ESA提前的恶意软件保护(安培)测验

目录

简介

本文描述如何测试，并且验证思科的先进的恶意软件保护(安培)功能给安全工具(ESA)发电子邮件。

测试在ESA的安培

使用版本ESA的AsyncOS 8.5，安培执行文件名誉扫瞄和文件分析为了检测在附件的恶意软件。

功能键

为了实现安培，您必须有**文件名誉**和**文件分析的**一个有效和活动功能键在您的ESA。访问在GUI的**系统Administration>功能键**或者请使用在CLI的**featurekeys**，为了验证功能键。

安全性服务

为了启用从GUI的服务，请导航对**安全服务>文件名誉和分析**。从CLI，您能运行**ampconfig**。提交并且确认您的对配置的更改。

流入的邮件策略

一旦启用服务，您必须有此服务附加对流入的邮件策略。

1. 导航**邮寄策略>流入的邮件策略**。
2. 选择您的**默认策略**或预先配置的策略当必要时。 在流入的邮件的**先进的恶意软件保护**列修正页显示。
3. 选择列的**已禁用**链路，并且**启用文件名誉**并且**启用**在选项页的**文件分析**。
4. 您能做任何另外配置增强到消息扫描、操作非能扫描的附件的和操作确实地已确定消息的，当必要时。
5. 提交并且确认您的对配置的更改。

测验

此时，您的流入的邮件策略启用扫描和检测恶意软件。您必须有测试的一真的恶意软件示例。如果需要有效示例，请拜访计算机防病毒研究(eicar)下载页欧洲学院。

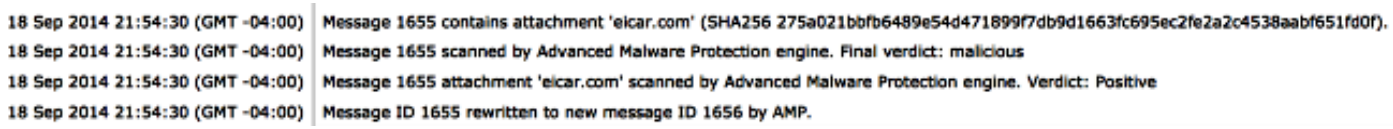
> **警告：** 当这些文件或您的AV扫描仪与这些文件的组合造成所有损伤对您的计算机或网络环境时，思科不可能保持负责。您下载这些FILE责任自负。 只有当是充分地安全在您的AV扫描仪、计算机设置和网络环境，使用情况请下载这些文件。此信息被提供作为礼貌为测验和再生产目的。

使用使用有效一个预先配置的电子邮件帐户，通过您ESA和正常处理发送附件。您能使用ESA的CLI，并且**尾标mail_logs**为了监控邮件作为它处理。您将看到在邮件日志(MID)列出的消息ID。 输出类似于此显示：

```
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
```

前一个示例显示安培检测恶意软件附件并且**丢弃了**作为每默认设置的最后的行动。

同样详细信息在从GUI的消息跟踪也被看到：



如果选择提供确实地已确定恶意软件，或者其他高级选项在安培配置里从流入的邮件策略，也许发现此邮件处理结果的您：

```
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
```

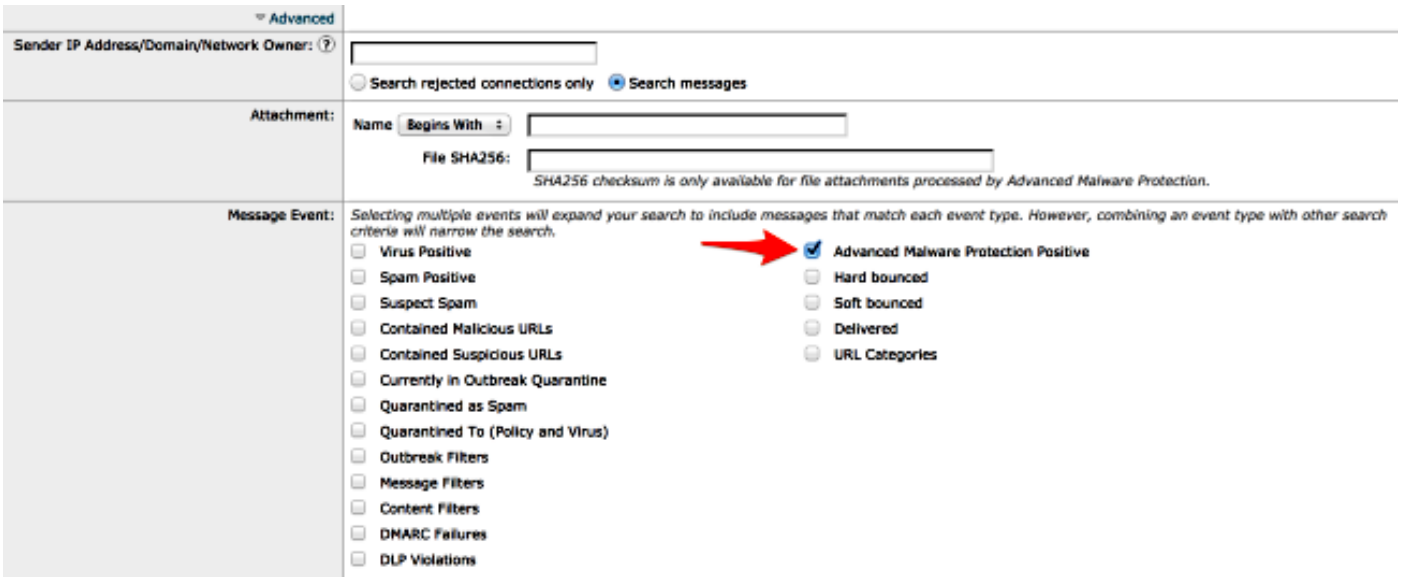
名誉判决为**恶意软件**是正的如显示。 重写的操作是每消息修改操作和标题栏加在前面**[警告：检测的恶意软件]**。

一个干净的文件或者未识别在处理时间作为恶意软件的文件，有此判决写入对邮件日志：

```
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
```

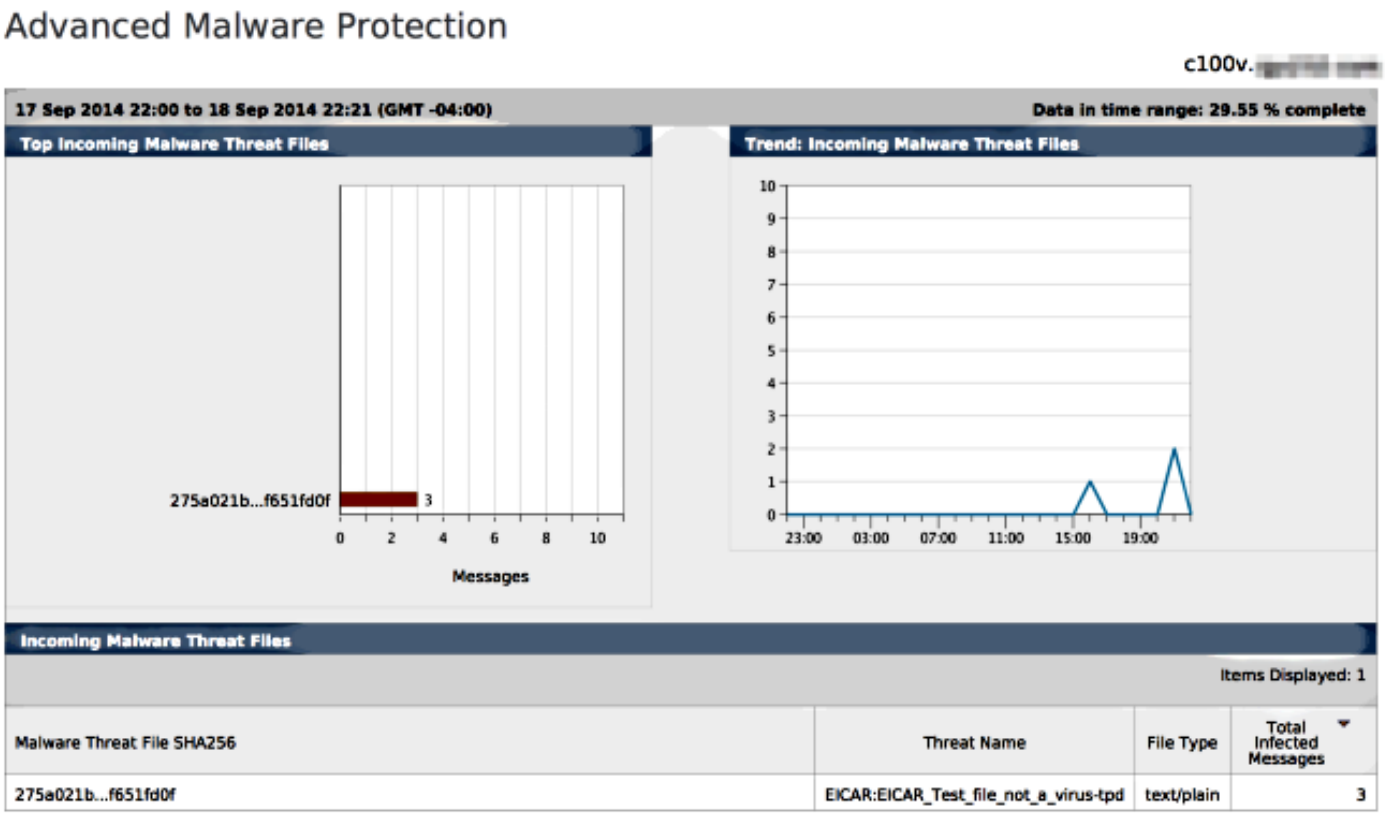
AMP+消息的先进的消息跟踪

并且从GUI，当您使用消息跟踪和先进的下拉菜单时，您能选择直接地搜索一个先进的恶意软件保护正消息：



先进的恶意软件保护报告

从ESA GUI，您为确实地已确定消息也看到报告跟踪通过AMP. Navigate对**监视器>提前的恶意软件保护**并且修改时间范围当必要时。您为输入当前看到类似，与前面的示例：



故障排除

如果看不到知道，由安培确实地扫描的真的恶意软件文件，查看邮件登录顺序保证另一服务没有采取在消息和附件的行动，在安培扫描了消息前。

从使用的更早的示例，当Sophos防病毒启用时，它实际上捉住并且采取在附件的行动：

```
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
```

在流入的邮件策略的Sophos抗病毒配置设置设为病毒被传染的消息**下降**。 在这种情况下，安培从未被到达扫描或采取在附件的行动。

但实际情况并非始终如此。邮件日志和消息ID (MID)的回顾也许是需要的为了保证另一服务或内容/消息过滤器没有采取行动MID在处理的安培前和操作被到达了。

相关信息

- 思科电子邮件安全工具-最终用户指南
- 技术支持和文档 - Cisco Systems