. Cette pratique devient indispensable lorsque les entreprises utilisent des fournisseurs et des applications multicloud dans le cadre de leurs infrastructures.

Dans cet article, nous examinons le fonctionnement de ces identifiants et de ces attaques au sein du périmètre et entre les environnements cloud.

Les jetons OAuth2 sont utilisés pour effectuer des appels autorisés aux API de la part d'un utilisateur ou d'une application. Ils sont généralement stockés dans les variables de session de l'application du point de terminaison, et peuvent être extraits et réutilisés dans de nombreux cas sans revalidation auprès de la plateforme émettrice, offrant aux attaquants un moyen de les réutiliser pour accéder aux sessions et aux ressources de la victime.

SAML est une norme ouverte pour l'échange de données d'authentification et d'autorisation entre les parties. SAML permet notamment d'effectuer une authentification unique (SSO) via le navigateur sur plusieurs plateformes. Le protocole SAML utilise des assertions de sécurité pour accorder l'accès et déterminer le niveau d'accès. L'assertion de sécurité est obtenue via l'interaction d'un principal (l'utilisateur), d'un fournisseur d'identité (le système qui émet l'assertion) et d'un fournisseur de services (le système qui accepte l'assertion). Ces assertions de sécurité contiennent des certificats et des clés. Ces certificats et clés permettent de vérifier l'identité et d'accorder ensuite des autorisations.

Un moyen efficace d'obtenir une connectivité transparente avec les services cloud consiste à mettre en œuvre des technologies de fédération. Les technologies de fédération utilisent les protocoles que nous venons d'évoquer en conjonction avec des services d'annuaire de gestion d'accès aux identités basés à l'intérieur ou à l'extérieur du périmètre, afin de permettre l'accès entre environnements. Voici un exemple de flux d'authentification/autorisation ADFS (Active Directory Federation Service).



Source : Sygnia Advisory – Détection des attaques Golden SAML

Le graphique précédent pourrait également s'appliquer à d'autres fournisseurs de services cloud qu'Azure, car ADFS permet la fédération avec AWS.

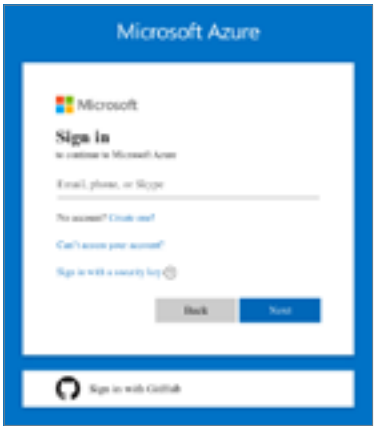
Les attaques récentes, comme la campagne SolarWinds, indiquent que les attaquants ciblent les assertions de sécurité SAML et les jetons OAuth2, en particulier lorsque les victimes ont des environnements connectés au cloud.

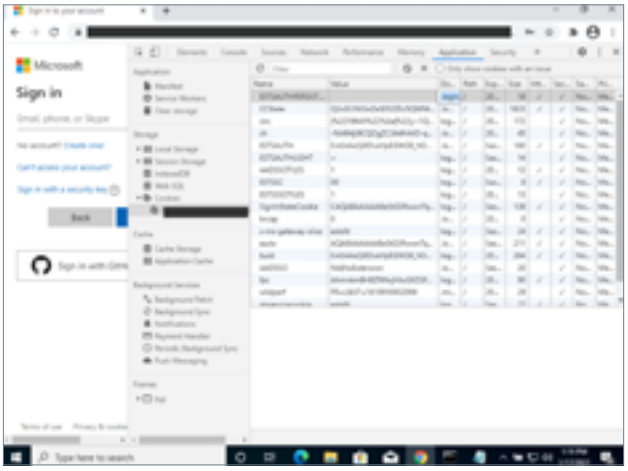
Processus d'attaque

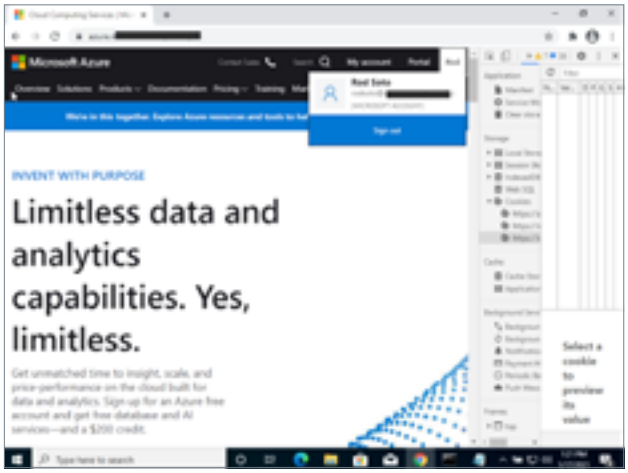
D'après une récente alerte CISA, une attaque qui cible les identifiants d'un périmètre lié au cloud ou connecté cherche essentiellement à obtenir un ou plusieurs de ces trois éléments :

1. **Jeton OAuth2**

   L'équipe de recherche sur les menaces de Splunk s'est déjà penchée sur le piratage et la réutilisation des jetons GCP OAuth. Un autre type de réutilisation de jetons OAuth2 peut être exécuté dans un environnement Azure via pass-the-cookie. Cette attaque contourne également l'authentification multifacteurs. Les schémas suivants montrent un exemple d'attaque par pass-the-cookie faisant suite au vol du cookie via l'outil Mimikatz.







2. **Assertion SAML**

   Comme indiqué ci-dessus, si un attaquant est en mesure d'obtenir une assertion SAML valide, il peut usurper l'identité de la victime et accéder à son environnement cloud. Cette attaque a une très faible probabilité de succès, car certains fournisseurs comme AWS font expirer les assertions, ainsi que d'autres vérifications de signature SAML, au bout de cinq minutes. Ce type d'attaque nécessiterait des étapes supplémentaires pour maintenir la validité de l'assertion : l'attaquant devrait, par exemple, changer la date d'expiration ou modifier certains des attributs (adresse e-mail, nom, etc.). Des mesures strictes de vérification des assertions empêchent ces types d'attaques.

   Une assertion SAML peut être extraite en ouvrant les outils de développeur dans la plupart des navigateurs.

3. **Service de certificat, de clé et d'annuaire**

   L'obtention de certificats à partir d'un service de fédération est l'attaque la plus difficile à exécuter, mais c'est aussi celle qui donne à l'adversaire le plus de pouvoir pour réutiliser ou falsifier des assertions signées SAML. Cette technique peut en effet lui permettre d'accéder à des environnements fédérés dans le cloud ou même de mettre en place des portes dérobées en créant de nouvelles entités fédérées via d'autres fournisseurs de cloud. Le pirate peut alors utiliser des outils de post-exploitation tels qu'ADFSDump, Mimikatz ou même des outils de système d'exploitation comme Certutil.exe afin d'accéder aux certificats ou aux clés, puis les utiliser pour forger des jetons ou des assertions à l'aide d'outils comme ADFSpoof ou Shimit. Il a besoin des identifiants d'une victime ayant accès à la fédération cloud et disposant d'un flux d'authentification allant de l'intérieur du périmètre au cloud.

Il faut aussi se rappeler que, sans avoir une fédération formelle avec le cloud, de nombreux environnements situés à l'intérieur du périmètre disposent toujours d'un accès quotidien et persistant à des environnements cloud. C'est notamment le cas des environnements DevOps, pour lesquels certaines de ces attaques sont toujours valides.

Défis et opportunités de détection

Ces attaques concernent les environnements où il existe des interactions importantes entre les services intra-périmètre et cloud, et où une fédération formelle a été établie via des technologies telles que Windows Active Directory Federation Services.

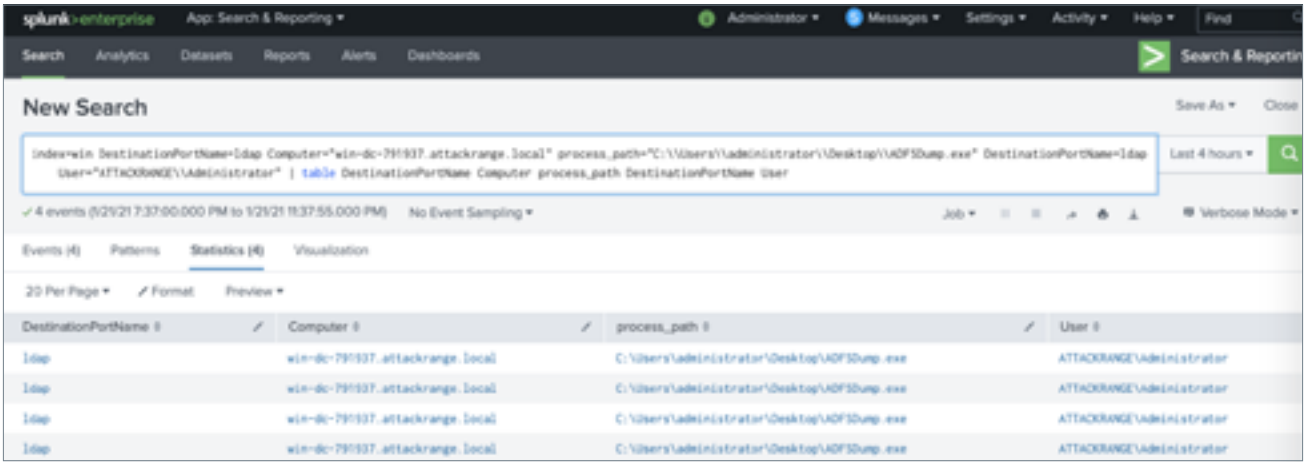
Il faut aussi tenir compte des fédérations informelles. Ce sont les environnements dans lesquels, même sans technologie de fédération formelle comme ADFS, il subsiste de nombreux environnements dans lesquels un développeur peut se trouver à la fois à l'intérieur du périmètre et connecté à un stockage ou à des instances de calcul cloud. Ce flux d'authentifications est lié par ses identifiants résidant au même point de terminaison ; les données circulent entre le cloud et l'environnement de développement local via ce point de terminaison. Il s'agit techniquement d'une fédération informelle, et un adversaire capable de compromettre le point de terminaison peut ensuite réutiliser les identifiants pour se déplacer du nord au sud ou d'est en ouest.

Ces scénarios de fédération prêtent le flanc aux vecteurs d'exploitation de la réutilisation des identifiants qui ciblent les services cloud.

Ces attaques peuvent être prises en charge à partir de deux environnements différents :

- à l'intérieur du périmètre. C'est là que se trouvent les objets clés pour ces types d'attaques. Ici, nous examinons la surface d'attaque des services qui fournissent des services d'annuaire d'identités et des services de fédération ;
- le cloud. L'infrastructure du fournisseur de cloud est la cible d'un mouvement sud-nord, car l'adversaire commence par accéder aux identifiants d'un appareil situé dans le périmètre, puis se déplace vers l'environnement cloud.

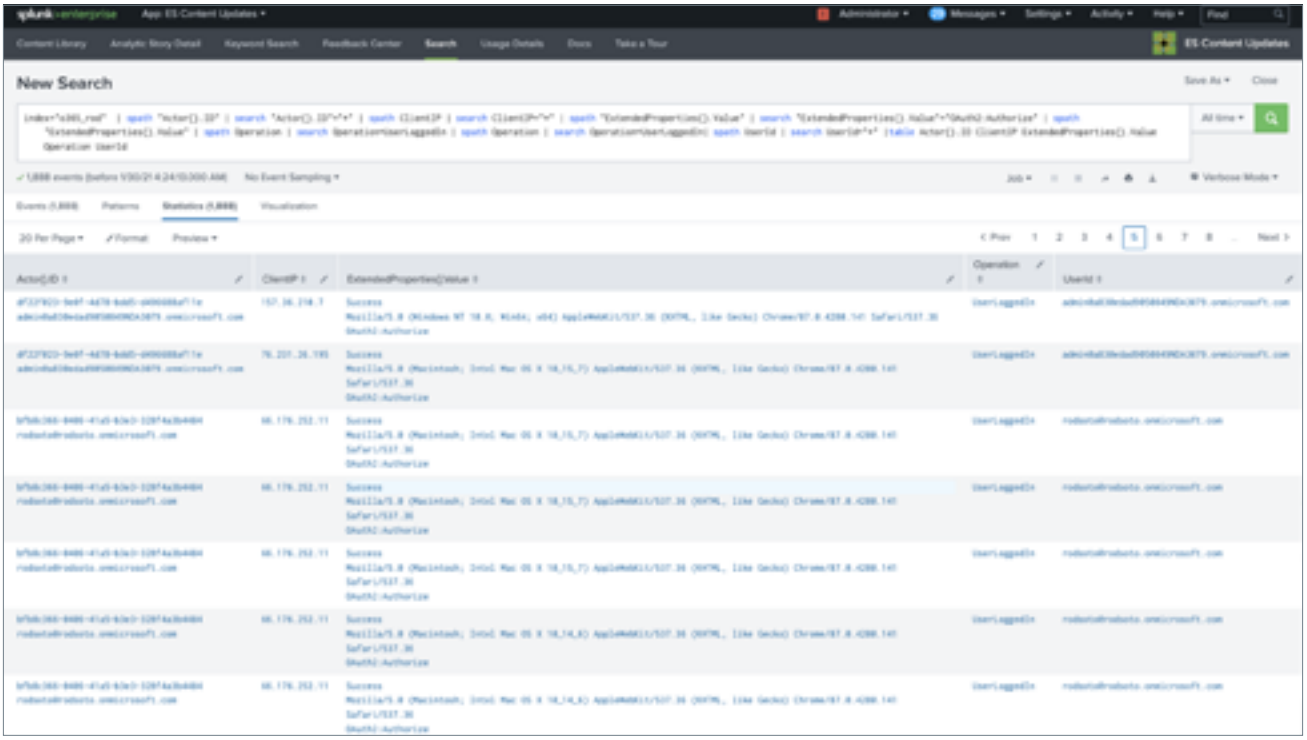
Les attaques par réutilisation des identifiants sont particulièrement difficiles à détecter car certains outils employés pour extraire les identifiants des postes de travail ou des serveurs ne sont pas détectables. Lorsque l'on examine le trafic cloud généré par leur utilisation, il ressemble exactement à tout autre accès provenant de sessions normales. Prenons l'exemple d'ADFSDump, outil de post-exploitation au niveau du serveur de bureau. Cet outil récupère les informations des services ADFS ; cette étape préalable permet à l'adversaire d'identifier les éléments nécessaires afin de falsifier des requêtes.



Comme le montre le schéma ci-dessus, nous avons exécuté l'outil sur une seule instance d'un serveur ADFS créé à l'aide de Splunk Attack Range. Il est fort probable que les antivirus ne détectent pas cet outil. C'est en partie parce qu'il n'a pas de signature cohérente, dans la mesure où il peut être compilé à l'aide de différentes variables.

Dans ce cas précis, nous avons compilé ADFSDump, puis nous l'avons exécuté sur un seul serveur ADFS Windows Server 2016 à l'aide de WID. Nous avons observé qu'au lieu de se connecter au port SQL, il utilisait LDAP. Ce cas particulier diffère des indicateurs attendus actuels qui suggèrent d'examiner un pipe SQL. Cette fois, cet indicateur ne permettra pas de détecter quoi que ce soit.

Du point de vue du cloud, nous avons exécuté l'attaque pass-the-cookie comme indiqué ci-dessus, nous l'avons enregistrée, puis nous avons élaboré une recherche pour tenter la détection. Ce que nous avons découvert, c'est que l'empreinte d'accès est exactement la même que celle des ouvertures de session normales.



Comme les jetons de fédération sont censés fournir un accès transparent aux environnements cloud, ils ne sont pas considérés comme des vulnérabilités. Cependant, sur la base des TTP de ces attaques, nous avons développé un scénario analytique qui couvre les deux éléments ci-dessus (cloud et périmètre) où les attaquants accèdent aux identifiants, puis les transmettent aux environnements cloud. Nous avons spécifiquement étudié des scénarios tels que le Golden SAML et d'autres scénarios d'abus d'identifiants à l'aide de jetons OAuth au niveau du cloud. Au niveau du périmètre, nous nous sommes concentrés sur l'escalade des privilèges Windows (nécessaire dans la plupart des cas pour accéder aux identifiants) et l'utilisation d'outils tels que Mimikatz et ADFSDump.

Recherches de détection axées sur le périmètre

Nom	Identifiant technique	Tactique	Remarque
Extraction du certificat par Certutil.exe	T1552.004	Accès aux identifiants	Nouvelle détection
Processus inhabituels sur un terminal	T1204.002	Exécution	Permet de détecter ADFSDump
Utilisation de clés de registre pour l'élévation des privilèges	T1546.012	Élévation de privilèges, persistance	
Détection de Mimikatz à l'aide d'images chargées	T1003.001	Accès aux identifiants	
Détection de Mimikatz via PowerShell et le code d'événement 4703	T1003.001	Accès aux identifiants	

Nouvelles recherches de chasse et de détection axées sur le cloud

Nom	Identifiant technique	Tactique	Fournisseur
AWS – Accès SAML par un utilisateur et principal du fournisseur	T1078	Contournement de défense, persistance, élévation des privilèges, accès initial	AWS
AWS – Mise à jour du fournisseur d'identité SAML	T1078	Contournement de défense, persistance, élévation des privilèges, accès initial	AWS
O365 Excès d'erreurs de connexion SSO	T1556	Accès aux identifiants, contournement de la défense	Azure
O365 Ajout d'un principal de service	T1136.003	Persistance	Azure
O365 Ajout d'un principal de service	T1136.003	Persistance	Azure
O365 Ajout d'un nouveau domaine fédéré	T1136.003	Persistance	Azure

Des attaques comme le Golden SAML sont difficiles à détecter. Cependant, en corrélant les événements du fournisseur de cloud et du périmètre, les analystes sont en mesure d'obtenir des informations utiles à la détection. Sans corrélation, les connexions au cloud ressemblent à n'importe quelle autre, et les événements d'attaque de point de terminaison ne révèlent d'eux-mêmes aucune utilisation abusive de la fédération.

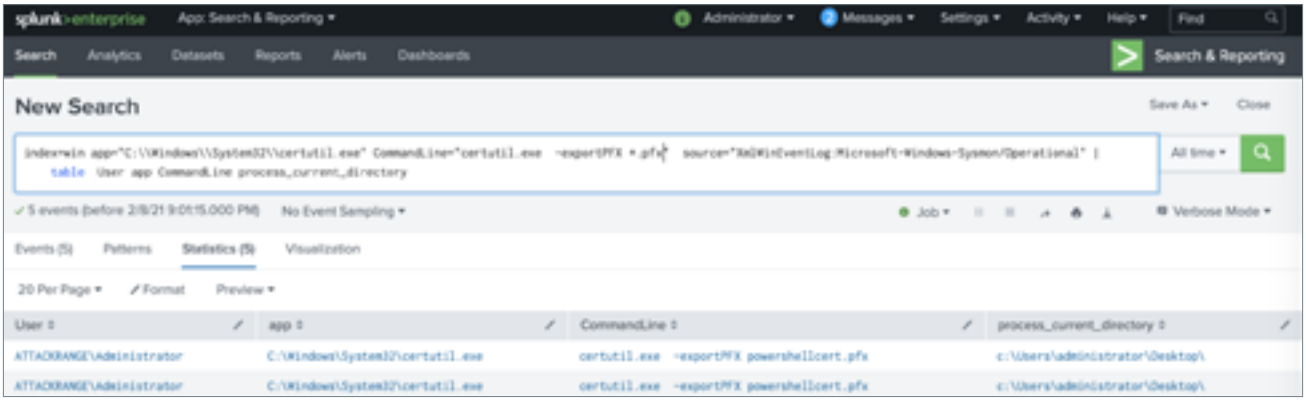
Voici quelques aperçus de notre prochain scénario analytique **Abus d'identifiants fédérés dans le cloud** dans la version v3.15.0. Ces recherches ciblent l'exploitation des jetons OAuth2 et des assertions SAML. Ces recherches doivent être menées dans le cadre d'une investigation. Exécutées de façon isolée, elles ne peuvent pas fournir une image complète d'un éventuel abus de fédération, compte tenu de la difficulté de détecter ces attaques en raison du flux d'authentification anormal.

Axé sur les points de terminaison

Extraction du certificat par Certutil.exe

Cette recherche détecte l'envoi d'arguments à certutil.exe, pouvant indiquer une manipulation ou une extraction de certificat. Les adversaires peuvent ensuite utiliser ce certificat pour signer de nouveaux jetons d'authentification, en particulier dans des environnements fédérés tels que Windows ADFS.

```
index=win app="C:\\Windows\\System32\\certutil.exe" CommandLine="certutil.exe  -exportPFX *.pfx"
source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" | table  User app CommandLine
process_current_directory
```

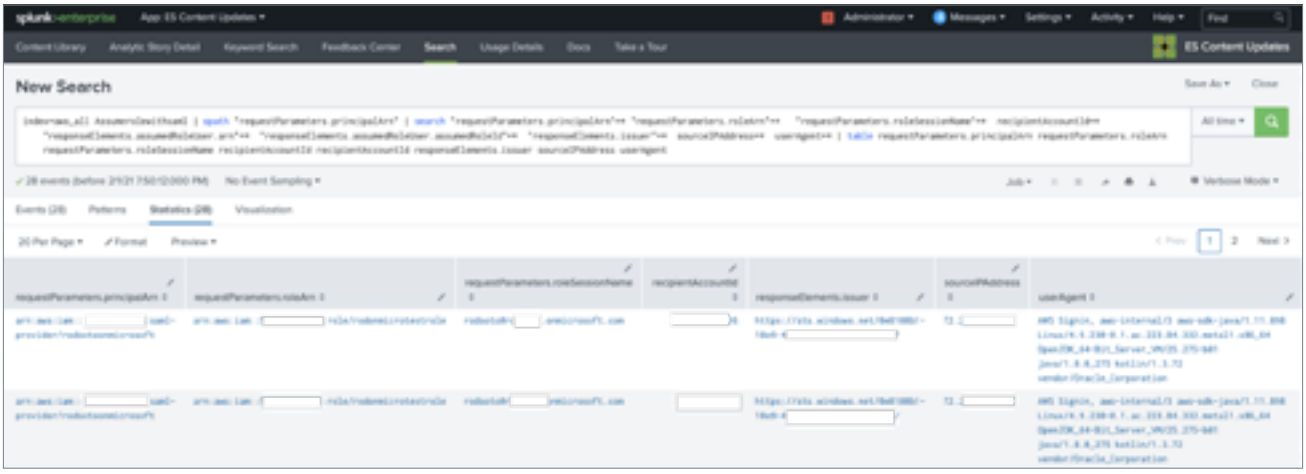


Axé sur le cloud

AWS

AWS – Accès SAML par un utilisateur et principal du fournisseur

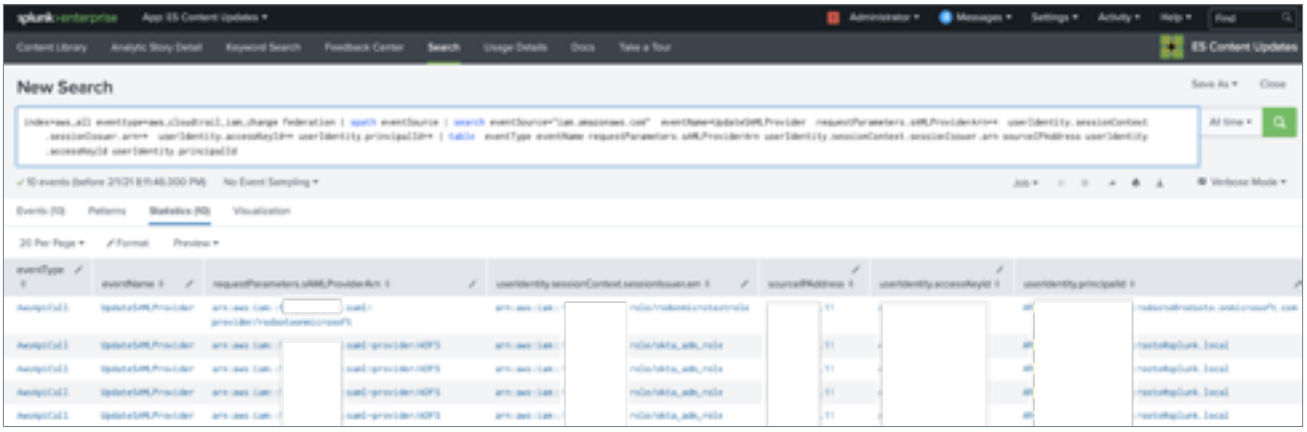
Cette recherche met au jour les accès SAML provenant de fournisseurs de services spécifiques, d'utilisateurs et de principaux ciblés chez AWS. Elle fournit également certaines informations permettant de détecter un accès anormal ou un cas de détournement ou de falsification d'identifiants, en particulier dans les environnements fédérés utilisant le protocole SAML à l'intérieur du périmètre ou du fournisseur de cloud.



Remarque : cette recherche en elle-même ne détectera aucune attaque liée à SAML. Cependant, en présence d'autres indicateurs contextuels, cette recherche fournira les indices nécessaires pour investiguer et identifier les éléments d'attaque : attributs dans l'assertion SAML, principaux, identité, fournisseurs de services et, bien sûr, utilisateur par requête et authentification accordée par l'assertion SAML. C'est une requête de chasse.

Mise à jour AWS : activité du fournisseur SAML

Cette recherche permet de détecter les mises à jour des fournisseurs SAML dans AWS. Les équipes doivent superviser de près les mises à jour des fournisseurs SAML, car elles peuvent indiquer une possible compromission du périmètre des identifiants fédérés ou l'accès par une porte dérobée à partir d'un autre fournisseur cloud créé par l'attaquant.

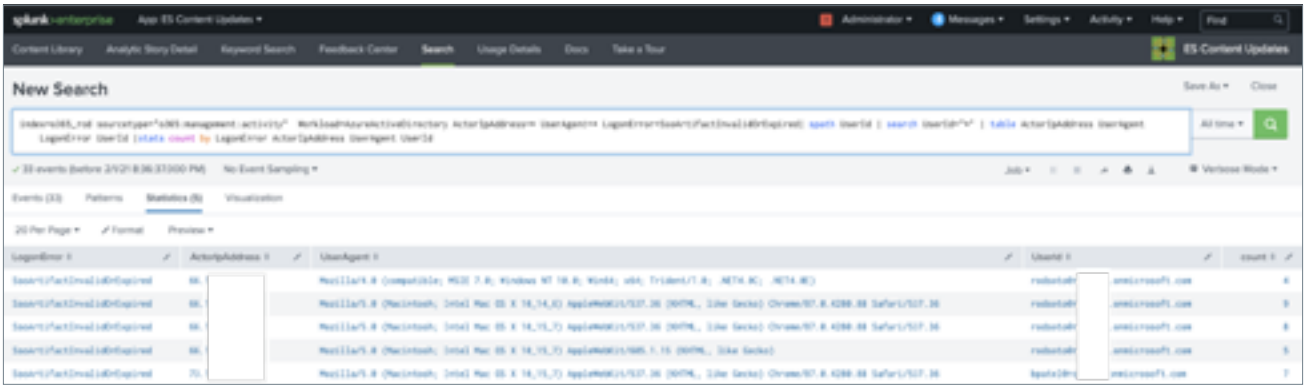


Remarque : cette recherche inclut la création de fournisseurs SAML, l'ajout de rôles et la présence de modifications dans le document PDI. Elle affiche également les utilisateurs du domaine fédéré.

Azure

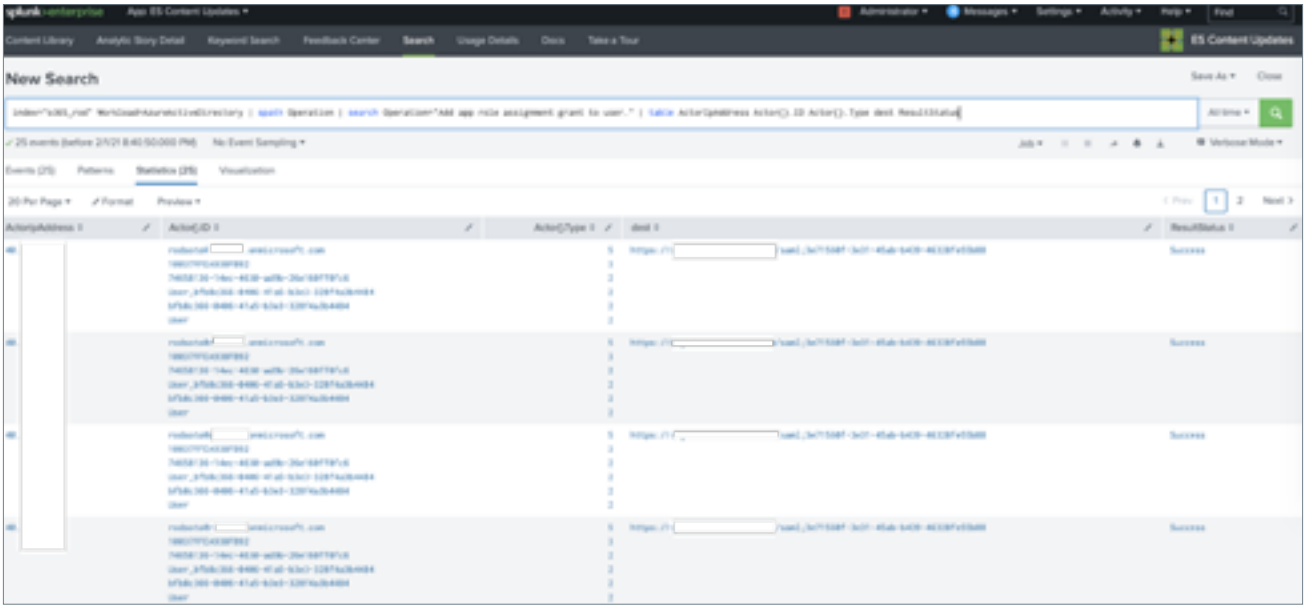
Excès d'erreurs de connexion SSO

Cette recherche détecte les comptes avec un nombre élevé d'erreurs de connexion SSO (Single Sign-On). Un nombre excessif d'erreurs de connexion peut indiquer des tentatives d'attaque par force brute, ou par réutilisation ou détournement de jeton SSO.



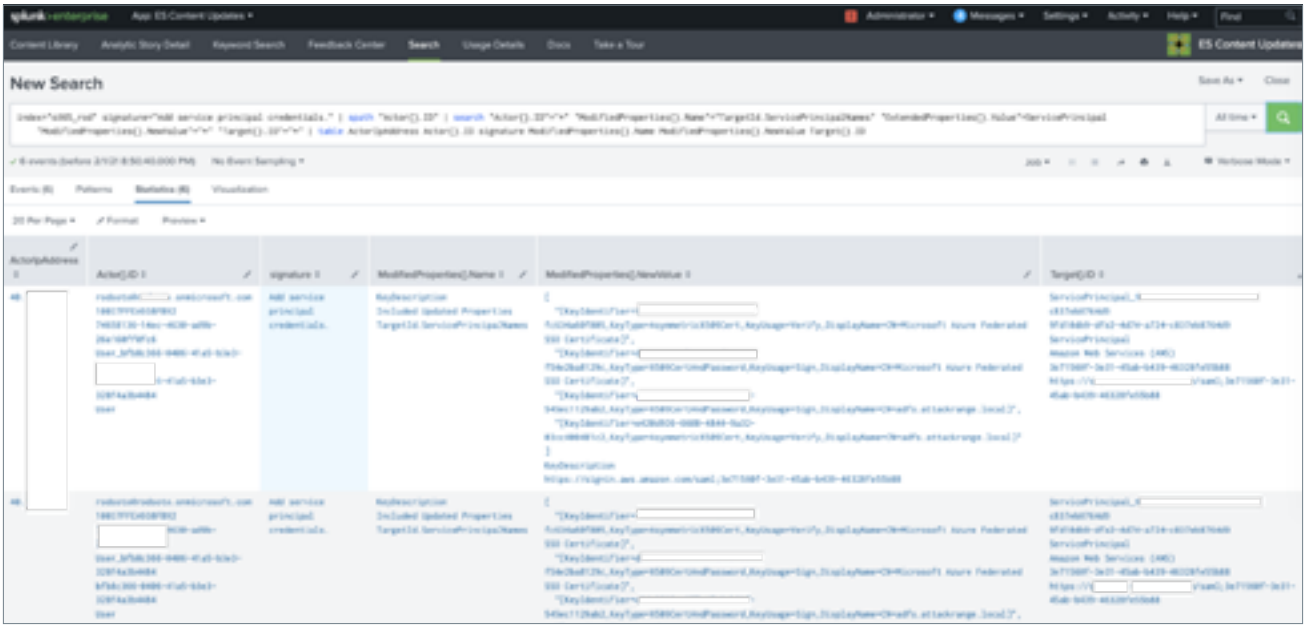
Ajout d'attribution de rôle d'application à l'utilisateur

Cette recherche détecte la création d'un nouveau paramètre de fédération en avertissant d'un événement spécifique lié à sa création. Dans ce cas, l'Attribution de rôle d'application est accordée à un utilisateur, ce qui est une étape nécessaire dans Azure pour créer une nouvelle fédération.



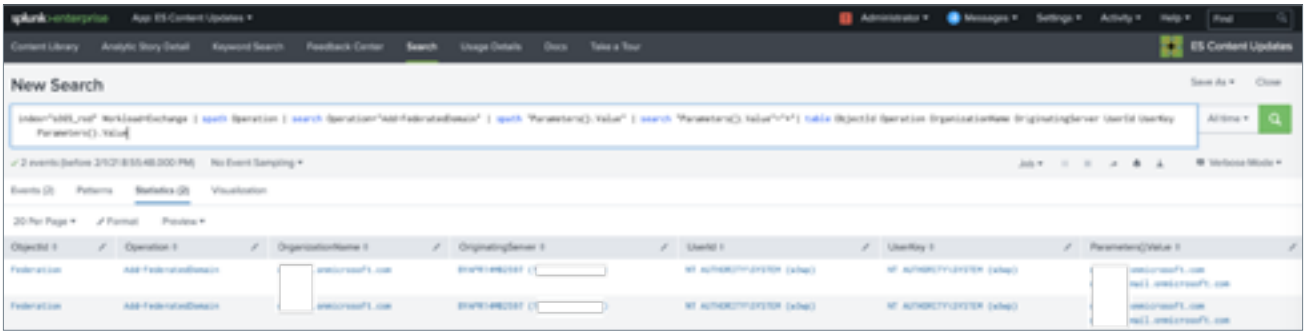
Ajout d'un principal de service

Cette recherche détecte la création d'un nouveau paramètre de fédération en avertissant d'un événement spécifique lié à sa création ; ici, il s'agit de l'ajout d'un principal de service.



Ajout d'un nouveau domaine fédéré

Cette recherche détecte l'ajout d'un nouveau domaine fédéré.



Certains de ces vecteurs d'attaque sont nouveaux et évolutifs, et ils semblent imiter les anciennes techniques de mouvement latéral telles que pass the hash ou pass the ticket. De nombreux fournisseurs ne considèrent pas ces vecteurs d'attaque comme des vulnérabilités mais plutôt comme un abus de fonctionnalité. Ces types d'attaques sont destinés à gagner en popularité avec l'implémentation de services cloud toujours plus nombreux par les entreprises.

Toutes les recherches ci-dessus sont disponibles gratuitement dès aujourd'hui dans le scénario analytique Abus d'identifiants fédérés dans le cloud via Splunk Security Content et Splunk Security Essentials.

À propos de l'équipe de recherche sur les menaces de Splunk

L'équipe de recherche sur les menaces de Splunk se consacre à comprendre le comportement des acteurs et à étudier les menaces connues afin de créer des détections pour le bénéfice de toute la communauté Splunk. Pour cela, l'équipe de recherche sur les menaces de Splunk crée et propose en open source des outils qui analysent les menaces et les acteurs, comme Splunk Attack Range ; elle utilise ensuite ces outils pour créer des ensembles de données d'attaque. À partir de ces ensembles de données, de nouvelles détections sont élaborées et partagées avec la communauté Splunk dans Splunk Security Content. Différents produits Splunk, dont Enterprise Security, Splunk Security Essentials et Mission Control, utilisent ensuite ces détections pour aider les clients à repérer rapidement et efficacement les menaces connues.

Vous voulez utiliser ces détections prédéfinies pour mettre votre centre des opérations de sécurité sur la bonne voie ? Téléchargez l'application Enterprise Security Content Updates sur Splunkbase !

21-17703-SPLK-CredentialReuseAttacksinCloud-ConnectedEnvironments-A4-103-WP