Détection des binaires suspects

Wazuh dispose de capacités de détection des anomalies et des logiciels malveillants, permettant d'identifier les binaires suspects sur un point de terminaison. Les binaires, qui sont des exécutables conçus pour automatiser des tâches, sont souvent exploités par les acteurs malveillants pour mener des opérations d'exploitation de manière discrète afin d'éviter toute détection.

Dans cet exemple d'utilisation, on illustre comment le module **Wazuh rootcheck** peut repérer un binaire système vérolé sur un point de terminaison **Linux**. Cela est réalisé en altérant le contenu d'un binaire légitime avec un code malveillant, incitant ainsi le point final à l'exécuter en tant que binaire légitime.

I – Configuration du point de terminaison Linux

1. Activation du module **Wazuh rootcheck** :
   - On vérifie le fichier de configuration de l'agent **Wazuh** situé dans **/var/ossec/etc/ossec.conf** et on s'assure que la section **<rootcheck>** aux configurations suivantes :

```
<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>
  <frequency>43200</frequency>
  <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
  <skip_nfs>yes</skip_nfs>
</rootcheck>
```

2. Si la configuration a dû être ajustée, on enregistre les modifications et on redémarre l'agent :

```
systemctl restart wazuh-agent
```

II – Émulation de l'attaque

1. On crée une copie du binaire système d'origine :

```
sudo cp -p /usr/bin/w /usr/bin/w.copy
```

2. On remplace le binaire système d'origine **/usr/bin/w** par le script shell suivant :

```
sudo tee /usr/bin/w << EOF
#!/bin/bash
echo "`date` this is evil" > /tmp/trojan_created_file
echo 'test for /usr/bin/w trojaned file' >> /tmp/trojan_created_file
Now running original binary
/usr/bin/w.copy
EOF
```

3. On force l'exécution de l'analyse rootcheck en redémarrant l'agent Wazuh :

```
sudo systemctl restart wazuh-agent
```

Visualisation des alertes :

Détection des binaires suspects

- On accède au tableau de bord **Wazuh** puis on se rend dans le module « **Security Events** » et dans « **Events** ».
- On peut ajouter les filtres suivants dans la barre de recherche pour interroger les alertes :

```
location:rootcheck AND rule.id:510 AND data.title:Trojaned version of file detected
```

Résultat de l'alerte – Cheval de Troie