Come inviare un messaggio di esempio per verificare che il motore antivirus stia eseguendo la scansione su un Cisco Email Security Appliance (ESA)

Sommario

Introduzione

In questo documento viene descritto come inviare un messaggio di esempio per verificare che il motore antivirus Sophos o McAfee stia eseguendo la scansione su una Cisco Email Security Appliance (ESA).

Come inviare un messaggio di esempio per verificare che il motore antivirus stia eseguendo la scansione su un Cisco Email Security Appliance (ESA)

Inviando un messaggio di esempio con un payload virale di test attraverso l'ESA, possiamo attivare il motore antivirus Sophos o McAfee. Prima di eseguire le operazioni elencate in questo documento, è necessario impostare i criteri di posta in arrivo o in uscita e configurare i criteri di posta in modo che i messaggi infetti da virus antivirus o di quarantena vengano eliminati. Questo documento utilizza il codice ASCII fornito da EICAR (www.eicar.org) che simula un virus di test come allegato:

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

> **Nota:** Per EICAR: *Questo file di prova è stato fornito all'EICAR per la distribuzione come "EICAR Standard Anti-Virus Test File" e soddisfa tutti i criteri elencati sopra. E 'sicuro per passare in giro, perché non è un virus e non include alcun frammento di codice virale. La maggior parte dei prodotti reagisce come se si trattasse di un virus (sebbene in genere lo riportino con un nome ovvio, come "EICAR-AV-Test").*

Creazione di un file TXT

Utilizzando la stringa ASCII precedente, create un file .txt e posizionate la stringa come corpo del file. Sarà possibile inviare questo file come allegato nel messaggio di esempio.

Invio messaggio di esempio

A seconda di come lavori, puoi inviare il messaggio di esempio attraverso l'ESA in vari modi. Due metodi di esempio sono tramite la CLI di UNIX che utilizza la **posta** o Outlook (o un'altra applicazione di posta elettronica).

CLI UNIX

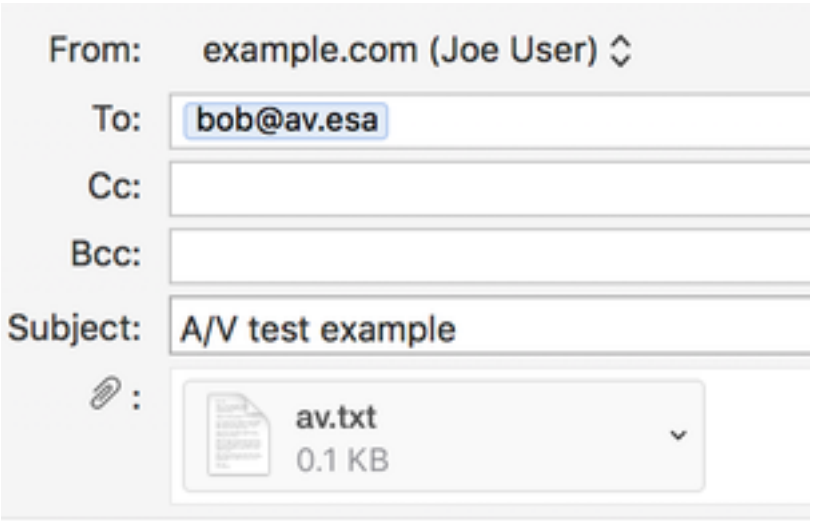
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt
bob@av.esa
```

L'ambiente UNIX dovrà essere configurato correttamente per l'invio o l'inoltro della posta attraverso l'ESA.

Outlook

Utilizzando Outlook (o un'altra applicazione di posta elettronica), è possibile inviare il codice ASCII in due modi: 1) utilizzando il file .txt creato, 2) incollare direttamente la stringa ASCII nel corpo del messaggio di posta.

Utilizzo del file txt come allegato:



TEST MESSAGE w/ ATTACHMENT

Utilizzando la stringa ASCII nel corpo del messaggio di posta:

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

Outlook (o un'altra applicazione di posta elettronica) dovrà essere configurato correttamente per l'invio o l'inoltro della posta attraverso l'ESA.

Verifica

Dalla CLI dell'ESA, usare il comando **tail mail_logs** prima di inviare il messaggio di esempio. Mentre si guarda il log di posta, si vede il messaggio viene analizzato e catturato da McAfee come "VIRAL":

```
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
```

Lo stesso messaggio inviato e analizzato da 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
```

In questa ESA lab, i 'Messaggi infetti da virus' sono configurati per essere messi in quarantena per l'"Azione applicata al messaggio" nella particolare policy di posta. L'azione sull'ESA può variare in base all'azione intrapresa per i messaggi con virus infetti gestiti da antivirus sulla policy di posta.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems