

Hoe een voorbeeldbericht te verzenden om ervoor te zorgen dat de anti-virusmotor wordt gescand op een Cisco e-mail security applicatie (ESA)

Inhoud

[Inleiding](#)

[Hoe een voorbeeldbericht te verzenden om ervoor te zorgen dat de anti-virusmotor wordt gescand op een Cisco e-mail security applicatie \(ESA\)](#)

[Een TXT-bestand maken](#)

[Bericht per monster verzenden](#)

[UNIX CLI](#)

[Outlook](#)

[Verificatie](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een voorbeeldbericht kunt verzenden om ervoor te zorgen dat ofwel de anti-viruscamera van Sfos of de anti-virusmotor van McAfee (McAfee) op een Cisco e-mail security applicatie (ESA) wordt gescand.

Hoe een voorbeeldbericht te verzenden om ervoor te zorgen dat de anti-virusmotor wordt gescand op een Cisco e-mail security applicatie (ESA)

Door een voorbeeldbericht te sturen met een testvirale lading door de ESA, kunnen we de Sofos of de McAfee antivirusmotor veroorzaken. Voordat u de stappen uitvoert die in dit document worden opgesomd, moet u uw inkomende of uitgaande Mail-beleid instellen en het postbeleid configureren om een met een virusdruppel of een quarantainevirus besmet bericht te hebben. In dit document wordt ASCII-code gebruikt die afkomstig is van EICAR (www.eicar.org) om een [testvirus](#) als bijlage te simuleren:

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Opmerking: Per EICAR: *Dit testbestand is aan EICAR verstrekt voor distributie als het "EICAR Standard Anti-Virus Test File" en het voldoet aan alle hierboven genoemde criteria. Het is veilig om door te geven, omdat het geen virus is en geen fragmenten van de virale code bevat. De meeste producten reageren erop alsof het een virus was (hoewel ze het doorgaans melden met een voor de hand liggende naam, zoals "EICAR-AV-Test").*

Een TXT-bestand maken

Gebruik de ASCII string hierboven, maak een .txt bestand en plaats de string zoals geschreven als de kern van het bestand. U kunt dit bestand als een bijlage in uw voorbeeldbericht verzenden.

Bericht per monster verzenden

Afhankelijk van de manier waarop u werkt, kunt u het voorbeeldbericht op verschillende manieren verzenden via het ESA. Twee voorbeeldmethoden zijn via UNIX CLI met behulp van de **post** of vanuit Outlook (of andere e-mailtoepassing).

UNIX CLI

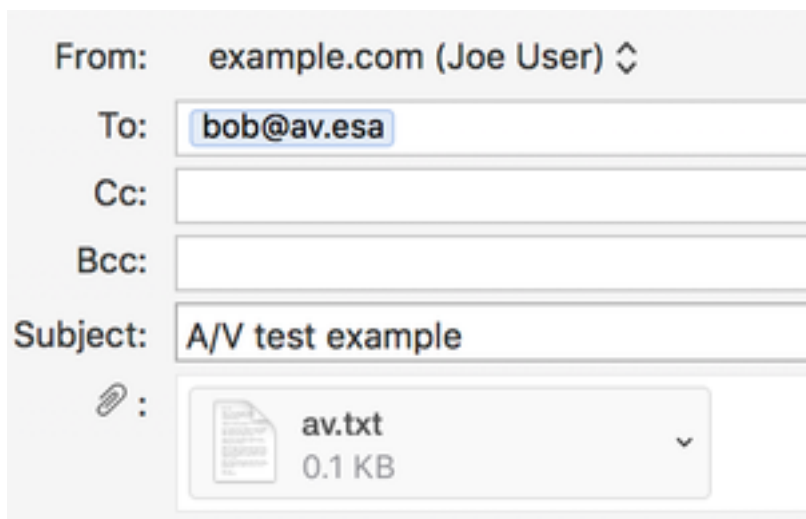
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt bob@av.esa
```

Uw UNIX-omgeving moet correct worden ingesteld om e-mail via uw ESA te verzenden of door te geven.

Outlook

Met behulp van Outlook (of een andere e-mailtoepassing) kunt u de ASCII-code op twee manieren verzenden: 1) het aanmaken .txt-bestand, 2) direct pasta van de ASCII-string in de inhoud van het e-mailbericht gebruiken.

Het .txt-bestand als een bijlage gebruiken:



The screenshot shows an email composition interface. The 'From' field is 'example.com (Joe User)'. The 'To' field is 'bob@av.esa'. The 'Cc' and 'Bcc' fields are empty. The 'Subject' field is 'A/V test example'. Below the subject field, there is an attachment icon (a paperclip) followed by a box containing a document icon, the filename 'av.txt', and the size '0.1 KB'.

TEST MESSAGE w/ ATTACHMENT

Gebruik van de ASCII-string in de inhoud van het e-mailbericht:

From: example.com (Joe User) ↕
To: bob@av.esa
Cc:
Bcc:
Subject: A/V test example

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

Uw Outlook (of andere e-mailtoepassing) dient correct te worden ingesteld om e-mail via uw ESA te verzenden of door te geven.

Verificatie

Gebruik in de ESA CLI de opdracht **tail mail_logs** voordat u het voorbeeldbericht verstuurt. Tijdens het zien van het maillogbestand ziet u dat het bericht gescand is en door McAfee als "VIRAL" is aangemerkt:

```
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
```

Het bericht werd doorgestuurd en gescand door SofS:

```
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 dit lab ESA, zijn 'Virus Infected Messages' zo ingesteld dat ze in quarantaine staan voor "Action Applied Message" op het betreffende postbeleid. De actie op uw ESA kan variëren, gebaseerd op de actie die is ondernomen voor virusgeïnfecteerde berichten die behandeld worden met het anti-virus op uw postbeleid.

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems](#)