¿Cómo puedo identificar y abordar una situación del lazo de correo en el ESA?

Contenido

Introducción

En este documento se describe cómo identificar un lazo del correo en el dispositivo de seguridad de correo electrónico (ESA).

Antecedentes

Los lazos de correo se pueden formar a partir de mensajes con el mismo ID de mensaje que fueron encorporados más de 3 veces. Los lazos de correo pueden causar síntomas de CPU elevada, entrega lenta y problemas de rendimiento general. Los ID de mensaje incorporados más de una vez indican lazos en circunstancias normales, pero a veces se incorporan más de una vez debido a problemas, o tratarse de un spammer descuidado que envía una y otra vez el mismo mensaje con el mismo ID de mensaje.

Más comúnmente, un lazo de correo es causado por un problema en la infraestructura del correo electrónico que envíe el mismo mensaje o conjunto de mensajes que compiten su red de servidor en servidor. Si bien estos mensajes pueden permanecer de esta manera durante un período de tiempo prolongado, esto no es bueno para su ancho de banda ni para el costo de procesamiento en que se incurre.

Solución

Si sospecha que este es el problema que experimenta, identificar un lazo de correo suele ser bastante fácil, aunque deberá hacerlo manualmente.
Inicie sesión en la interfaz de comando de líneas (CLI) del sistema y envíe uno de estos comandos, o ambos, según considere necesario:

```
grep "Subject" mail_logs
grep "Message-ID" mail_logs
```

Si encuentra varias repeticiones de correos con el mismo ID de mensaje, sabrá que tiene un lazo de correo. No obstante, a veces esto no es suficiente, porque uno de los servidores de correo

que reenvía el mismo mensaje puede haber cambiado o eliminar el encabezado de ID de mensaje. Entonces, si no consigue identificar un mismo ID de mensaje repetido, intente comprobar los encabezados de Asunto.

En el caso de que haya encontrado el ID de mensaje enlazado, deberá buscar información adicional sobre dicho mensaje y su conexión principal (ICID). Con la información de ID de mensaje y MID que figura en la misma línea del registro, haga lo siguiente:

```
grep -e "MessageID_I_found" -e "MID 123456" mail_logs
```

La información que resulte de esta búsqueda le ayudará a identificar el ICID y DCIC relevantes para hacer lo siguiente:

```
grep -e "MessageID_I_found" -e "MID 123456" -e "ICID 1234567" -e "DCID 2345767" mail_logs
```

Ahora que tiene la información completa de la transacción conexión - mensaje, podrá descubrir de dónde viene el mensaje y a quién fue entregado (si esto ocurre). Una vez que haya identificado el mensaje enlazado, el próximo paso será echar un vistazo al mensaje para solucionar el problema. Si no resuelve el problema que origina el lazo, es probable que este y los otros mensajes permanezcan enlazados, o que el problema se presente nuevamente pronto.

Cree un filtro de mensajes parecido al que se muestra a continuación:

```
loganddrop_looper:
if(header("Message-ID") == "MessageID_I_found") {
  archive("looper");
  drop();
}
```

Después, aplique los cambios y envíe el comando que se detalla a continuación para echar un vistazo a la información del mensaje:

```
tail looper
```

Con la información obtenida sobre el sistema remoto a partir de los registros de correo, más la otra información obtenida del mensaje en sí, debería poder determinar donde está su problema.

¿Cómo se Pueden Prevenir los Lazos de Correo?

Esto puede resultar difícil de hacer en entornos complejos (es importante comprender el flujo de correo en su entorno y cómo un cambio de red, ya sea en el ESA o en otro dispositivo, afectará el tráfico). Una causa común de lazos de correo fugitivos es la eliminación del encabezado Recibido. El ESA detectará y parará automáticamente un lazo de correo cuando vea 100 encabezados de Recibido en un mensaje, pero el ESA permite eliminar este encabezado, lo que a menudo conduce a un mal lazo de correo. A menos que haya una buena razón para hacerlo, no desabilite el encabezado Recibido ni haga que se elimine.

A continuación se detalla un ejemplo de filtro que puede ayudarle a prevenir o a reparar un lazo del correo:

```
External_Loop_Count:
if (header("X-ExtLoop1")) {
```

```
 if (header("X-ExtLoopCount2")) {
   if (header("X-ExtLoopCount3")) {
     if (header("X-ExtLoopCount4")) {
       if (header("X-ExtLoopCount5")) {
         if (header("X-ExtLoopCount6")) {
           if (header("X-ExtLoopCount7")) {
             if (header("X-ExtLoopCount8")) {
               if (header("X-ExtLoopCount9")) {
                  notify ('joe@example.com');
                  drop();
               }
             else {insert-header("X-ExtLoopCount9", "from
                  $RemoteIP");}}
           else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}
         else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}
       else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}
     else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}
   else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}
 else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}
else {insert-header("X-ExtLoop1", "1"); }
```