Dépannage d'AMP dans Secure Web Appliance

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Dépannage des journaux SWA AMP

Options Champ détaillé et Valeur

Autres informations utiles

Introduction

Ce document décrit la section ampverdict dans le niveau de journal INFO et DEBUG du moteur Advanced Malware Protection du dispositif Web sécurisé.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- AMP est activé
- Accès SSH à SWA
- SWA installé et sous licence
- Réputation des fichiers et analyse des fichiers activées

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

SWA offre une intégration avec AMP pour les terminaux et un moteur AMP local. AMP assure une protection contre les programmes malveillants de type « zero-day » grâce aux fonctionnalités File Reputation et File Analysis. Le SWA inclut un moteur de préclassification qui est responsable des analyses de fichiers en interne avant les vérifications du cloud public. Les journaux décrits dans la section suivante concernent le moteur AMP sur SWA, et non le cloud AMP ou Threat Grid.

Dépannage des journaux SWA AMP

Accédez aux journaux AMP. Connectez-vous via l'interface de ligne de commande et queue ou grep les journaux amp :

1. Connectez-vous à l'interface de ligne de commande via le client SSH.

2. Exécutez la commande grep, puis appuyez sur Entrée.

3. Entrez le numéro de amp_logs comme indiqué.

4. Répondez aux invites. Si vous exécutez du trafic en direct, choisissez l'option pour suivre les journaux.
5. Appuyez sur la touche Entrée.

6. Les journaux sont affichés.

Les journaux SWA AMP sont disponibles à différents niveaux de détail. Vous pouvez sélectionner le niveau INFO ou DEBUG. Les résultats présentent de légères différences, qui sont expliquées dans la section suivante

---

Remarque : La licence AMP doit être installée sur SWA pour sélectionner les journaux AMP.

Journaux de niveau INFO AMP :

```
Wed Apr 27 12:21:26 2022 Info: Txn 18210 Binary scan on instance[0] Id[1345]: AMP allocated memory = 0,
Wed Apr 27 12:21:35 2022 Info: Binary scan on instance[0] id[1345]: filename[npp.8.4.Installer.x64.exe]
Wed Apr 27 12:22:28 2022 Info: File uploaded for analysis. Server: https://panacea.threatgrid.com, SHA2
```

Journaux de niveau INFO AMP (ampverdict) :

```
ampverdict[(1, 1, 'amp', '', 0, 0, True)]
(analysis_Action, scan_verdict, ‘verdict_source', ‘spyname’, malware_verdict, file_reputation, upload_a
```

Journaux de niveau AMP DEBUG :

```
Fri Apr 29 01:38:40 2022 Debug: Binary scan: proxid[3951] filename[favicon.ico] len[41566b] readtime[10
```

Journaux de niveau DEBUG AMP (ampverdict) :

```
ampverdict[(1, 1, 'amp', '', 0, 0, False)]
ampverdict[(analysis_action, scan_verdict,disposition, ‘spyname: policy name if amp registered with con
```

Options Champ détaillé et Valeur

Champ	Valeur
Action_Analyse	"0" : Indique que l'Advanced Malware Protection n'a pas demandé le téléchargement du fichier pour analyse. "1" : Indique que la protection avancée contre les programmes malveillants a demandé le téléchargement du fichier pour analyse.
Verdict_numérisation	"0" : Le fichier n'est pas malveillant. "1" : Le fichier n'a pas été analysé en raison de son type. "2" : Expiration de l'analyse du fichier. "3" : Erreur d'analyse. Supérieur à 3 : Le fichier est malveillant.
Verdict_source	amp : Analyse des fichiers.
Disposition	"1" : Inconnu. "2" : Propre. "3" : Malveillant (amp). "4" : Non analysable (non analysable).
Nom D'Espion	Vide : Si la stratégie d'attaque AMP n'est pas utilisée. Détection_Personnalisée_Simple : Si une stratégie d'attaque AMP est utilisée.
Action_téléchargement	Vrai : est défini sur sandbox. Faux : n'est pas envoyé au sandbox.
Sha256	SHA256 du fichier.

Nom_menace	Nom de la menace basé sur les types de menace AMP.

Autres informations utiles

- Intégrer AMP for Endpoints et Threat Grid à SWA
- Filtrage par réputation de fichiers et analyse de fichiers
- Systèmes d'assistance technique et de documentation

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.