Solución de problemas de Secure Web Appliance y registros de protección frente a malware avanzado (ampverdict)

Contenido

Introducción

Este documento describe la sección "ampverdict" en el nivel de registro **INFO** y **DEBUG** del motor de protección frente a malware avanzado (AMP) del dispositivo de seguridad web (WSA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- WSA instalado
- Reputación de archivos y Análisis de archivos habilitados
- Protección frente a malware avanzado
- Dispositivo web seguro de Cisco
- cliente SSH

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

WSA ofrece integración con AMP para terminales y un motor AMP local. AMP ofrece protección frente a malware frente a malware de día cero mediante las funciones de análisis de archivos y

reputación de archivos. WSA incluye un motor de preclasificación que se encarga de los análisis de archivos internamente antes de las comprobaciones de la nube pública. Los registros descritos en la siguiente sección están relacionados con el motor de AMP en WSA, no con la nube de AMP o Threat Grid.

Solución de problemas de registros de WSA AMP

Acceda a los registros de AMP. Inicie sesión a través de CLI y siga o aumente los registros amp:

1. Inicie sesión en la **CLI** a través del cliente SSH.

2. Escriba el comando **grep** y presione la **tecla Intro**.

3. Introduzca el número de **amp_logs** a medida que se solicita.

4. Responda a las siguientes opciones (Si ejecuta tráfico en directo, elija la opción para **seguir** los registros).
5. Pulse la tecla **Intro**.

6. Se muestran los registros.

Los registros de AMP de WSA existen en diferentes niveles de información, puede seleccionar el nivel **INFO** o **DEBUG** los resultados que tienen ligeras diferencias explicadas en la siguiente sección.

> **Nota:** La licencia de AMP debe instalarse en WSA para seleccionar los registros de AMP.

Registros de nivel de AMP INFO:

```
Wed Apr 27 12:21:26 2022 Info: Txn 18210 Binary scan on instance[0] Id[1345]: AMP allocated
memory = 0, AMP used memory = 0, Scans in flight = 1, Active faster connections = 1, Active
slower connections = 0
Wed Apr 27 12:21:35 2022 Info: Binary scan on instance[0] id[1345]:
filename[npp.8.4.Installer.x64.exe] filemime[application/x-dosexec] file_extension[exe]
length[4493047b] ampverdict[(1, 1, 'amp', '', 0, 0, True)] scanverdict[0] malwareverdict[0]
spyname[] SHA256[ecdcf497418a1988ebf20c647acadc9eca7bc8569fd980713582acd0de011ba1] From[Cloud]
uploadreason[Enqueued in the local queue for submission to upload] verdict_str[FILE UNKNOWN]
is_slow[0] scans_in_flight[0] Active faster connections[0] Active slower connections[0]
Wed Apr 27 12:22:28 2022 Info: File uploaded for analysis. Server:
https://panacea.threatgrid.com, SHA256:
ecdcf497418a1988ebf20c647acadc9eca7bc8569fd980713582acd0de011ba1, Filename:
npp.8.4.Installer.x64.exeTimestamp: 1651044116 sampleid[]
```

Registros de nivel de AMP INFO (ampverdict):

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

Registros de nivel de DEBUG de AMP:

```
Fri Apr 29 01:38:40 2022 Debug: Binary scan: proxid[3951] filename[favicon.ico] len[41566b]
readtime[109.721680ms] scantime[2.205322ms] ampverdict[(1, 1, 'amp', '', 0, 0, False)]
```

```
scanverdict[0] malwareverdict[0]
SHA256[e7a2345c75a03e63202b12301c29bb8b6bae7cef9e191ed58797ec028def7c4f] From[Cloud]
FileName[favicon.ico] FileMime[application/octet-stream]
```

Registros de nivel de DEBUG de AMP (ampverdict):

```
ampverdict[(1, 1, 'amp', '', 0, 0, False)]
ampverdict[(analysis_action, scan_verdict,disposition, ‘spyname: policy name if amp registered
with console’, file_reputation, upload_action, ‘sha256', ‘threat_name’)]
```

Campos detallados frente a opciones de valor:

Campo	Valor
Acción_de_análisis	"0" indica que la protección frente a malware avanzado solicitó la carga del archivo para su análisis. "1" indica que la protección frente a malware avanzado solicitó la carga del archivo para su análisis
Scan_verdict	0: El archivo no es malicioso 1: El archivo no se escaneó debido a su tipo de archivo 2: Se agotó el tiempo de espera del análisis de archivo 3: Error de escaneo Más de 3: El archivo es malicioso
Verdict_source	amp: análisis de archivos
Disposición	1: Desconocido 2: Limpiar 3: Malintencionado (amp) 4: No escaneable (no escaneable)
Nombre de espía	Vacío: si no se utiliza la política de brotes de AMP Simple_Custom_Detection: si se utiliza una política de de AMP
Cargar_acción	Verdadero: archivo establecido en sandbox Falso: el archivo no se envía al sandbox
Sha256	SHA256
Threat_name	Nombre de amenaza basado en tipos de amenazas de AMP

Información Relacionada

- Integre AMP para terminales y Threat Grid con WSA
- Filtrado de reputación de archivos y análisis de archivos
- Soporte técnico y documentación - Cisco Sistemas