Como enviar um exemplo de mensagem para assegurar o motor anti-vírus está fazendo a varredura em uma ferramenta de segurança do email de Cisco (o ESA)

Índice

Introdução

Este documento descreve como enviar um exemplo de mensagem para assegurar-se de que Sophos anti-vírus ou motor anti-vírus da McAfee esteja fazendo a varredura em uma ferramenta de segurança do email de Cisco (ESA).

Como enviar um exemplo de mensagem para assegurar o motor anti-vírus está fazendo a varredura em uma ferramenta de segurança do email de Cisco (o ESA)

Enviando um exemplo de mensagem com um payload viral do teste com o ESA, nós podemos provocar o motor anti-vírus de Sophos ou da McAfee. Antes de executar as etapas alistadas neste documento, você precisará de estabelecer sua política entrante ou que parte do correio e de configurar a política do correio para ter mensagens contaminadas vírus anti-vírus da gota ou da quarentena. Este documento usa o código ASCII fornecido de EICAR (www.eicar.org) que simulará um vírus do teste como um acessório:

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

> **Note**: Por EICAR: *Este arquivo de teste foi fornecido a EICAR para a distribuição como "o arquivo de teste anti-vírus padrão EICAR", e satisfaz todos os critérios alistados acima. É seguro passar ao redor, porque não é um vírus, e não inclui nenhuns fragmentos do código viral. A maioria de Produtos reage-lhe como se era um vírus (embora o relata tipicamente com um nome óbvio, tal como o "EICAR-AV-teste").*

Crie um arquivo txt

Usando o string ascii acima, crie um arquivo de .txt e coloque a corda como escrito como o corpo do arquivo. Você poderá enviar este arquivo como um acessório em seu exemplo de mensagem.

Enviando o exemplo de mensagem

Segundo como você trabalha, você pode enviar o exemplo de mensagem com as várias maneiras ESA. Dois métodos do exemplo são através de UNIX CLI usando o **correio** ou da probabilidade (ou do outro aplicativo de e-mail).

UNIX CLI

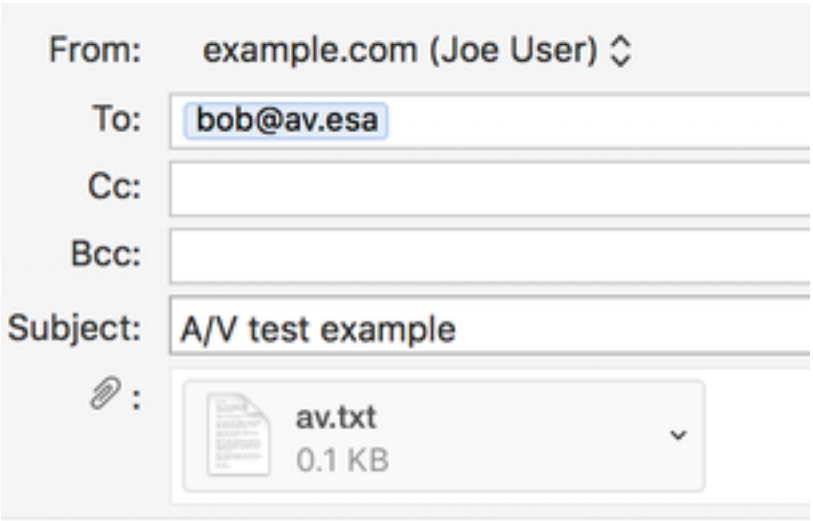
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt
bob@av.esa
```

Seu ambiente UNIX deverá ser setup corretamente para enviar ou retransmitir o correio com seu ESA.

Probabilidade

Usando a probabilidade (ou um outro aplicativo de e-mail), você tem duas escolhas em enviar o código ASCII completamente: 1) que usa o arquivo criado de .txt,) pasta 2 direta do string ascii no corpo da mensagem do correio.

Usando o arquivo de .txt como um acessório:



TEST MESSAGE w/ ATTACHMENT

Usando o string ascii no corpo da mensagem do correio:


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

Sua probabilidade (ou o outro aplicativo de e-mail) deverão ser setup corretamente para enviar ou retransmitir o correio com seu ESA.

Verificação

No ESA CLI, use os **mail_logs do** comando tail antes de enviar o exemplo de mensagem. Ao olhar o correio o registrar verá a mensagem é feita a varredura e travada pela 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
```

A mesma mensagem enviada completamente e feita a varredura 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
```

Neste laboratório ESA, “as mensagens contaminadas vírus” são configuradas para quarantine para a “ação aplicada à mensagem” na política particular do correio. A ação em seu ESA pode variar, com base na ação tomada para as mensagens contaminadas vírus seguradas por anti-vírus em sua política do correio.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems