Detecte los correos electrónicos del spoofed en el ESA y cree las excepciones para los remitentes que se permiten al spoof

Contenido

Introducción

Este documento describe cómo controlar el spoofing del email en el dispositivo de seguridad del email de Cisco (ESA) y cómo crear las excepciones para los usuarios permitidos enviar los email del spoofed.

Prerequisites

Requisitos

Su ESA debe procesar los correos entrantes y salientes, y debe utilizar una configuración estándar de RELAYLIST para señalar los mensajes por medio de una bandera como salientes.

Componentes Utilizados

La información en este documento se basa en el ESA con cualquier versión de AsyncOS. La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Los componentes específicos usados incluyen:

- Diccionario: utilizado para salvar todos sus dominios internos.
- Filtro del mensaje: utilizado para manejar la lógica de detectar el correo electrónico del spoofed y de insertar una encabezado en la cual los filtros contentos pueden actuar.
- Cuarentena de la directiva: utilizado para salvar los duplicartes de los correos electrónicos del spoofed temporalmente. Considere agregar el IP Address de los mensajes liberados al MY_TRUSTED_SPOOF_HOSTS para prevenir los mensajes futuros de este remitente de ingresar la cuarentena de la directiva.
- MY_TRUSTED_SPOOF_HOSTS: enumere para referirse a sus IP Addresses de envío de confianza. Agregar una dirección IP de un remitente a esta lista saltará la cuarentena y permitirá el remitente al spoof. Estamos colocando los remitentes de confianza en su grupo del remitente MY_TRUSTED_SPOOF_HOSTS para no quarantined los mensajes del spoofed de estos remitentes.
- RELAYLIST: enumere para los IP Addresses de autenticidad que se permite retransmitir, o envíe el correo electrónico saliente. Si el correo electrónico se está entregando vía este grupo del remitente la suposición es que el mensaje no es un mensaje del spoofed.

  Note: Si el grupo del remitente se llama algo diferente que MY_TRUSTED_SPOOF_HOSTS o RELAYLIST, usted tendrá que modificar el filtro con el nombre del grupo correspondiente del remitente. También, si usted tiene los módulos de escucha múltiples, usted puede también tener más de un MY_TRUSTED_SPOOF_HOSTS.

Antecedentes

El spoofing se habilita por abandono en el Cisco ESA. Hay varios, las razones válidas para permitir que otros dominios envíen encendido su favor. Un ejemplo común, administrador ESA puede querer al spoofed que controla los correos electrónicos quarantining los mensajes del spoofed antes de que se entreguen.

Para tomar medidas específicas tales como cuarentena en el correo electrónico del spoofed, usted debe primero detectar el correo electrónico del spoofed.

¿Cuál es spoofing del email?

El spoofing del email es la falsificación de una encabezado del email de modo que el mensaje aparezca haber originado alguien o en alguna parte con excepción de la fuente real. El spoofing del email es una táctica usada en phishing y las campañas del Spam porque la gente es más probable abrir un email cuando ella lo piensa han sido enviadas por una fuente legítima.

¿Cómo detectar el correo electrónico del spoofed?

Usted querrá filtrar cualquier mensaje que tenga un remitente del sobre (Correo-de) y “cómodo” (de) de la encabezado que contiene uno de sus propios dominios entrantes en la dirección de correo electrónico.

¿Cómo permitir el spoofing para los remitentes específicos?

Al implementar el filtro del mensaje proporcionado dentro de este artículo, los mensajes del spoofed se marcan con etiqueta con una encabezado, y el filtro contento se utiliza para tomar medidas en la encabezado. Para agregar una excepción, agregue simplemente el IP del remitente

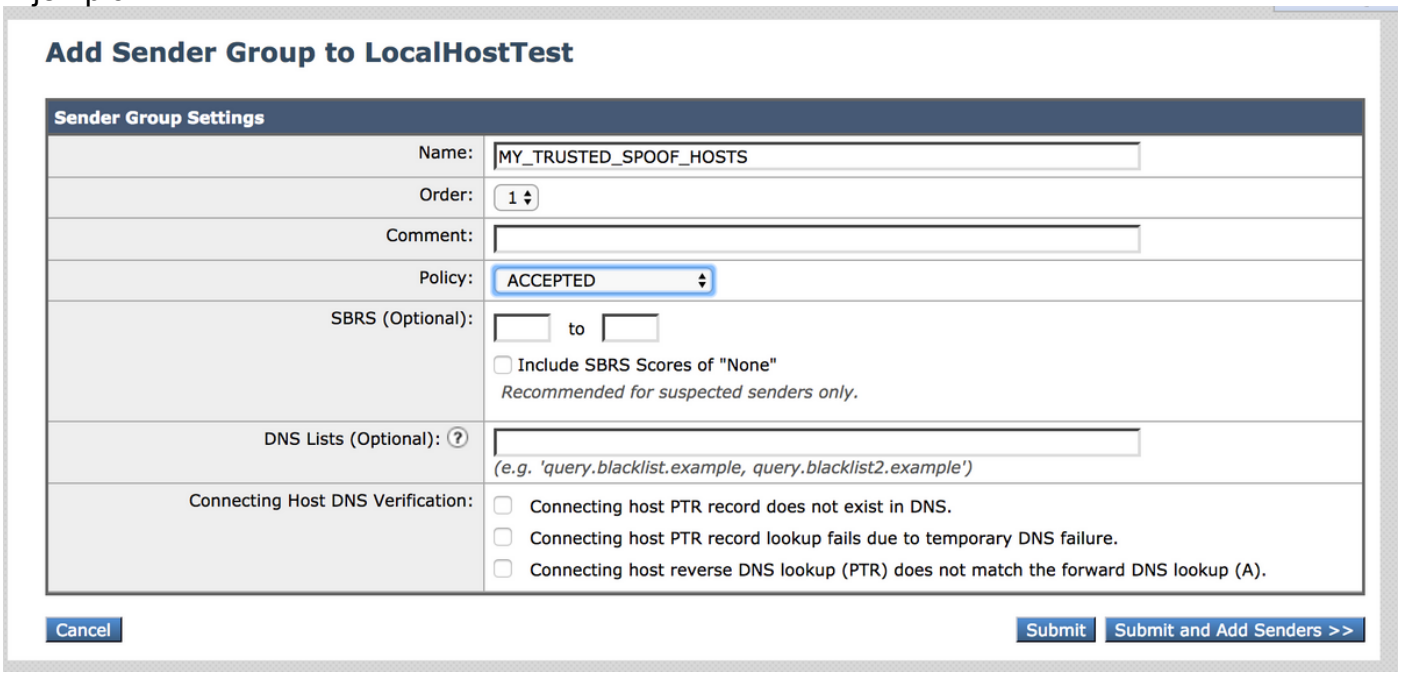
a MY_TRUSTED_SPOOF_HOSTS.

Configurar

Cree un Sendergroup

1. Del ESA GUI, navegue **para enviar las directivas > la descripción del SOMBRERO**
2. Haga clic en Add (Agregar).
3. En el campo “Nombre” especifique **MY_TRUSTED_SPOOF_HOSTS**
4. En el campo de la “orden” especifique **1**
5. Para el campo de la “directiva”, especifique **VALIDADO**
6. El tecleo **somete** para salvar los cambios.
7. Finalmente, el **cometer del** tecleo **cambia** para salvar la configuración

Ejemplo:

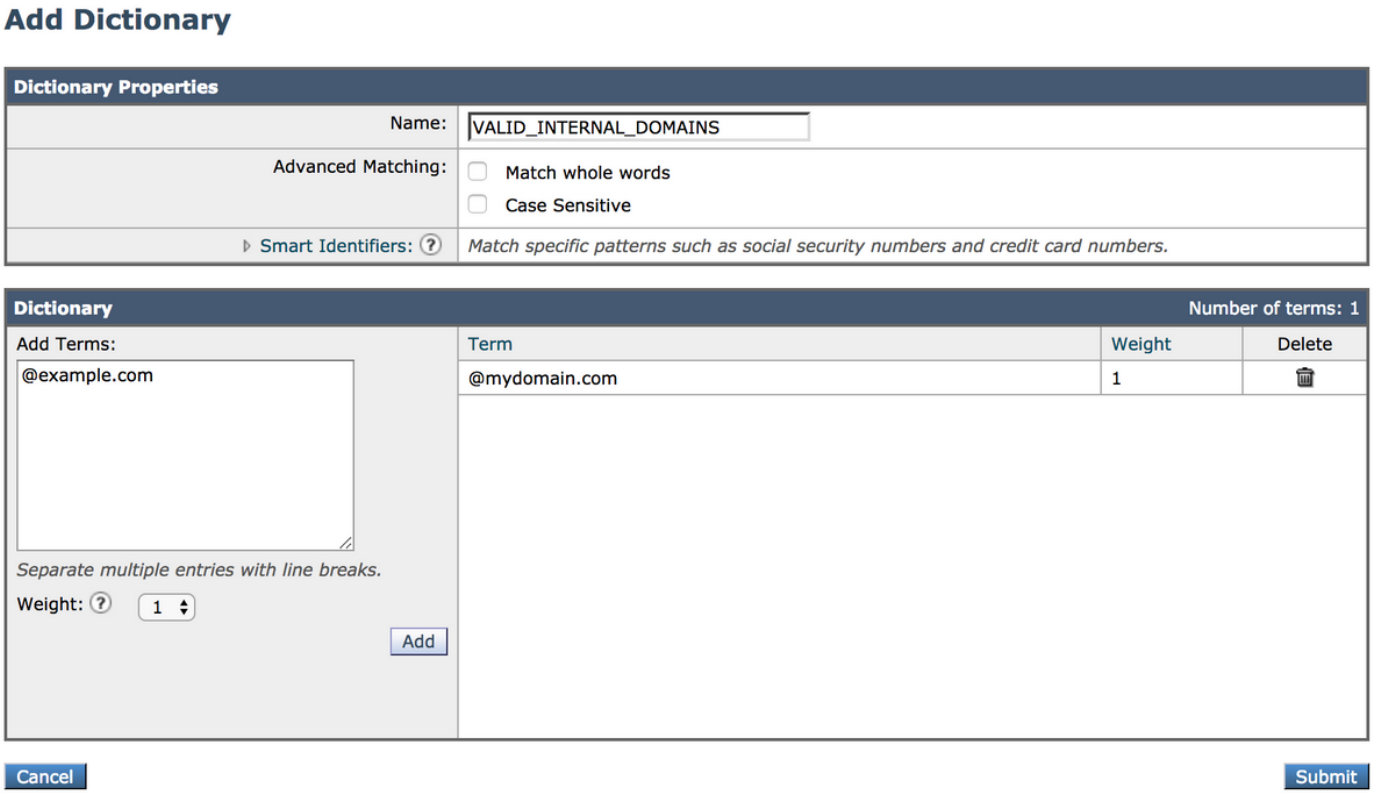


Cree un diccionario

Cree un diccionario para todos los dominios que usted quiera para inhabilitar el spoofing para en el ESA:

1. Del ESA GUI, navegue **para enviar las directivas > los diccionarios.**
2. El tecleo **agrega el diccionario.**
3. En el campo “Nombre” especifique “VALID_INTERNAL_DOMAINS”, para hacer el copiado y pegar del filtro del mensaje sin error.
4. Bajo “agregue los términos”, agregan todos los dominios que usted quiera para detectar el spoofing. Ingrese el dominio con @ una muestra prepending el dominio y el tecleo agrega.
5. Asegúrese que “el checkbox de las palabras enteras de la coincidencia” esté desmarcado.
6. El tecleo **somete** para salvar los cambios del diccionario.
7. Finalmente, el **cometer del** tecleo **cambia** para salvar la configuración

Ejemplo:



Cree un filtro del mensaje

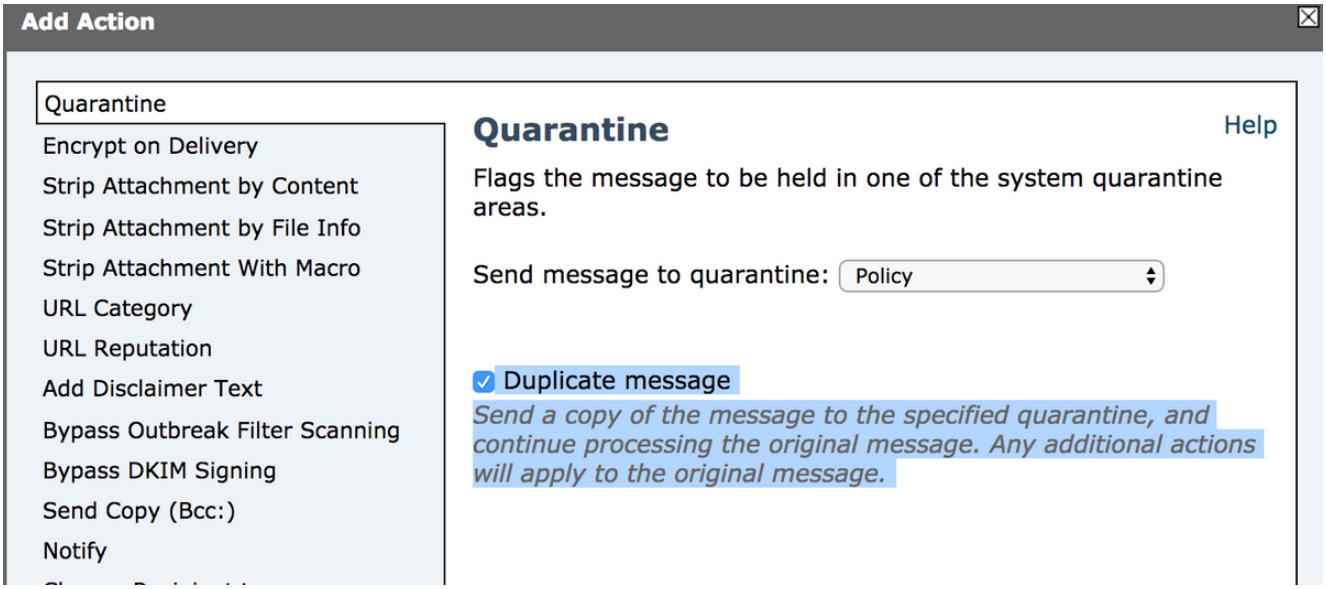
Después, usted necesitará crear un filtro del mensaje para leverage el diccionario apenas creado, “VALID_INTERNAL_DOMAINS”:

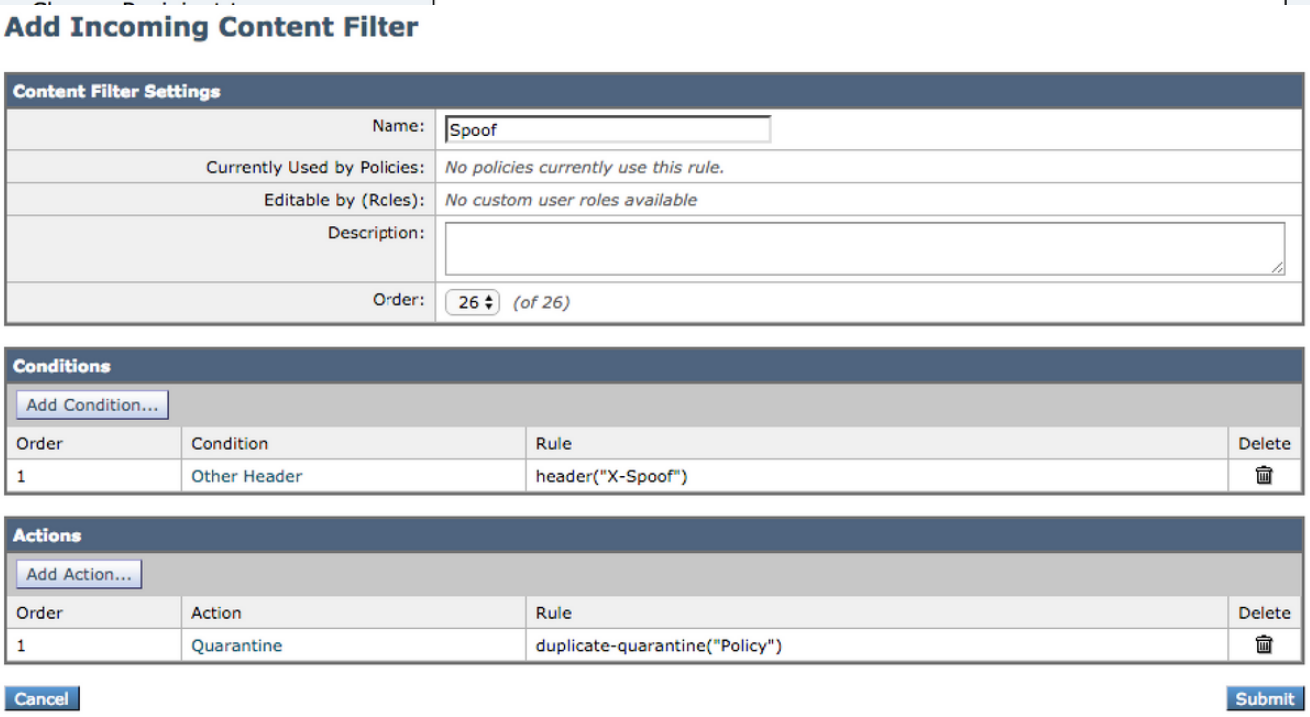
1. Conecte con el comando line interface(cli) del ESA.
2. Funcione con los **filtros del** comando.
3. Funcione con el comando new **de crear un nuevo filtro del mensaje.**
4. La copia y pega el ejemplo siguiente del filtro, haciendo edita para sus nombres del grupo reales del remitente si es necesario:

```
mark_spoofed_messages:
if(
(mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
OR (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
AND ((sendergroup != "RELAYLIST")
AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
)
{
insert-header("X-Spoof", "");
}
```

5. Vuelva al prompt principal CLI y ejecute el **cometer** para salvar la configuración.
6. Navegue al GUI > las directivas del correo > los filtros contentos entrantes
7. Cree el filtro contento entrante que toma medidas en el X-spoof de la encabezado del spoof: Agregue la acción: duplicado-cuarentena (“directiva ").

Note: La característica duplicado del mensaje mostrada aquí guardará una copia del mensaje, y continúa enviando el mensaje original al beneficiario.





8. Conecte el filtro contento a las directivas del correo entrante en GUI > las directivas del correo entrante de Policies> del correo
9. Someta y confíe los cambios

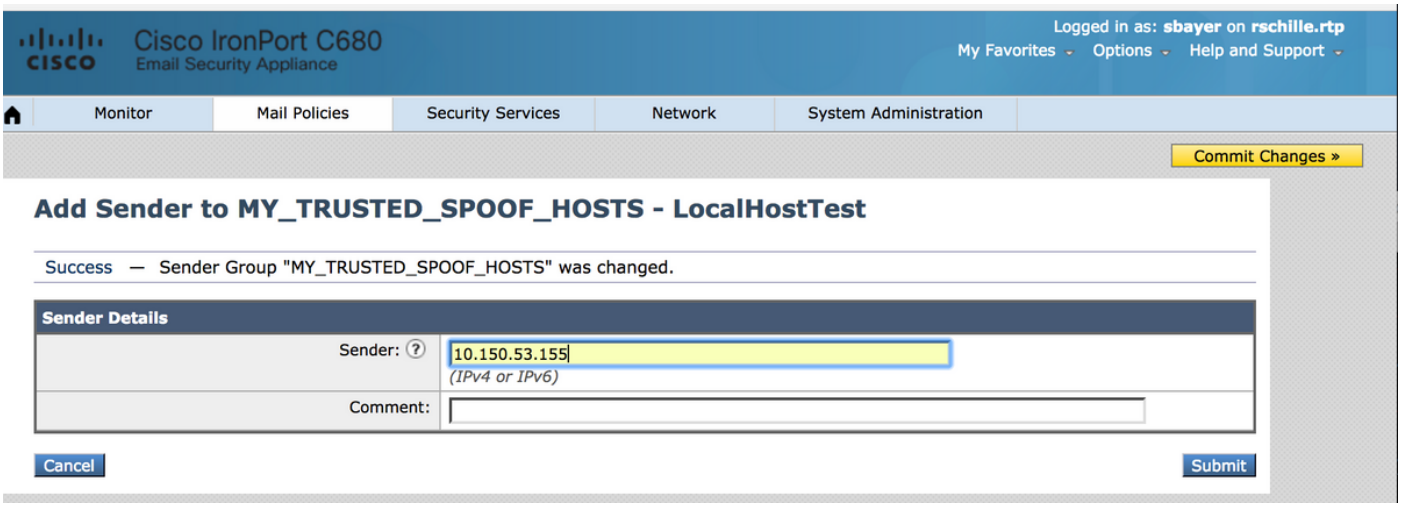
Agregue las Spoof-excepciones a MY_TRUSTED_SPOOF_HOSTS

Finalmente, usted necesitará agregar las spoof-excepciones (los IP Addresses o los nombres de host) al sendergroup MY_TRUSTED_SPOOF_HOSTS.

1. Navegue vía la red GUI: **Envíe las directivas > la descripción del SOMBRERO**
2. Haga clic y abra el grupo del remitente MY_TRUSTED_SPOOF_HOSTS.
3. Haga clic en “agregan el remitente…” para agregar una dirección IP, un rango, un nombre del host, o un nombre del host parcial.

4. El tecleo **somete** para salvar los cambios del remitente.
5. Finalmente, el **cometer del** tecleo **cambia** para salvar la configuración.

Ejemplo:



Verificación

Verifique los mensajes del spoofed Quarantined

Envíe un mensaje de prueba que especifica uno de sus dominios como el remitente del sobre. Valide el filtro está trabajando como se esperaba realizando una pista del mensaje en ese mensaje. El resultado esperado es que el mensaje conseguirá quarantined porque no hemos creado ninguna excepciones con todo para esos remitentes se permite que al spoof.

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <test_user@domain.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user_1@example.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative
Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message
filter:quarantine_spoofed_messages)
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

Verifique los mensajes de la Spoof-excepción se están entregando

Los remitentes de la “Spoof-excepción” son IP Addresses en sus grupos del remitente referidos al filtro arriba.

Se refiere RELAYLIST porque es utilizado por el ESA para enviar el correo saliente. Los mensajes que son enviados por RELAYLIST son correo típicamente saliente, y no incluyendo esto crearían los falsos positivos, o los mensajes de salida quarantined por el filtro arriba.

Seguimiento de mensajes ejemplo de una dirección IP de la “Spoof-excepción” que fue agregada a MY_TRUSTED_SPOOF_HOSTS. La acción prevista es entrega y no quarantine. (Este IP se permite al spoof).

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user_1@example.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <test_user@domain.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user_1@example.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598 Message accepted
for delivery'
Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done
```

Información Relacionada

- Filtración del correo del spoofed ESA
- Protección del spoof usando la verificación del remitente