Extraire des fichiers à partir de paquets via l'API REST

Publié: 2024-09-26

Ce guide fournit des instructions pour extraire des fichiers (également appelée sculpture de fichiers) via l'explorateur d'API ExtraHop REST et via un script Python.

Avant de commencer

- Pour les capteurs et les machines virtuelles ECA, vous devez disposer d'une clé API valide pour apporter des modifications via l' API REST et suivre les procédures ci-dessous. (Voir Générer une clé API).
- Pour RevealX 360, vous devez disposer d'informations d'identification d'API REST valides pour apporter des modifications via l' API REST et suivre les procédures ci-dessous. (Voir Création d'informations d'identification pour l'API REST).

Extraire des fichiers via l'explorateur d'API REST

1. Dans un navigateur, accédez à l'explorateur d'API REST.

   L'URL est le nom d'hôte ou l'adresse IP de votre sonde ou console, suivi par `/api/v1/explore/`. Par exemple, si votre nom d'hôte est seattle-eda, l'URL est `https://seattle-eda/api/v1/explore/`.
2. Entrez les informations d'identification de votre API REST.
   - Pour les capteurs et les machines virtuelles ECA, cliquez **Entrez la clé API** puis collez ou saisissez votre clé API dans le **Clé API** champ.
   - Pour RevealX 360, cliquez sur **Entrez les identifiants de l'API** puis collez ou saisissez l'ID et le code secret de vos informations diciatives d'API dans le **IDENTIFIANT** et **Secret** champs.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **Recherche de paquets** puis cliquez sur **POST /paquets/search**.
5. Cliquez **Essayez-le**.

   Le schéma JSON est automatiquement ajouté au **corps** zone de texte.
6. Dans le **corps** zone de texte, spécifiez les paramètres de recherche pour les paquets dont vous souhaitez extraire des fichiers.

   Par exemple, les paramètres suivants extraient des fichiers à partir de paquets envoyés vers ou depuis l'adresse IP 10.10.10.10 au cours des 30 dernières minutes :

   ```
   {
       "from": "-30m",
       "output": "extract",
       "ip1": "10.10.10.10"
   }
   ```
7. Cliquez **Envoyer la demande**.

   Lorsque la demande est terminée, Réponse du serveur section apparaît. Si la demande aboutit, un code dquo 200 s'affiche.
8. À côté du code dveloppement 200, cliquez sur **Télécharger le fichier**.

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub ExtraHop contient un exemple de script Python qui extrait des fichiers à partir de paquets via l'API REST.

© 2024ExtraHop Networks, Inc. Tous droits réservés.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `extract_files/extract_files.py` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez le `extract_files.py` archivez et remplacez les variables de configuration par des informations provenant de votre environnement.
   a) Pour les capteurs et les machines virtuelles ECA, spécifiez les variables de configuration suivantes :
      - **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la console.
      - **CLÉ_API:** La clé API.

   b) Pour Reveal (x) 360, spécifiez les variables de configuration suivantes :
      - **HÔTE:** Le nom d'hôte de l'API Reveal (x) 360. Ce nom d'hôte est affiché sur la page d'accès à l'API Reveal (x) 360 sous API Endpoint. Le nom d'hôte n'inclut pas le /oauth2/token.
      - **IDENTIFIANT:** L'ID des informations d'identification de l'API REST Reveal (x) 360.
      - **SECRET:** Le secret des informations d'identification de l'API REST Reveal (x) 360.

   c) Pour tous les systèmes, spécifiez **RECHERCHE** variable de configuration pour les paquets dont vous souhaitez extraire des fichiers.
3. Exécutez la commande suivante :

```
python3 extract_files.py
```

Si le système fonctionne correctement, les fichiers sont enregistrés dans un `.zip` fichier nommé `extracted_files.zip`.

Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat TLS a échoué, assurez-vous que un certificat fiable a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter `verify=False` option permettant de contourner la vérification des certificats. Cependant, cette méthode n'est pas sûre et n'est pas recommandée. Le code suivant envoie une requête HTTP GET sans vérification du certificat :

```
requests.get(url, headers=headers, verify=False)
```