查看ESA上mail_logs中的图像分析裁决分数

目录

简介

概述

- 支持的文件类型

先决条件

限制

查看特定邮件的判定得分

- 步骤
- 预期结果

相关信息

简介

本文档介绍如何在运行AsyncOS for Email Security的ESA上查看邮件的图像分析判定得分。

概述

ESA代表思科邮件安全设备。图像分析需要许可证才能启用。某些邮件包含组织可以扫描不适当内容的图像。图像分析不是为了补充或替换防病毒和防垃圾邮件扫描引擎而设计的。其目的是通过识别电子邮件中的不当内容来强制进行可接受的使用。

配置用于图像分析的邮件安全的Cisco AsyncOS后，使用图像分析过滤器规则对可疑或不适当的邮件执行操作。

支持的文件类型

图像分析可以扫描附加的图像文件类型：

- BMP
- GIF
- ICO
- JPEG
- PCX
- PNG
- TGA
- TIFF

图像分析器使用测量皮肤颜色、身体大小和曲率的算法来确定图形包含不适当内容的概率。扫描图像附件时，Cisco指纹确定文件类型，图像分析器评估图像内容。如果图像嵌入到另一个文件中

，Stellent扫描引擎会提取该图像（例如，从Word、Excel和PowerPoint文档）。 图像分析判定的结果是对整个消息进行计算。如果邮件不包含图像，则Image Analysis将指定得分为0（正常）。

注意：无法从PDF文件中提取图像。

先决条件

- 已安装映像分析许可证。
- Cisco AsyncOS for Email Security(AsyncOS)中启用了映像分析。
- 访问mail_logs（CLI或GUI访问）和邮件ID(MID)，以便邮件进行调查。

限制

- 对消息整体进行判定；邮件日志报告每个附件的结果（例如，ZIP附件显示ZIP文件名及其内部图像的最大得分）。
- 无法从PDF文件中提取图像。

查看特定邮件的判定得分

步骤

1. 标识消息的消息ID(MID)。
2. 访问mail_logs（从GUI或CLI，具体取决于部署）。
3. 搜索包含MID和图像分析的日志条目。
4. 记录附件名称、分数，以及附件是否标记为不可扫描。
5. 查看后续日志行以了解所采取的操作（例如，过滤规则操作、隔离或丢弃）。

预期结果

日志条目显示附件名称、图像分析分数，以及附件是可扫描的还是不可扫描的。日志不会直接将分数映射到判定标签。

此示例显示了mail_logs中与图像分析相关的条目：

```
Thu Apr 3 08:17:56 2009 Debug: MID 154 IronPort Image Analysis: image 'Unscannable.jpg'
 is unscannable.
Thu Apr 3 08:17:56 2009 Info: MID 154 IronPort Image Analysis: attachment
 'Unscannable.jpg' score 0 unscannable
Thu Apr 3 08:17:56 2009 Info: MID 6 rewritten to MID 7 by
 drop-attachments-where-image-verdict filter 'f-001'
Thu Apr 3 08:17:56 2009 Info: Message finished MID 6 done
```

相关信息

- AsyncOS电子邮件用户指南
- 思科全球支持联系方式
- 产品技术支持和文档

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。