排除安全Web设备和高级恶意软件防护日志(ampverdict)故障

目录

简介

本文档介绍网络安全设备(WSA)的高级恶意软件防护(AMP)引擎的**INFO**和**DEBUG** 日志级别中的ampverdict部分。

先决条件

要求

Cisco 建议您了解以下主题：

- 已安装WSA
- 已启用文件信誉和文件分析
- 高级恶意软件保护
- 思科安全网络设备
- SSH客户端

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

WSA提供与面向终端的AMP和本地AMP引擎的集成。AMP通过文件信誉和文件分析功能提供零日恶意软件防护。WSA包括一个预分类引擎，负责在公共云检查之前进行内部文件扫描。下一节中介绍的日志与WSA上的AMP引擎相关，与AMP云或Threat Grid无关。

排除WSA AMP日志故障

访问AMP日志。通过CLI和tail或grep登录amp日志：

1.通过SSH客户端登录CLI。

2.键入命令grep并按Enter键。

3.输入按顺序排列的amp_log数。

4.回答以下选项(如果运行实时流量，请选择跟踪日志的选项)。
5.按Enter键。

6.显示日志。

WSA AMP日志存在于不同的信息级别，您可以选择INFO级别或DEBUG结果，这些结果在下一节中会有所说明。

注意：需要在WSA上安装AMP许可证，以选择AMP日志。

AMP信息级别日志：

```
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[]
```

AMP信息级别日志(ampverdict):

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

AMP调试级别日志：

```
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]
```

AMP调试级别日志(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’)]
```

详细字段与值选项：

字段	价值
Analysis_action	“0”表示高级恶意软件防护未请求上传文件以供分析 “1”表示高级恶意软件防护确实请求上传文件进行分析
Scan_verdict	0:该文件不是恶意的 1:由于文件类型，未扫描该文件 2:文件扫描超时 3:扫描错误 大于 3:文件是恶意的
裁决源	amp:文件分析
处置	1:未知 2:Clean（清理） 3:恶意(amp) 4:不可扫描（不可扫描）
Spyname	空：如果未使用AMP爆发策略 Simple_Custom_Detection:如果使用AMP爆发策略
Upload_action	正确：文件设置为沙盒 错误：文件不发送到沙盒
SHA256	SHA256
Threat_name	基于AMP威胁类型的威胁名称

相关信息

- 将面向终端的AMP和Threat Grid与WSA集成
- 文件信誉过滤和文件分析
- 技术支持和文档 — 思科 系统