Cómo enviar un mensaje de ejemplo para asegurar el motor antivirus está analizando en un dispositivo de seguridad del correo electrónico de Cisco (el ESA)

Contenido

Introducción

Este documento describe cómo enviar un mensaje de ejemplo para asegurarse que el contra virus de Sophos o el motor antivirus del McAfee está analizando en un dispositivo de seguridad del correo electrónico de Cisco (ESA).

Cómo enviar un mensaje de ejemplo para asegurar el motor antivirus está analizando en un dispositivo de seguridad del correo electrónico de Cisco (el ESA)

Enviando un mensaje de ejemplo con un payload viral de la prueba con el ESA, podemos accionar el motor antivirus de Sophos o del McAfee. Antes de realizar los pasos enumerados en este documento, usted necesitará configurar su directiva entrante o saliente del correo y configurar la directiva del correo para tener el descenso del contra virus o mensajes infectados virus de la cuarentena. Este documento utiliza el código ASCII proporcionado de EICAR (www.eicar.org) que simule un virus de la prueba como conexión:

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

> Nota: Por EICAR: *Estos archivos de prueba se han proporcionado a EICAR para la distribución como “los archivos de prueba estándar del contra virus EICAR”, y satisfacen todos los criterios enumerados arriba. Es seguro pasar alrededor, porque no es un virus, y no incluye ningunos fragmentos del código viral. La mayoría de los Productos reaccionan a él como si fuera un virus (lo señalan sin embargo típicamente con un nombre obvio, tal como “EICAR-AV-prueba”).*

Cree un archivo txt

Usando la cadena de ASCII arriba, cree un archivo de .txt y coloque la cadena según lo escrito como el cuerpo del archivo. Usted podrá enviar este archivo como conexión en su mensaje de ejemplo.

Envío del mensaje de ejemplo

Dependiendo de cómo usted trabaja, usted puede enviar el mensaje de ejemplo a través de las distintas maneras ESA. Dos métodos del ejemplo son vía UNIX CLI usando el **correo** o de la perspectiva (o de la otra aplicación de correo electrónico).

UNIX CLI

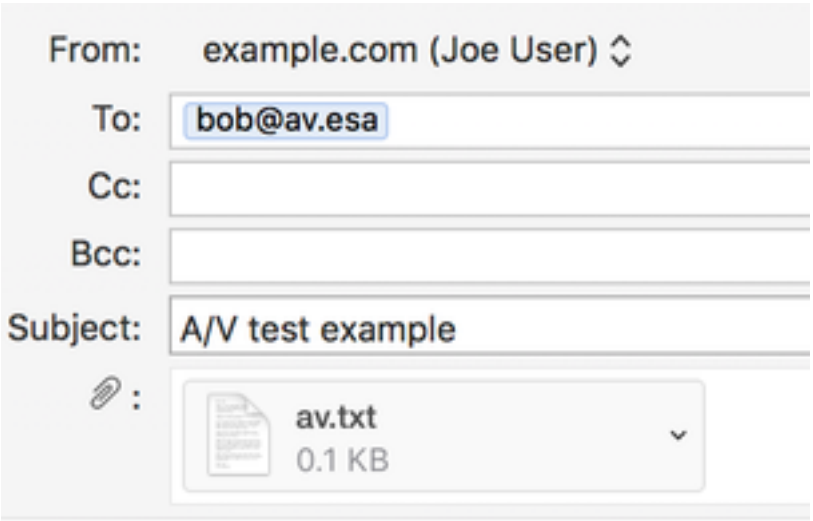
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt
bob@av.esa
```

Su entorno de Unix necesitará ser puesto correctamente para enviar o para retransmitir el correo con su ESA.

Perspectiva

Usando la perspectiva (u otra aplicación de correo electrónico), usted tiene dos opciones en el envío del código ASCII a través: 1) usando el archivo creado de .txt, 2) goma directa de la cadena de ASCII en el cuerpo del mensaje del correo.

Usando el archivo de .txt como conexión:



TEST MESSAGE w/ ATTACHMENT

Usando la cadena de ASCII en el cuerpo del mensaje del correo:

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

La su perspectiva (o la otra aplicación de correo electrónico) necesitará ser puesta correctamente para enviar o para retransmitir el correo con su ESA.

Verificación

En el ESA CLI, utilice los **mail_logs del** comando tail antes de enviar el mensaje de ejemplo. Mientras que mira el correo registrarle verá el mensaje es analizado y cogido por el McAfee como “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
```

El mismo mensaje enviado a través y analizado por 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
```

En este laboratorio ESA, “los mensajes infectados virus” se configuran para quarantine para la “acción aplicada al mensaje” en la directiva determinada del correo. La acción en su ESA puede variar, sobre la base del acción realizada para los mensajes infectados virus manejados por el contra virus en su directiva del correo.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems