Risoluzione dei problemi relativi a Secure Web Appliance e registri di protezione avanzata da malware (ampverdict)

Sommario

Introduzione

Questo documento descrive la sezione Ampverdict nel livello di log **INFO** e **DEBUG** del motore Advanced Malware Protection (AMP) di Web Security Appliance (WSA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- WSA installato
- Reputazione dei file e analisi dei file abilitate
- Protezione avanzata da malware
- Cisco Secure Web Appliance
- Client SSH

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

WSA offre l'integrazione con AMP for Endpoints e un motore AMP locale. AMP fornisce protezione da malware per malware zero-day attraverso la reputazione dei file e le funzionalità di analisi dei

file. WSA include un motore di preclassificazione che è responsabile della scansione dei file internamente prima dei controlli cloud pubblici. I registri descritti nella sezione successiva sono relativi al motore AMP su WSA e non al cloud AMP o alla Threat Grid.

Risoluzione dei problemi relativi ai registri AMP WSA

Accedere ai registri AMP. Effettuare il login dalla CLI e completare o eliminare i log amp:

1. Accedere alla **CLI** tramite il client SSH.

2. Digitare il comando **grep** e premere il tasto **Invio**.

3. Inserire il numero di **amp_logs** così come è ordinato.

4. Rispondi alle opzioni seguenti (Se esegui traffico in tempo reale, scegli l'opzione per la **coda** dei log).
5. Premere **Invio**.

6. Vengono visualizzati i registri.

I registri AMP WSA sono disponibili in diversi livelli di informazioni. È possibile selezionare il livello **INFO** o eseguire il **DEBUG** dei risultati che presentano lievi differenze, come illustrato nella sezione successiva.

> **Nota:** Per selezionare i registri AMP, è necessario installare la licenza AMP su WSA.

Registri livello 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[]
```

Registri livello AMP INFO (ampverdict):

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

Registri livello DEBUG 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]
```

Registri livello DEBUG 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’)]
```

Opzioni Campo dettagliato e Valore:

Campo	Valore
Analisi	"0" indica che Advanced Malware Protection non ha richiesto il caricamento del file per l'analisi "1" indica che Advanced Malware Protection ha richies caricamento del file per l'analisi
Analizza_verdetto	0: Il file non è dannoso 1: Impossibile analizzare il file a causa del tipo di file 2: Timeout dell'analisi dei file 3: Errore di scansione Maggiore di 3: Il file è dannoso
Origine_verdetto	amp: analisi dei file
Disposizione	1: Sconosciuto 2: Clean 3: Dannoso (amp) 4: Non analizzabile (non analizzabile)
Spyname	Vuoto: se non si utilizza la politica in materia di focolai AMP Simple_Custom_Detection: se si utilizza una politica in materia di focolai di AMP
Azione_caricamento	Vero: il file è impostato sulla sandbox Falso: il file non viene inviato alla sandbox
Sha256	SHA256
Nome_minaccia	Nome della minaccia in base ai tipi di minaccia AMP

Informazioni correlate

- Integrazione di AMP for Endpoints and Threat Grid con WSA
- Filtraggio della reputazione e analisi dei file
- Documentazione e supporto tecnico - Cisco Sistemi