方法アンチウィルス エンジンを確認するためにサンプル メッセージを送信 する Cisco E メール セキュリティ アプライアンス (ESA) でスキャンしています

目次

概要

この資料にアンチウィルス Sophos を確認するためにサンプル メッセージを送信 する方法を記述されていますまたは McAfee アンチウィルス エンジンは Cisco E メール セキュリティ アプライアンス (ESA) でスキャンしています。

方法アンチウィルス エンジンを確認するためにサンプル メッセージを送信 する Cisco E メール セキュリティ アプライアンス (ESA) でスキャンしています

ESA によるテスト ウイルス ペイロードが付いているサンプル メッセージの送信によって、Sophos または McAfee アンチウィルス エンジンを引き起こすことができます。 リストされているこの資料でステップを実行する前に、着信か発信 メール ポリシーを設定し、アンチウィルス ドロップするか検疫ウイルスによって感染させたメッセージを持つためにメール ポリシーを設定する必要があります。 この資料は添付ファイルとしてテスト ウイルスを模倣する EICAR (www.eicar.org) から提供される ASCII コードを使用します:

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

> **注:** EICAR ごと: *このテストファイルは「EICAR 標準アンチウィルス テストファイル」としてディストリビューションに EICAR に提供され、上記リストに記載されているすべての基準を満たします。 それはウイルスではない、でウイルス コードのフラグメントを含まれていませんので渡ることは安全。 ほとんどの製品はそれにそれがウイルス (しかし「EICAR AV テスト」のような明らかな名前と一般的にそれを、報告します) だったように反応します。*

Txtファイルを作成して下さい

上記の ASCII ストリングを使用する .txt ファイルを作成し、ファイルの本文として書かれているようにストリングを置いて下さい。 サンプル メッセージの添付ファイルとしてこのファイルを送信できます。

サンプル メッセージの送信

どのようににによってははたらくか、ESA さまざまな方法によってサンプル メッセージを送信できます。 2 つのメソッド例は**メール**を使用してまたは Outlook あります（または他の電子メールアプリケーション）から UNIX CLI によって。

UNIX CLI

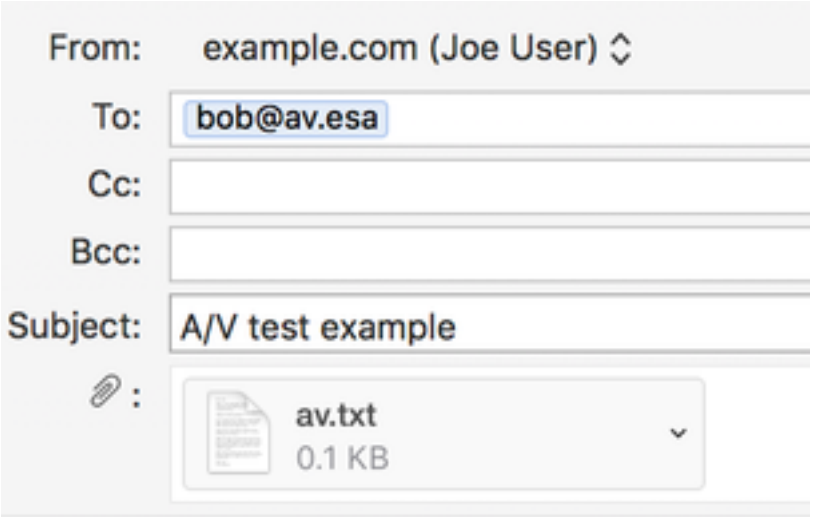
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt
bob@av.esa
```

UNIX環境は ESA によってメールを送信するか、または中継で送るためにきちんと設定される必要があります。

Outlook

Outlook（か別の電子メールアプリケーションを使用する）、ASCII コードを送信 することで 2 つの選択があります: 1） .txt 作成されたファイルを使用して、2） メール メッセージの本文の ASCII ストリングの貼り付けを指示して下さい。

添付ファイルとして .txt ファイルの使用:



TEST MESSAGE w/ ATTACHMENT

メール メッセージの本文の ASCII ストリングの使用:

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

Outlook（か他の電子メールアプリケーション）ESA によってメールを送信するか、または中継で送るためにきちんと設定される必要があります。

確認

ESA CLI で、サンプル メッセージを送信 する前にコマンド**末尾 mail_logs を**使用して下さい。メール ログを視聴している間見るメッセージは「ウイルス」として McAfee によってスキャンされ、つかまえられます:

```
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
```

同じメッセージは送信 し、Sophos によってスキャンしました:

```
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
```

このラボ ESA で、「ウイルスによって感染させるメッセージは「特定のメール ポリシーのメッセージに」適用される処理のために検疫するために設定されます。 ESA の操作はメール ポリシーのアンチウィルスによって処理されるウイルスによって感染させるメッセージのためにとられる処置に基づいて、変わるかもしれません。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems