ESA高级恶意软件防护(AMP)测试

目录

简介

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

在ESA上测试AMP

随着AsyncOS 8.5 for the ESA的发布，AMP会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，您必须在ESA上同时具有文件信誉和文件分**析的有效**和活**动功**能密钥。访**问GUI上的System Administration > Feature Keys**，或在CLI上使用**featurekeys**，以验证功能密钥。

安全性服务

要从GUI启用服务，请导航至“安全服务”(**Security Services)>“文件信誉和分析”(File Reputation and Analysis)**。从CLI，您可以运行**ampconfig**。提交并提交对配置的更改。

传入邮件策略

启用服务后，必须将此服务与传入邮件策略关联。

1. 导航至“邮**件策略”>“传入邮件策略**”。
2. 根据需要**选择默**认策略或预配置策略。将显**示“传入邮**件策略”页上的“高级恶意软件防护”列。
3. 在选项**页**上，选择列的禁**用链接**，并**选择启用文**件信誉**和启用文件**分析。
4. 您可以根据需要对邮件扫描、不可扫描附件的操作和已确认邮件的操作进行任何进一步的配置增强。
5. 提交并提交对配置的更改。

测试

此时，您的传入邮件策略已启用，可扫描和检测恶意软件。您必须拥有真正的恶意软件样本，才能进行测试。如果需要有效的示例，请访[问欧洲计算机防病毒研究所(eicar)](#)下载页。

> **注意**：当这些文件或您的AV扫描仪与这些文件一起对您的计算机或网络环境造成任何损害时，思科不能承担责任。您以自己的风险下载这些文件。仅当您在使用AV扫描程序、计算机设置和网络环境时足够安全时，才下载这些文件。为了测试和复制目的，我们礼节性地提供此信息。

使用有效的预配置电子邮件帐户，通过ESA和正常处理发送附件。您可以使用ESA的CLI和**tail mail_logs**，以便在邮件处理时监控该邮件。您将看到邮件日志中列出的邮件ID(MID)。 如下所示的输出：

```
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**丢弃**作为根据默认设置的最终操作。

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

18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 contains attachment 'eicar.com' (SHA256 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f).
18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 scanned by Advanced Malware Protection engine. Final verdict: malicious
18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 attachment 'eicar.com' scanned by Advanced Malware Protection engine. Verdict: Positive
18 Sep 2014 21:54:30 (GMT -04:00)	Message ID 1655 rewritten to new message ID 1656 by AMP.

如果选择从传入邮件策略中提供明确识别的恶意软件或AMP配置中的其他高级选项，您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
```

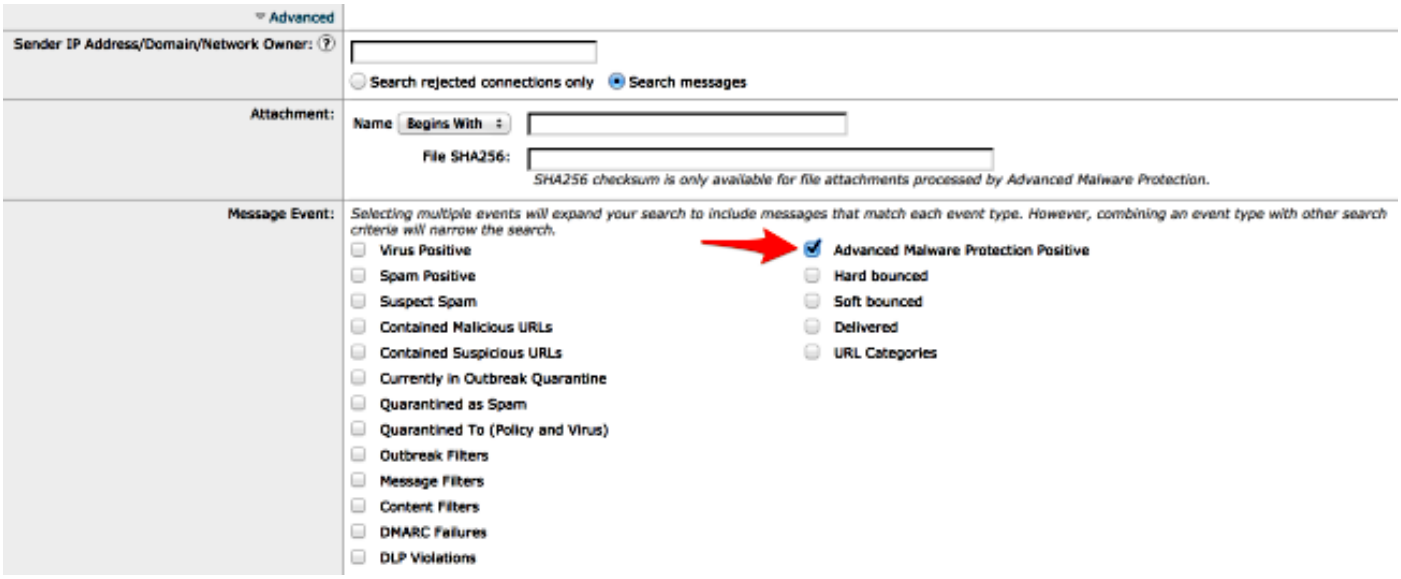
如图所示，信誉判定对**MALWARE**仍为正数。重写的操作是根据邮件修改操作和主题行预置的**[WARNING:检测到恶意软件]**。

干净的文件或在处理时未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
```

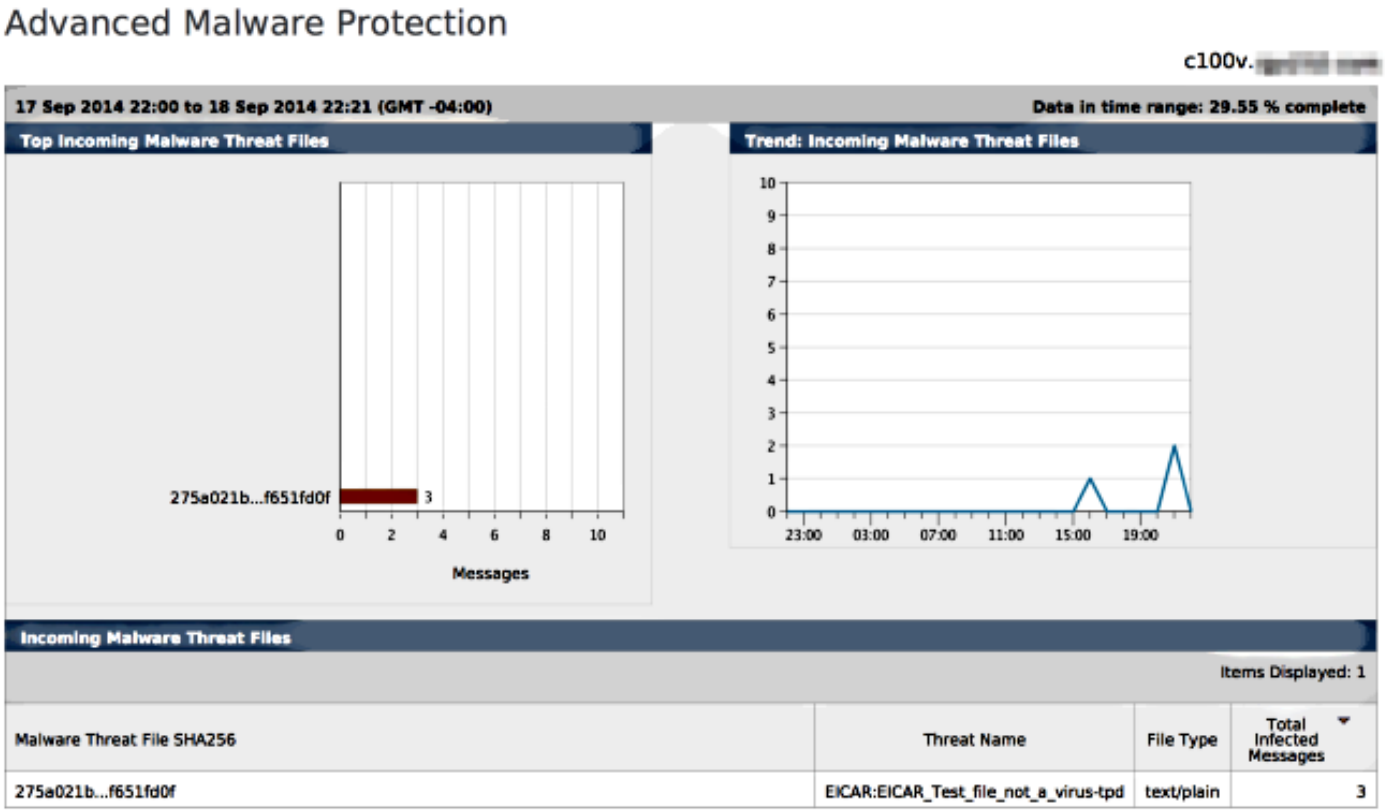
AMP+邮件的高级邮件跟踪

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



高级恶意软件防护报告

从ESA GUI中，您还会看到通过AMP确认的邮件的报告跟踪。导航至**Monitor > Advanced Malware Protection**，并根据需要修改时间范围。您现在看到类似的输入示例：



故障排除

如果您没有看到AMP正在扫描的已知的真恶意软件文件，请查看邮件日志，以确保在AMP扫描邮件之前，其他服务未对邮件和/或附件采取操作。

在前面使用的示例中，当启用Sophos防病毒时，它实际上会捕获并对附件采取操作：

```
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防病毒配置设置设置为**丢弃**受病毒感染的邮件。在此实例中，永远不会访问AMP以扫描附件或对附件执行操作。

但实际情况并非始终如此。可能需要查看邮件日志和邮件ID(MID)，以确保在AMP处理和操作到达之前，其他服务或内容/邮件过滤器未对MID采取操作。

相关信息

- 思科邮件安全设备 — 最终用户指南
- 技术支持和文档 - Cisco Systems