Determinación de la disposición del mensaje ESA

Contenido

Introducción

Este documento describe cómo determinar la disposición de un mensaje con los registros del correo extraídos de los diversos comandos en el dispositivo de seguridad del email de Cisco (ESA).

Prerequisites

La información en este documento se basa encendido:

- ESA
- Todas las versiones de AsyncOS

Seguimiento de mensajes

Si usted ejecuta AsyncOS para la versión 6.0 o posterior del email, la mayoría de la manera eficaz de determinar qué sucedió a un mensaje particular es utilizar Seguimiento de mensajes la página de la lengueta del monitor. Esto permite que usted busque con una variedad de opciones en una interfaz Web fácil de usar.

Si usted funciona con una versión anterior o necesita recolectar todas las líneas del registro para los propósitos de Troubleshooting, utilice el **grep** o los comandos **findevent** como se detalla en las siguientes secciones.

Comando de Findevent

Si usted tiene AsyncOS para la versión 5.1.2 o posterior del correo electrónico, el comando **findevent** CLI hace más simple buscar para un mensaje específico. **Findevent** le deja buscar por el sobre de, el beneficiario del sobre, o el tema del mensaje. Esto se puede hacer sin importar el

caso también. Una vez que usted encuentra su mensaje, usted puede volver cada línea del registro relevante a ese mensaje. Si usted ejecuta **findevent** sin los argumentos, inicia a un Asisitente para dirigirle con el proceso. Como siempre, usted puede utilizar el **comando help** para aprender la forma corta:

```
> help findevent
findevent [-i] [-f from | -s subject | -t to] log_name
findevent -m mid log_name
```

La primera forma conduce una búsqueda para un sobre de, un tema, o un sobre específico dentro del log_name Nombrado y enumera los ID del mensaje (MIDs) esa coincidencia. - El indicador i se puede utilizar para las búsquedas NON-caso-sensibles.

La segunda forma visualiza todas las líneas del registro para el MEDIADOS DE dado.

Si usted tiene una versión anterior, el **comando grep** CLI puede ser utilizado para lograr la misma cosa. Sin embargo, el uso del **comando grep** requiere un conocimiento más detallado de cómo los eventos del mensaje del registro ESA.

Comando grep

El primer desafío cuando usted busca los registros del correo es encontrar su mensaje. Usted puede hacer esto si usted busca para el remitente, el beneficiario, o para el tema. Una vez que usted ha encontrado su mensaje, es importante entender cómo se ordenan los registros del correo. Los eventos contentos del registro del correo de la Seguridad se dan las siglas. Los eventos más importantes son ICID, MEDIADOS DE, LIBRAN, y DCID.

ID de conexión de la inyección (ICID): Cuando un host remoto establece una conexión al dispositivo, esa conexión se asigna un ICID. Un ICID puede spawn/generar mucho el MIDs.

> **Note**: **ICID 0** define un mensaje que fue inyectado de sí mismo. De hecho, el número 0 después de que un ICID o un DCID refiera a las sesiones abiertas a o desde el direccionamiento del local loop del dispositivo.

MEDIADOS DE: Una vez que se establece una conexión, cada **correo** acertado del Simple Mail Transfer Protocol (SMTP) **de:** el comando crea un nuevo MEDIADOS DE. Una sola MEDIADOS DE freza de la poder muchos RID.

Beneficiario ID (LIBRADO): Cada beneficiario (a: Cc: o Bcc consigue LIBRADO. Los RID spawn/generan solamente DCIDs múltiple si hay una despedida suave (error de conexión) y se reintenta la salida.

ID de conexión de la salida (DCID): Cada beneficiario que va al mismo dominio del destino recibe el mismo DCID hasta los límites del sistema receptor. Tan si los receipients del los mensajes todos van al mismo dominio, después hay un DCID para todos los RID. Si en lugar de otro, cada uno LIBRADA va a un dominio separado, después hay una correlación de uno a uno.

> **Note**: **DCID 0** define un mensaje que nunca fue enviado. De hecho, el número 0 después de que un ICID o un DCID refiera a las sesiones abiertas a o desde el direccionamiento del local loop del dispositivo.

Generalmente, cuando usted encuentra su mensaje, usted encuentra su MEDIADOS DE. Entonces usted grep para el MEDIADOS DE y determina el ICID y LO LIBRA. Con el ICID, usted puede determinar la cuenta de la reputación de SenderBase (SBR) para el remitente. Con HABER LIBRADO y entonces el DCID, usted puede determinar qué sucedió cuando el ESA intentó la salida.

> **Note**: Una vez que usted tiene el MEDIADOS DE, ICID, y DCID, usted puede extraer todas las filas para ese mensaje en un **grep**, si el origen del mensaje no es más viejo que su registro más viejo del correo.

```
example.com> grep -e " MID 11123" -e " ICID 11092" -e " DCID 23349" mail_logs
```

Ejemplo:

1. Búsqueda para el tema del mensaje:

```
example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> test
Do you want this search to be case insensitive? [Y]>
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Mon Jan 23 10:25:03 2006 Info: SMTP listener testpairlist starting
Tue Jan 24 12:10:15 2006 Info: Message aborted MID 8 Dropped by filter
'testdrop'
Tue Jan 31 23:55:38 2006 Info: MID 32 Subject 'testmsgquarantine'
Wed Feb 1 00:23:59 2006 Info: MID 62 Subject 'testmsgquarantine'
Wed Feb 1 00:27:48 2006 Info: MID 64 Subject 'testmsg2'
Wed Feb 1 22:30:37 2006 Info: MID 80 Subject 'test zip'
Wed Feb 1 22:37:51 2006 Info: MID 83 Subject 'FW: test zip'
Wed Feb 1 22:41:50 2006 Info: MID 84 Subject 'FW: test zip'
Fri Feb 3 15:17:47 2006 Info: MID 94 Subject 'test'
Fri Feb 3 15:42:06 2006 Info: MID 96 Subject 'test'
```

Esto generó varias coincidencias que contuvieron la **prueba** en el tema. El mensaje fue enviado en aproximadamente 3:42pm, así que usted puede utilizar eso MEDIADOS DE para la búsqueda siguiente.

Aquí están algunas puntas impotant a observar sobre las preguntas:

¿Usted quisiera que esta búsqueda fuera sin diferenciación entre mayúsculas y minúsculas? [y] **>**
Si usted contesta **sí a** esta pregunta, encuentra las entradas sin importar el caso.

¿Usted quiere atar los registros? [n] **>**
Si usted contesta **sí a** esta pregunta, encuentra solamente las nuevas entradas mientras que

se generan. No busca todos los archivos del registro. Elija **ningún** para buscar todos los registros.

¿Usted quiere paginar la salida? [n] **>**
Si usted contesta **sí a** esta pregunta, visualiza el en un momento de la página de las entradas una. Esto es útil si usted necesita hacer una búsqueda general y esperarla extraer muchas entradas. Esto para las entradas de navegar apagado de la visualización.

2. Búsqueda para el MEDIADOS DE:

```
mail.example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> MID 96
Do you want this search to be case insensitive? [Y]>
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Fri Feb 3 15:41:43 2006 Info: Start MID 96 ICID 10394
Fri Feb 3 15:41:43 2006 Info: MID 96 ICID 10394 From: <bob@example.net>
Fri Feb 3 15:41:58 2006 Info: MID 96 ICID 10394 RID 0 To:
<nasir@example.com>
Fri Feb 3 15:42:06 2006 Info: MID 96 Message-ID
<4o8836$30@mail.example.com>
Fri Feb 3 15:42:06 2006 Info: MID 96 Subject 'test'
Fri Feb 3 15:42:06 2006 Info: MID 96 ready 23 bytes from
<bob@example.net>
Fri Feb 3 15:42:06 2006 Info: MID 96 matched all recipients for
per-recipient policy DEFAULT in the outbound table
Fri Feb 3 15:42:06 2006 Info: MID 96 antivirus negative
Fri Feb 3 15:42:06 2006 Info: MID 96 queued for delivery
Fri Feb 3 15:42:06 2006 Info: Delivery start DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: Message done DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: MID 96 RID [0] Response '2.6.0
<4o8836$30@mail.example.com> Queued mail for delivery'
Fri Feb 3 15:42:06 2006 Info: Message finished MID 96 done
```

Note que las MEDIADOS DE entradas proporcionan más información sobre cómo se procesa el mensaje. Las MEDIADOS DE entradas también se refieren al ICID y al DCID. Si usted quiere saber más sobre la conexión entrante, **grep** para el ICID. Si usted quiere saber más sobre qué sucedió cuando el ESA intentó la salida, **grep** para el DCID.

3. Para determinar donde el mensaje fue entregado, busque para el DCID.

```
mail.example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> DCID 14
Do you want this search to be case insensitive? [Y]>
```

```
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Fri Feb 3 15:42:06 2006 Info: New SMTP DCID 14 interface 192.168.0.199
address 10.1.1.112 port 25
Fri Feb 3 15:42:06 2006 Info: Delivery start DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: Message done DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:11 2006 Info: DCID 14 close
```

Note que el mensaje fue entregado de la interfaz de **192.168.0.199 al** host con la dirección IP 10.1.1.112 sobre el puerto 25.

Si la salida no fue intentada, pero el mensaje **fue hecho cola para la salida**, indica que el sistema pudo tener dificultad en sus comunicaciones con el servidor de destino. Usted puede utilizar el **hoststatus del** CLI para ver si el estatus del host receptor está **abajo de** y verificar que los IP pedidos hacen juego sus rutas S TP para el dominio del destino o los expedientes del público MX, como aplicable.