Dépannage des journaux Secure Web Appliance et Advanced Malware Protection (ampverdict)

Table des matières

Introduction

Ce document décrit la section ampverdict dans le niveau de journal INFO et DEBUG du moteur Advanced Malware Protection (AMP) de l'appliance de sécurité Web (WSA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- WSA installé
- Réputation des fichiers et analyse des fichiers activés
- Protection avancée contre les malwares
- Appareil Web sécurisé Cisco
- Client SSH

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

WSA offre une intégration avec AMP for Endpoints et un moteur AMP local. AMP offre une protection contre les programmes malveillants de type « zero-day » grâce aux fonctions de

réputation et d'analyse des fichiers. Le WSA 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 WSA et non le cloud AMP ou Threat Grid.

Dépannage des journaux WSA 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 CLI via le client SSH.

2. Tapez la commande grep et appuyez sur la touche Entrée.

3. Entrez le numéro de amp_logs tel qu'il est commandé.

4. Répondez aux options suivantes (si vous exécutez du trafic en direct, choisissez l'option pour suivre les journaux).
5. Appuyez sur la touche Entrée.

6. Les journaux s'affichent.

Les journaux WSA AMP existent dans différents niveaux d'information, vous pouvez sélectionner le niveau INFO ou DEBUG les résultats qui ont de légères différences expliquées dans la section suivante.

 Remarque : la licence AMP doit être installée sur WSA 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 qu'Advanced Malware Protection n'a pas demandé le téléchargement du fichier pour analyse « 1 » indique qu'Advanced Malware Protection 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 de fichier 2 : Expiration de l'analyse des fichiers 3 : Erreur d'analyse Supérieur à 3 : fichier malveillant
Verdict_source	amp : analyse de fichiers
Disposition	1 : Inconnu 2 : Nettoyer 3 : Malveillant (amp) 4 : Non analysable (non analysable)
Nom D'Espion	Vide : si la stratégie d'attaque AMP n'est pas utilisée Simple_Custom_Detection : si une stratégie d'attaque AMP est utilisée
Action_téléchargement	True : le fichier est défini sur sandbox False : le fichier n'est pas envoyé au sandbox
Sha256	SHA256

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

Informations connexes

- Intégration d'AMP for Endpoints et de Threat Grid avec WSA
- Filtrage par réputation de fichiers et analyse de fichiers
- Assistance et documentation techniques - Cisco Systems

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.