如何传送示例消息保证抗病毒引擎在思科电子邮件安全工具(ESA)扫描

目录

简介

本文描述如何传送示例消息保证或者抗病毒的Sophos或McAfee抗病毒引擎在思科电子邮件安全工具(ESA)扫描。

如何传送示例消息保证抗病毒引擎在思科电子邮件安全工具(ESA)扫描

通过发送与一测验病毒有效负载的一个示例消息通过ESA，我们能触发Sophos或McAfee抗病毒引擎。 在之前执行在本文列出的步骤，您将需要设置您的流入或流出的邮件策略和配置邮件策略有抗病毒丢弃或检疫病毒被传染的消息。 本文使用从将模拟测验病毒作为附件的EICAR提供的ASCII代码(www.eicar.org) ：

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

> **Note**:每EICAR ：*此测试文件提供了给EICAR为分配作为"EICAR标准的抗病毒测试文件"，并且满足以上所列的所有标准。通过，因为它不是病毒是安全的和不包括恶意代码的任何片段。多数产品起反应对它，好象它病毒(他们典型地虽则报告它与一明显的名称，例如"EICAR AV TEST")。*

创建Txt文件

使用以上的ASCII字符串，请创建.txt文件并且放置字符串如写入作为文件的正文。 您能发送此文件作为在您的示例消息的一个附件。

发送示例消息

根据您如何工作，您能通过ESA多种方式传送示例消息。 两个示例方法是通过UNIX CLI使用**邮件**或从Outlook (或其他电子邮件应用程序)。

UNIX CLI

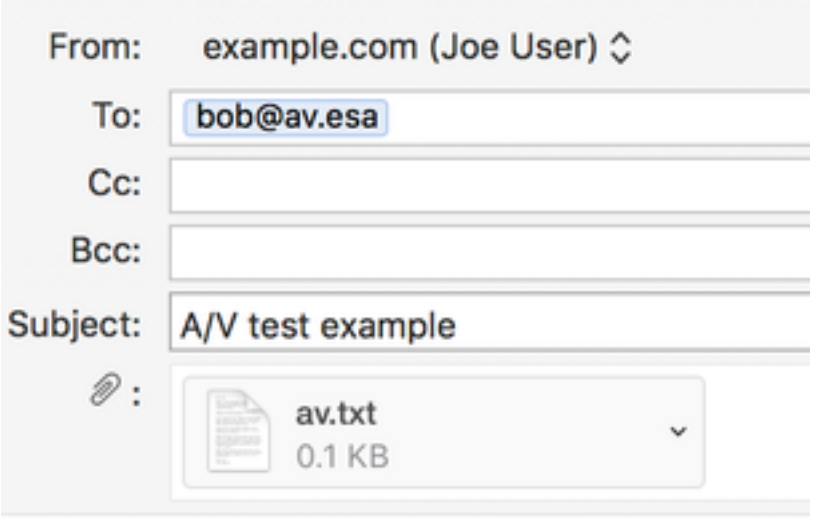
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt
bob@av.esa
```

您的UNIX环境将需要适当地设置通过您的ESA发送或中继邮件。

Outlook

使用Outlook (或另一个电子邮件应用程序)，您有两选择在通过发送ASCII代码：1)使用已创建.txt文件， 2) ASCII字符串的直接粘贴在邮件消息的正文的。

使用.txt文件作为附件：



TEST MESSAGE w/ ATTACHMENT

使用在邮件消息的正文的ASCII字符串：

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

您的Outlook (或其他电子邮件应用程序)将需要适当地设置通过您的ESA发送或中继邮件。

验证

在ESA CLI，请在发送示例消息之前请使用tail命令**mail_logs**。 当观看邮件记录您将看到时消息由

McAfee扫描并且捉住作为“病毒”：

```
Wed Sep 13 11:42:38 2017 Info: New SMTP ICID 306 interface Management (10.1.2.84) address
10.1.2.85 reverse dns host zane.local verified yes
Wed Sep 13 11:42:38 2017 Info: ICID 306 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country
Australia
Wed Sep 13 11:42:38 2017 Info: Start MID 405 ICID 306
Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 From: <joe@example.com>
Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 RID 0 To: <bob@av.esa>
Wed Sep 13 11:42:38 2017 Info: MID 405 Message-ID '<20170913153801.0EDA1A0121@example.com>'
Wed Sep 13 11:42:38 2017 Info: MID 405 Subject 'A/V test attachment'
Wed Sep 13 11:42:38 2017 Info: MID 405 ready 1057 bytes from <joe@example.com>
Wed Sep 13 11:42:38 2017 Info: MID 405 attachment 'av.txt'
Wed Sep 13 11:42:38 2017 Info: ICID 306 close
Wed Sep 13 11:42:38 2017 Info: MID 405 matched all recipients for per-recipient policy my_av in
the inbound table
Wed Sep 13 11:42:38 2017 Info: MID 405 interim AV verdict using McAfee VIRAL
Wed Sep 13 11:42:38 2017 Info: MID 405 antivirus positive 'EICAR test file'
Wed Sep 13 11:42:38 2017 Info: MID 405 enqueued for transfer to centralized quarantine "Virus"
(a/v verdict VIRAL)
Wed Sep 13 11:42:38 2017 Info: MID 405 queued for delivery
Wed Sep 13 11:42:38 2017 Info: New SMTP DCID 239 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:42:38 2017 Info: DCID 239 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-
SHA384 the.cpq.host
Wed Sep 13 11:42:38 2017 Info: Delivery start DCID 239 MID 405 to RID [0] to Centralized Policy
Quarantine
Wed Sep 13 11:42:38 2017 Info: Message done DCID 239 MID 405 to RID [0] (centralized policy
quarantine)
Wed Sep 13 11:42:38 2017 Info: MID 405 RID [0] Response 'ok:  Message 49 accepted'
Wed Sep 13 11:42:38 2017 Info: Message finished MID 405 done
Wed Sep 13 11:42:43 2017 Info: DCID 239 close
```

通过同样发送的消息和扫描用Sophos ：

```
Wed Sep 13 11:44:24 2017 Info: New SMTP ICID 307 interface Management (10.1.2.84) address
10.1.2.85 reverse dns host zane.local verified yes
Wed Sep 13 11:44:24 2017 Info: ICID 307 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country
Australia
Wed Sep 13 11:44:24 2017 Info: Start MID 406 ICID 307
Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 From: <joe@example.com>
Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 RID 0 To: <bob@av.esa>
Wed Sep 13 11:44:24 2017 Info: MID 406 Message-ID '<20170913153946.E20C7A0121@example.com>'
Wed Sep 13 11:44:24 2017 Info: MID 406 Subject 'A/V test attachment'
Wed Sep 13 11:44:24 2017 Info: MID 406 ready 1057 bytes from <joe@example.com>
Wed Sep 13 11:44:24 2017 Info: MID 406 attachment 'av.txt'
Wed Sep 13 11:44:24 2017 Info: ICID 307 close
Wed Sep 13 11:44:24 2017 Info: MID 406 matched all recipients for per-recipient policy my_av in
the inbound table
Wed Sep 13 11:44:24 2017 Info: MID 406 interim AV verdict using Sophos VIRAL
Wed Sep 13 11:44:24 2017 Info: MID 406 antivirus positive 'EICAR-AV-Test'
Wed Sep 13 11:44:24 2017 Info: MID 406 enqueued for transfer to centralized quarantine "Virus"
(a/v verdict VIRAL)
Wed Sep 13 11:44:24 2017 Info: MID 406 queued for delivery
Wed Sep 13 11:44:24 2017 Info: New SMTP DCID 240 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:44:24 2017 Info: DCID 240 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-
SHA384 the.cpq.host
Wed Sep 13 11:44:24 2017 Info: Delivery start DCID 240 MID 406 to RID [0] to Centralized Policy
Quarantine
Wed Sep 13 11:44:24 2017 Info: Message done DCID 240 MID 406 to RID [0] (centralized policy
quarantine)
Wed Sep 13 11:44:24 2017 Info: MID 406 RID [0] Response 'ok:  Message 50 accepted'
```

```
Wed Sep 13 11:44:24 2017 Info: Message finished MID 406 done
Wed Sep 13 11:44:29 2017 Info: DCID 240 close
```

在此实验室ESA，‘病毒被传染的消息的配置为“操作检疫应用对消息”在特定的邮件策略。 在您的ESA的操作可能根据病毒抗病毒处理的被传染的消息的执行的操作变化，在您的邮件策略。

相关信息

- 技术支持和文档 - Cisco Systems