Solucionar problemas do Secure Web Appliance e dos Logs de Proteção Avançada contra Malware (ampverdict)

Contents

Introduction

Este documento descreve a seção ampverdict no nível de log **INFO** e **DEBUG** do mecanismo de Proteção avançada contra malware (AMP) do Web Security Appliance (WSA).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- WSA instalado
- Reputação de arquivos e análise de arquivos ativados
- Proteção avançada contra malware
- Cisco Secure Web Appliance
- cliente SSH

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O WSA oferece integração com o AMP para endpoints e um mecanismo AMP local. A AMP oferece proteção contra malware de dia zero por meio de recursos de análise de arquivos e reputação. O WSA inclui um mecanismo de pré-classificação que é responsável por verificações

de arquivos internamente antes de verificações de nuvem pública. Os registros descritos na próxima seção estão relacionados ao mecanismo AMP no WSA e não à nuvem AMP ou ao Threat Grid.

Solucionar problemas de registros do WSA AMP

Acesse os registros do AMP. Efetue login via CLI e siga ou esfregue os logs de amp:

1. Faça login na **CLI** através do SSH Client.

2. Digite o comando **grep** e pressione a tecla **Enter**.

3. Digite o número de **amp_logs** conforme solicitado.

4. Responda às opções a seguir (se você executar o tráfego ao vivo, escolha a opção para **seguir** os registros).
5. Pressione a tecla **Enter**.

6. Os registros são exibidos.

Os registros do WSA AMP existem em diferentes níveis de informações. Você pode selecionar o nível **INFO** ou **DEBUG** dos resultados que têm pequenas diferenças explicadas na próxima seção.

> **Note**: A licença do AMP precisa ser instalada no WSA para selecionar os registros do AMP.

Logs de nível de INFORMAÇÕES da AMP:

```
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[]
```

Logs de nível de INFORMAÇÕES da AMP (ampverdict):

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

Logs de nível de DEPURAÇÃO do 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]
```

Logs de nível de DEPURAÇÃO do 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’)]
```

Campo detalhado vs opções de valor:

Campo	Valor
Analysis_action	"0" indica que o Advanced Malware Protection não sol o upload do arquivo para análise "1" indica que o Advanced Malware Protection solicitou upload do arquivo para análise
Varredura_veredito	0: O arquivo não é mal-intencionado 1: O ficheiro não foi analisado devido ao respectivo tip ficheiro 2: Tempo limite da verificação de arquivo esgotado 3: Erro de digitalização Maior que 3: O arquivo é mal-intencionado
Fonte_do_veredito	amp: análise de arquivo
Disposição	1: Desconhecido 2: Limpar 3: Mal-intencionado (amp) 4: Não verificável (não verificável)
Spyname	Vazio: se a política de detecção de AMP não for usada Simple_Custom_Detection: se uma política de detecçã AMP for usada
Upload_action	Verdadeiro: arquivo definido como sandbox Falso: o arquivo não foi enviado para o sandbox
Sha256	SHA256
Nome_da_ameaça	Nome da ameaça com base nos tipos de ameaça da A

Informações Relacionadas

- Integre o AMP para endpoints e o Threat Grid com o WSA
- Filtragem de reputação de arquivo e análise de arquivo
- Suporte técnico e documentação - Cisco Sistemas