Orden de la cuarentena ESA/CES cuando es señalado por medio de una bandera por los servicios múltiples

Contenido

Introducción

Este documento describe el comportamiento de los dispositivos de la Seguridad del correo electrónico del dispositivo de seguridad (ESA) y de la nube del correo electrónico de Cisco (CES) cuando un correo electrónico es señalado por medio de una bandera por los servicios múltiples para quarantining y el flujo FO el correo electrónico con el resto de la tubería del correo electrónico.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en Cisco ESA con la versión de AsyncOS 12.1.0.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los correos electrónicos que atraviesa Cisco ESA y dispositivos CES para filtrar siguen la tubería de la cola de trabajo del correo electrónico. La tubería es estática y si hay acciones múltiples de los servicios múltiples definidos para señalar un correo electrónico por medio de una bandera para las cuarentenas, no sigue la orden según la tubería; en lugar, el ESA/CES quarantines la con

su propia orden.

> Nota: Los correos electrónicos a los cuales se señalan por medio de una bandera con las acciones fijadas (última acción) tomarán la precedencia inmediata y salen el proceso de la cola de trabajo.

¿Qué sucede al correo electrónico cuando es señalada por medio de una bandera por los servicios múltiples para la cuarentena?

El correo electrónico se da prioridad en la cuarentena del brote de virus de la directiva (PVO) primero. No hay orden concreto el cual la cuarentena de la directiva él entra mientras que el PVO enumera cada otra cuarentena que el correo electrónico también se sostiene adentro. Después de que el correo electrónico se libere fuera de una de las cuarentenas PVO, se sostiene en cualquier cuarentena respectiva que se señalará por medio de una bandera adentro.

Después de que el email fuera liberado (manualmente o a través del temporizador donde se fija la acción predeterminada para liberar) los email después ingresan la cuarentena del Spam. Cuando el correo electrónico se libera de la cuarentena del Spam, los transverses en la salida hace cola para la salida final después de eso.

> Nota: Un correo electrónico que se borra de una cuarentena PVO, quitará el correo electrónico de todo el subsiguiente quarantines lo se ha sostenido adentro también.

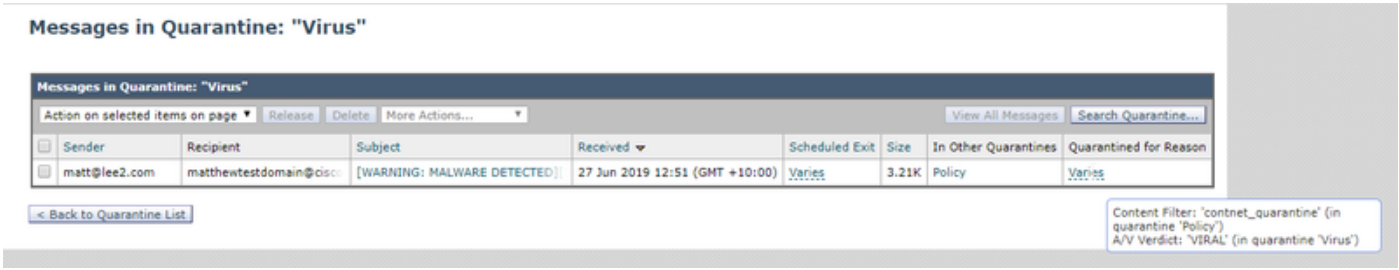
- Los mensajes liberados de las cuarentenas de la directiva y del virus son pre-explorados por los contras virus, la protección avanzada del malware, y los motores del graymail.
- Los mensajes liberados de la cuarentena del brote son pre-explorados por el anti-Spam, los contras virus, y los motores AMP.
- Los mensajes liberados de la cuarentena del análisis del archivo se pre-exploran para las amenazas.
- Los mensajes con las conexiones son pre-explorados por el servicio de la reputación del archivo sobre la versión de las cuarentenas de la directiva, del virus, y del brote.

Inyección inicial del correo electrónico con la filtración hecha por el ESA. En esta salida usted ve que es señalada por medio de una bandera por la cuarentena del Spam, la cuarentena del virus, y la cuarentena de la directiva:

```
Thu Jun 27 12:51:03 2019 Info: Start MID 378951 ICID 391696
Thu Jun 27 12:51:03 2019 Info: MID 378951 ICID 391696 From: <matt@lee2.com>
Thu Jun 27 12:51:10 2019 Info: MID 378951 ICID 391696 RID 0 To: <matthewtestdomain@cisco.com>
Thu Jun 27 12:51:14 2019 Info: MID 378951 Subject 'Test email with AV EICAR and other triggers'
Thu Jun 27 12:51:15 2019 Info: MID 378951 ready 3292 bytes from <matt@lee2.com>
Thu Jun 27 12:51:15 2019 Info: MID 378951 matched all recipients for per-recipient policy matt
in the inbound table
Thu Jun 27 12:51:15 2019 Info: MID 378951 interim verdict using engine: CASE spam positive
Thu Jun 27 12:51:15 2019 Info: MID 378951 using engine: CASE spam positive
Thu Jun 27 12:51:15 2019 Info: ISQ: Tagging MID 378951 for quarantine
Thu Jun 27 12:51:15 2019 Info: MID 378951 interim AV verdict using Sophos VIRAL
Thu Jun 27 12:51:15 2019 Info: MID 378951 antivirus positive 'EICAR-AV-Test'
Thu Jun 27 12:51:15 2019 Info: MID 378951 AMP file reputation verdict : MALWARE
```

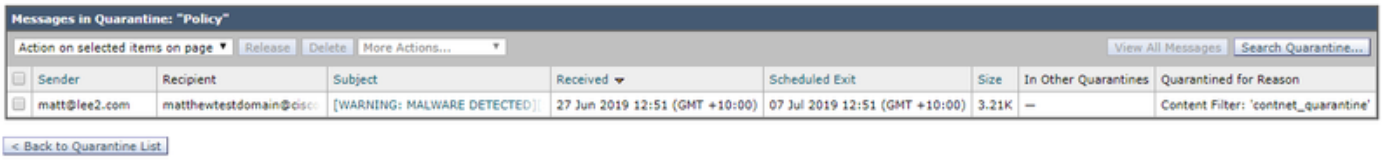
```
Thu Jun 27 12:51:15 2019 Info: MID 378951 attachment 'testAV.txt'
Thu Jun 27 12:51:15 2019 Info: MID 378951 URL https://ihaveabadreputation.com has reputation -
9.3 matched Condition: URL Reputation Rule
Thu Jun 27 12:51:15 2019 Info: MID 378951 Custom Log Entry:  - Match whole word filter
Thu Jun 27 12:51:15 2019 Info: ISQ: Tagging MID 378951 for quarantine (X-Ironport-Quarantine)
Thu Jun 27 12:51:15 2019 Info: MID 378951 quarantined to "Policy" (content
filter:contnet_quarantine)
Thu Jun 27 12:51:15 2019 Info: MID 378951 quarantined to "Virus" (a/v verdict:VIRAL)
Thu Jun 27 12:51:15 2019 Info: Message finished MID 378951 done
Thu Jun 27 12:51:15 2019 Info: ICID 391696 close
```

Investigado una vez dentro de la cuarentena, del correo electrónico sostenido en la cuarentena PVO que usted marcó se ve, así como de cualquier otras cuarentenas señala por medio de una bandera para estar adentro.



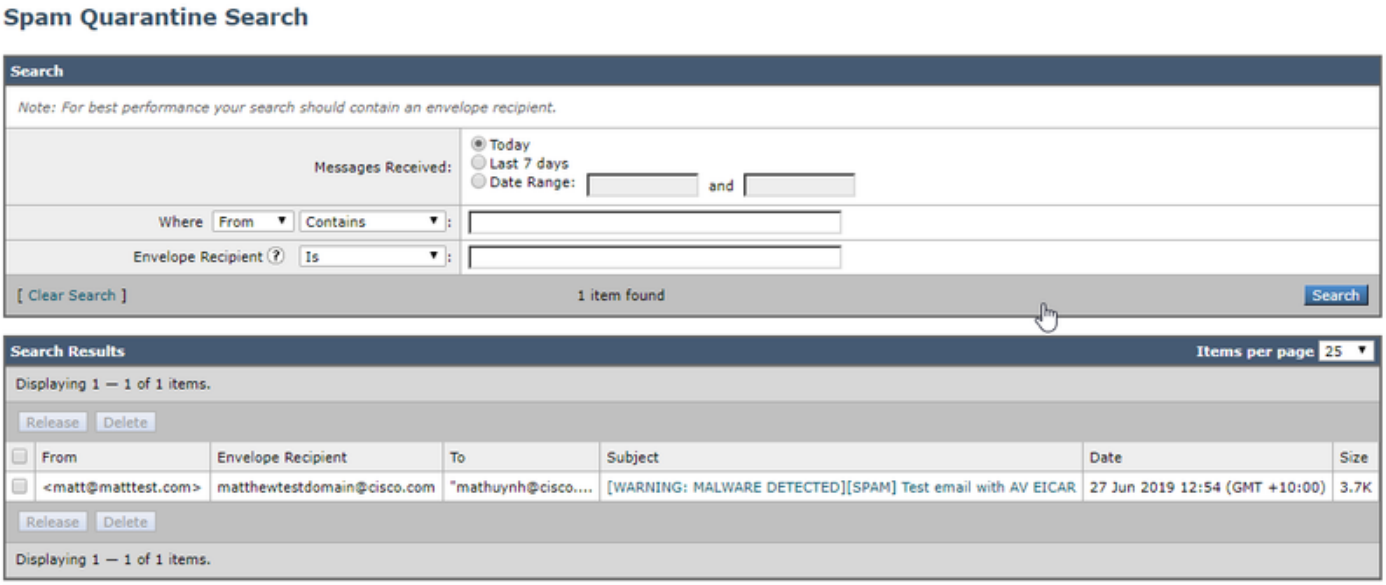
Después de que libere de esta cuarentena, registra este evento en sus **mail_logs** y refleja en las otras cuarentenas también que está no más disponible en la otra cuarentena.

```
Thu Jun 27 12:52:59 2019 Info: MID 378951 released from quarantine "Virus" (manual) t=104
```



Liberela la cuarentena de los PVO que sigue habiendo permite que los correos electrónicos viajen a la cuarentena señalada por medio de una bandera del Spam después de eso.

```
Thu Jun 27 12:54:15 2019 Info: MID 378951 released from quarantine "Policy" (manual) t=180
Thu Jun 27 12:54:15 2019 Info: MID 378951 released from all quarantines
Thu Jun 27 12:54:15 2019 Info: MID 378951 matched all recipients for per-recipient policy matt
in the inbound table
Thu Jun 27 12:54:15 2019 Info: MID 378951 interim AV verdict using Sophos VIRAL
Thu Jun 27 12:54:15 2019 Info: MID 378951 antivirus positive 'EICAR-AV-Test'
Thu Jun 27 12:54:15 2019 Info: MID 378951 AMP file reputation verdict : MALWARE
Thu Jun 27 12:54:15 2019 Info: ISQ: Tagging MID 378951 for quarantine (X-Ironport-Quarantine)
Thu Jun 27 12:54:15 2019 Info: MID 378951 queued for delivery
Thu Jun 27 12:54:15 2019 Info: RPC Delivery start RCID 13914 MID 378951 to local IronPort Spam
Quarantine
Thu Jun 27 12:54:15 2019 Info: ISQ: Quarantined MID 378951
Thu Jun 27 12:54:15 2019 Info: RPC Message done RCID 13914 MID 378951
Thu Jun 27 12:54:15 2019 Info: Message finished MID 378951 done
```



Allí en la versión final de la cuarentena del Spam, el correo electrónico es destinado para la cola de la salida.

```
Thu Jun 27 12:55:33 2019 Info: Start MID 378952 ICID 0 (ISQ Released Message)
Thu Jun 27 12:55:33 2019 Info: ISQ: Reinjected MID 378951 as MID 378952
Thu Jun 27 12:55:33 2019 Info: MID 378952 ICID 0 From: <matt@lee2.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 ICID 0 RID 0 To: <matthewtestdomain@cisco.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 Subject '[WARNING: MALWARE DETECTED][SPAM] Test email
with AV EICAR'
Thu Jun 27 12:55:33 2019 Info: MID 378952 ready 9661 bytes from <matt@lee2.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 queued for delivery
```

Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems