

ESA先进的Malware保护(AMP)测试

Contents

[Introduction](#)

[测试在ESA的AMP](#)

[功能键](#)

[安全服务](#)

[流入的邮件策略](#)

[测试](#)

[AMP+消息的先进的消息跟踪](#)

[先进的Malware保护报告](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

本文描述如何测试，并且验证Cisco的先进的Malware保护(AMP)功能给安全工具(ESA)发电子邮件。

测试在ESA的AMP

使用版本ESA的AsyncOS 8.5，AMP执行文件名扫描和文件分析为了发现在附件的malware。

功能键

为了实现AMP，您必须有**文件名扫描和文件分析**的一个有效和活动功能键在您的ESA。访问**系统 Administration>**在GUI的**功能键**或者请使用在CLI的**featurekeys**，为了验证功能键。

安全服务

为了enable (event)从GUI的服务，连接对**安全服务>文件名扫描和分析**。从CLI，您能运行**amconfig**。提交并且确认您的对配置的更改。

流入的邮件策略

一旦启用了服务，您必须有此服务附加对一个流入的邮件策略。

1. 连接**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Malware保护**列修正页显示。
3. 为列选择**失效链路**和**Enable (event)文件名誉**和**Enable (event)文件分析**在选项页。
4. 您能做任何另外配置增进到消息扫描、动作非能扫描的附件的和动作确实地被识别的消息的，当必要时。
5. 提交并且确认您的对配置的更改。

测试

此时，您的流入的邮件策略被启用扫描和发现malware。您必须有测试的一个真的malware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扫描程序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，Cisco不可能负责任。您下载这些FILE责任自负。只有当是充分地安全在您的AV扫描程序、计算机设置和网络环境，使用方法请下载这些文件。此信息被提供作为礼貌为测试和再生产目的。

使用使用有效一个预先配置的电邮帐户，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

前一个示例表示，AMP发现了malware附件并且下降了作为每默认设置的最后的行动。

同样详细资料在从GUI的消息跟踪也被看到：

```
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.
```

如果选择提供确实地被识别的malware，或者其他高级选项在AMP配置从流入的邮件策略，您也许发现此邮件处理结果：

```
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MALWARE是正的如显示。重写的动作是每消息修改动作和标题栏加在前面[警告：被发现的MALWARE]。

一个干净的文件或者未被识别在处理时间作为malware的文件，有给邮件日志被写的此判决：

```
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Malware保护正消息：

Advanced

Sender IP Address/Domain/Network Owner: ?

Search rejected connections only Search messages

Attachment:

Name: Begins With

File SHA256:

SHA256 checksum is only available for file attachments processed by Advanced Malware Protection.

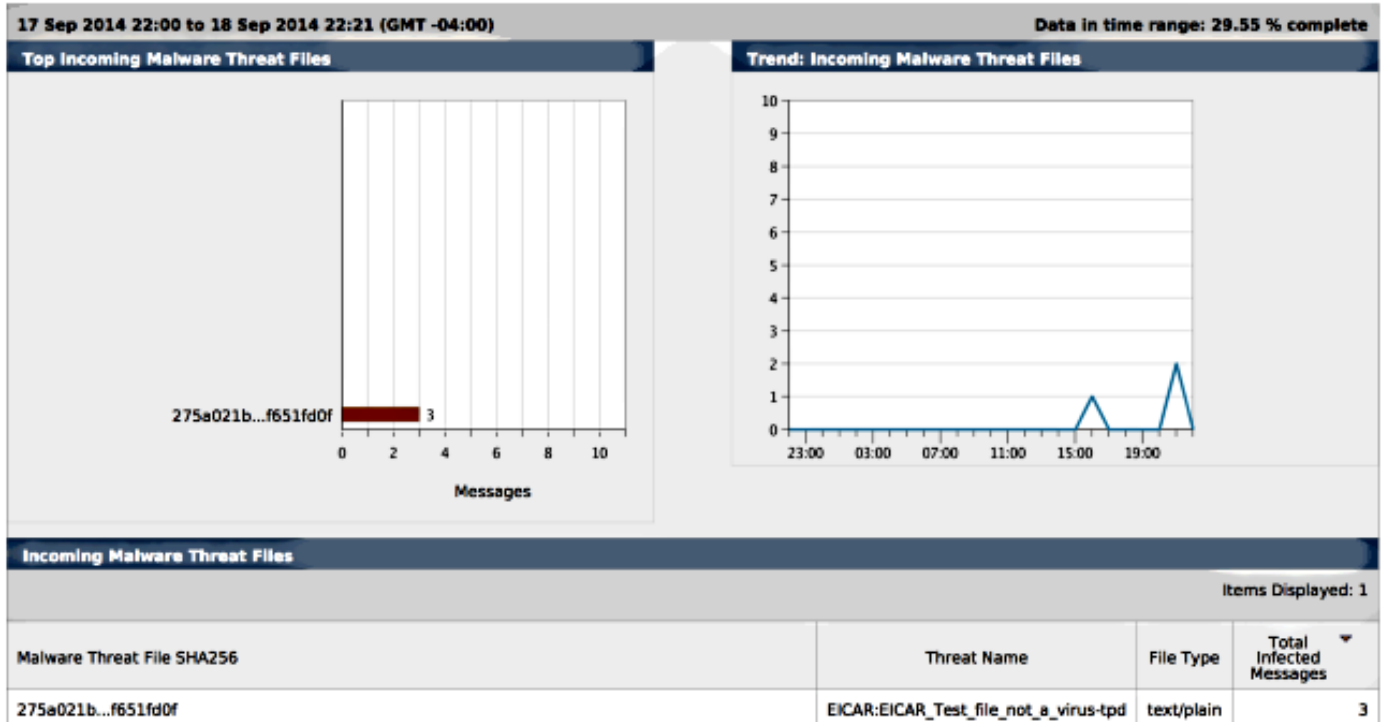
Message Event:

Selecting multiple events will expand your search to include messages that match each event type. However, combining an event type with other search criteria will narrow the search.

- Virus Positive
- Spam Positive
- Suspect Spam
- Contained Malicious URLs
- Contained Suspicious URLs
- Currently in Outbreak Quarantine
- Quarantined as Spam
- Quarantined To (Policy and Virus)
- Outbreak Filters
- Message Filters
- Content Filters
- DMARC Failures
- DLP Violations
- Advanced Malware Protection Positive
- Hard bounced
- Soft bounced
- Delivered
- URL Categories

先进的Malware保护报告

从ESA GUI，您为确实地被识别的消息也看到报告跟踪通过AMP. Navigate **监控>Advanced Malware保护**和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：



Troubleshoot

如果看不到知道，由AMP确实地扫描的真的malware文件，查看邮件登录顺序保证另一项服务没有采取对消息和附件的行动，在AMP扫描了消息前。

从使用的更早的示例，当抗病毒的Sophos是启用的时，它实际上捉住并且采取对附件的行动：

```
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 sbars
[-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
```

设在流入的邮件策略的Sophos抗病毒配置设置为病毒被传染的消息下降。在这种情况下，AMP从未被到达扫描或采取对附件的行动。

这总是不是实际情形。邮件日志和消息ID (MIDs)的回顾也许是为了保证另一项服务或内容/消息过滤器没有采取行动MID在处理的AMP前和动作被到达了。

Related Information

- [Cisco电子邮件安全工具-终端用户指南](#)
- [Technical Support & Documentation - Cisco Systems](#)