在邮件安全设备上测试高级恶意软件防护

目录

[简介](#)

[背景信息](#)

[在ESA上测试AMP](#)

[功能密钥](#)

[安全性服务](#)

[传入邮件策略](#)

[测试](#)

[AMP+邮件的高级邮件跟踪](#)

[高级恶意软件防护报告](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何测试和验证思科邮件安全设备(ESA)上的高级恶意软件防护(AMP)功能。

背景信息

开始之前，请确认文件信誉和文件分析功能密钥处于活动状态，并且AMP已在传入邮件策略中启用。此过程验证ESA扫描附件，并在检测到恶意软件时应用预期操作，例如丢弃或重写。在mail_logs for AMP verdict entries和GUI中的Message Tracking and Monitor > Advanced Malware Protection中确认结果。

在ESA上测试AMP

随着ESA版AsyncOS 8.5的发布，AMP将执行文件信誉扫描和文件分析，以检测附件中的恶意软件。

功能密钥

要实施AMP，您必须拥有用于文件信誉和文件分析的有效且活动的ESA功能密钥。访问GUI上的系统管理>功能密钥，或者使用CLI上的功能密钥验证功能密钥。

安全性服务

要从GUI启用该服务，请导航到安全服务>文件信誉和分析。从CLI，您可以运行ampconfig。提交并确认对配置的更改。

传入邮件策略

启用服务后，您必须将此服务与传入邮件策略关联。

1. 导航到邮件策略>传入邮件策略。
2. 根据需要选择您的默认策略或预配置的策略。此时将显示“传入邮件策略”页上的高级恶意软件防护列。
3. 为该列选择Disabled链接，并在选项页面上选择Enable File Reputation和Enable File Analysis。
4. 您可以根据需要对邮件扫描、不可扫描附件的操作以及确认的邮件的操作进行任何其他配置增强功能。
5. 提交并确认对配置的更改。

测试

您的传入邮件策略现已启用以扫描和检测恶意软件。您必须具有用于测试的真实恶意软件样本。如果您需要有效示例，请访问欧洲计算机防病毒研究所(eicar) 下载页面。

⚠ 注意：当这些文件或AV扫描仪与这些文件结合使用导致计算机或网络环境受到任何损害时，思科不承担任何责任。下载这些文件需要您自担风险。仅当使用AV扫描程序、计算机设置和网络环境足够安全时，才下载这些文件。提供此信息是出于测试和复制目的而提供的。

通过您的ESA发送附件，并使用有效的预配置电子邮件帐户进行正常处理。您可以使用ESA的CLI和tail mail_logs监控邮件处理。您可以看到邮件日志中列出的邮件ID(MID)。 屏幕上会显示与下图类似的输出：

<#root>

```
Thu Sep 18 16:17:38 2014 Info: New SMTP ICID 16488 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
```

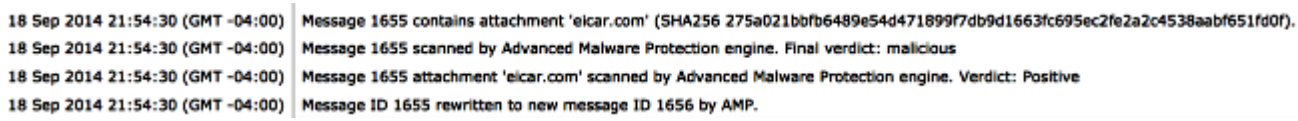
```
Thu Sep 18 16:17:38 2014 Info: ICID 16488 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
Thu Sep 18 16:17:38 2014 Info: Start MID 1653 ICID 16488
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 From: <joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 Message-ID '<BLU437-SMTP10E1315A60354F2
906677B9DB70@phx.gbl>'
Thu Sep 18 16:17:38 2014 Info: MID 1653 Subject 'Your Daily Update''
Thu Sep 18 16:17:38 2014 Info: MID 1653 ready 2313 bytes from
<joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Thu Sep 18 16:17:38 2014 Info: ICID 16488 close
Thu Sep 18 16:17:39 2014 Info: MID 1653 interim verdict using engine:
CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 using engine: CASE spam negative

Thu Sep 18 16:17:39 2014 Info: MID 1653 AMP file reputation verdict : MALWARE
Thu Sep 18 16:17:39 2014 Info: Message aborted MID 1653 Dropped by amp


Thu Sep 18 16:17:39 2014 Info: Message finished MID 1653 done
```

上一个示例显示，AMP检测到恶意软件附件，并根据默认设置将其作为最终操作进行丢弃。

从GUI的“邮件跟踪”(Message Tracking)中也会看到相同的详细信息：



如果您选择从“传入邮件策略”(Incoming Mail Policies)传送已确认的恶意软件或AMP配置中的其他高级选项，则可能会看到以下邮件处理结果：

```
Thu Sep 18 21:54:30 2014 Info: MID 1655 AMP file reputation verdict : MALWARE
Thu Sep 18 21:54:30 2014 Info: MID 1655 rewritten to MID 1656 by AMP
```

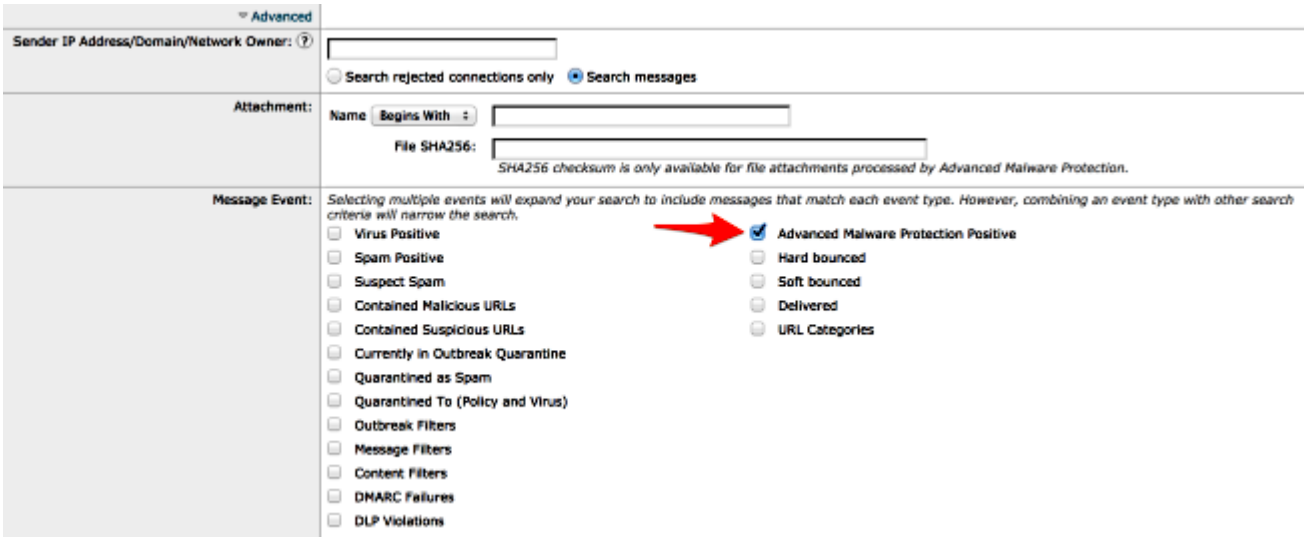
信誉判定结果对于MALWARE仍为正值，如下所示。重写操作取决于邮件修改操作和主题行的预置[警告：MALWARE DETECTED]。

干净的文件或处理时未被识别为恶意软件的文件会将此判定写入邮件日志：

```
Thu Sep 18 21:58:33 2014 Info: MID 1657 AMP file reputation verdict : CLEAN
```

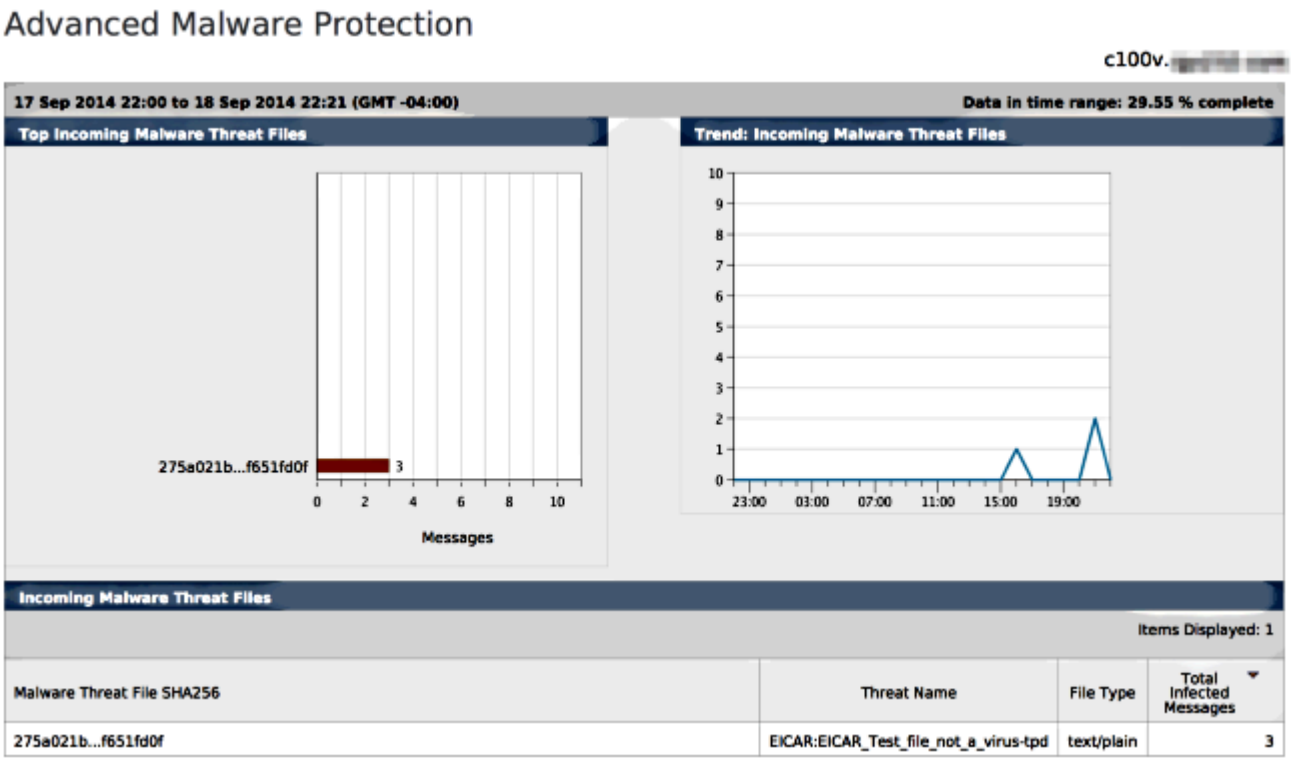
AMP+邮件的高级邮件跟踪

此外，在GUI中，当您使用“邮件跟踪”(Message Tracking)和“高级”(Advanced)下拉菜单时，您可以选择直接搜索高级恶意软件防护(Advanced Malware Protection Positive)邮件：



高级恶意软件防护报告

在ESA GUI中，您还会看到通过AMP的已识别邮件的报告跟踪。导航到监控>高级恶意软件防护，并根据需要修改时间范围。现在您会看到类似内容，前面几个示例用于输入：



故障排除

如果您没有看到已知、真实的恶意软件文件，AMP会主动扫描该文件，请查阅邮件日志，以确保在AMP扫描邮件之前，其他服务不会对邮件和/或附件采取措施。

从前面使用的示例来看，启用Sophos防病毒后，它实际上会捕获附件，并对其执行操作：

<#root>

```
Thu Sep 18 22:15:34 2014 Info: New SMTP ICID 16493 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 22:15:34 2014 Info: ICID 16493 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
Thu Sep 18 22:15:34 2014 Info: Start MID 1659 ICID 16493
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 From: <joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 Message-ID '<BLU437-SMTP2399199FA50FB
5E71863489DB40@phx.gbl>'
Thu Sep 18 22:15:34 2014 Info: MID 1659 Subject 'Daily Update Final'
Thu Sep 18 22:15:34 2014 Info: MID 1659 ready 2355 bytes from
<joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Thu Sep 18 22:15:35 2014 Info: ICID 16493 close
Thu Sep 18 22:15:35 2014 Info: MID 1659 interim verdict using engine:
CASE spam negative
Thu Sep 18 22:15:35 2014 Info: MID 1659 using engine: CASE spam negative

Thu Sep 18 22:15:37 2014 Info: MID 1659 interim AV verdict using Sophos VIRAL
Thu Sep 18 22:15:37 2014 Info: MID 1659 antivirus positive 'EICAR-AV-Test'
Thu Sep 18 22:15:37 2014 Info: Message aborted MID 1659 Dropped by antivirus


Thu Sep 18 22:15:37 2014 Info: Message finished MID 1659 done
```

传入邮件策略上的Sophos防病毒配置设置被设置为drop，以查找受病毒感染的邮件。在这种情况下，无法联系AMP对附件进行扫描或执行操作。

但实际情况并非始终如此。可能需要检查邮件日志和邮件ID(MID)，以确保其他服务或内容/邮件过滤器在AMP处理和达到操作之前未对MID执行操作。

相关信息

- ESA高级恶意软件防护最佳实践指南

- 思科邮件安全设备管理员指南 — 高级恶意软件防护
- 思科邮件安全设备 — 最终用户指南
- 技术支持和文档 - Cisco Systems

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）。