Determinação da disposição da mensagem ESA

Índice

Introdução

Este documento descreve como determinar a disposição de uma mensagem com os logs do correio recuperados dos vários comandos na ferramenta de segurança do email de Cisco (ESA).

Pré-requisitos

A informação neste documento é baseada sobre:

- ESA
- Todas as versões de AsyncOS

Rastreamento de mensagem

Se você executa AsyncOS para a versão 6.0 ou mais recente do email, a maioria de maneira eficaz determinar o que aconteceu a um mensagem particular é usar a página do rastreamento de mensagem da aba do monitor. Isto permite que você procure com uma variedade de opções em uma interface da WEB fácil de usar.

Se você executa uma versão mais velha ou a precisa de recolher todas as linhas de registro para propósitos de Troubleshooting, use o **grep** ou os comandos **findevent** como detalhado nas próximas seções.

Comando de Findevent

Se você tem AsyncOS para a versão 5.1.2 ou mais recente do email, o comando **findevent** CLI faz mais simples procurar por uma mensagem específica. **Findevent** deixa-o procurar pelo envelope de, pelo receptor do envelope, ou pelo assunto da mensagem. Isto pode ser feito apesar do caso também. Uma vez que você encontra sua mensagem, você pode retornar cada linha de registro relevante a essa mensagem. Se você executa **findevent** sem argumentos, lança um assistente a fim guiá-lo com o processo. Como sempre, você pode usar o **comando help** a fim

aprender a forma resumida:

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

O primeiro formulário conduz uma busca para um envelope de, um assunto, ou um envelope específico dentro do log_name Nomeado e alista os ID de mensagem (MIDs) esse fósforo. - A bandeira i pode ser usada para buscas NON-caso-sensíveis.

O segundo formulário indica todas as linhas de registro para o MEADOS DE dado.

Se você tem uma versão mais velha, o **comando grep** CLI pode ser usado a fim realizar a mesma coisa. Contudo, o uso do **comando grep** exige um conhecimento mais detalhado de como eventos do mensagem de registro ESA.

Comando grep

O primeiro desafio quando você procura logs do correio é encontrar sua mensagem. Você pode fazer este se você procura pelo remetente, o receptor, ou pelo assunto. Uma vez que você encontrou sua mensagem, é importante compreender como os logs do correio são organizados. Os eventos satisfeitos do log do correio da Segurança são dados acrônimos. Os eventos os mais importantes são ICID, MEADOS DE, LIVRAM, e DCID.

Identificador de conexão da injeção (ICID): Quando um host remoto estabelece uma conexão ao dispositivo, essa conexão está atribuída um ICID. Um ICID pode desovar muito o MIDs.

> **Note**: **ICID 0** define uma mensagem que seja injetada dse. De fato, o numeral 0 depois que um ICID ou um DCID referem as sessões abertas a ou do endereço do loop local do dispositivo.

MEADOS DE: Uma vez que uma conexão é estabelecida, cada **correio** bem sucedido do Simple Mail Transfer Protocol (SMTP) **de:** o comando cria um MEADOS DE novo. Um único MEADOS DE pode desovar muitos RID.

Receptor ID (LIVRADO): Cada receptor (a: Centímetro cúbico: ou Bcc obtém LIVRADO. Os RID desovam somente DCIDs múltiplo se há um salto macio (erro de conexão) e a entrega reattempted.

Identificador de conexão da entrega (DCID): Cada receptor que vai ao mesmo domínio do destino recebe o mesmo DCID até os limites do sistema de recepção. Assim se os receipients do mensagens todas vão ao mesmo domínio, a seguir há um DCID para todos os RID. Se pelo contrário, cada um LIVRADO vai a um domínio separado, a seguir há uma correlação um a um.

> **Note**: **DCID 0** define uma mensagem que seja enviada nunca. De fato, o numeral 0 depois que um ICID ou um DCID referem as sessões abertas a ou do endereço do loop local do dispositivo.

Geralmente, quando você encontra sua mensagem, você encontra seu MEADOS DE. Então você grep para o MEADOS DE e determina o ICID e LIVRA-O. Com o ICID, você pode determinar a

contagem da reputação de SenderBase (SBR) para o remetente. Com LIVRADO e então o DCID, você pode determinar o que aconteceu quando o ESA tentou a entrega.

> **Note**: Uma vez que você tem o MEADOS DE, ICID, e DCID, você pode recuperar todas as fileiras para essa mensagem em um **grep**, se a origem da mensagem não é mais velha do que seu log mais velho do correio.

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

Exemplo

1. Busca para o assunto da mensagem:

```
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'
```

Isto gerou diversos fósforos que contiveram o **teste no** assunto. A mensagem foi enviada em aproximadamente 3:42pm, assim que você pode usar aquele MEADOS DE para a busca seguinte.

Estão aqui alguns pontos impotant a notar sobre as perguntas:

Você quer esta busca ser não diferenciando maiúsculas e minúsculas? [Y] >
Se você responde **sim a** esta pergunta, encontra entradas apesar do caso.

Você quer atar os logs? [N] >
Se você responde **sim a** esta pergunta, encontra somente entradas novas enquanto são geradas. Não procura todos os arquivos de registro. Escolha **nenhum** a fim procurar todos os logs.

Você quer paginar a saída? [N] >

Se você responde **sim a** esta pergunta, indica entradas uma página de cada vez. Isto é útil se você precisa de fazer uma busca geral e da esperar recuperar muitas entradas. Isto para as entradas do enrolamento fora do indicador.

2. Busca para o MEADOS 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
```

Observe que as entradas MEADOS DE fornecem mais informação sobre como a mensagem é processada. As entradas MEADOS DE igualmente proveem o ICID e o DCID. Se você quer saber mais sobre a conexão recebida, **grep** para o ICID. Se você quer saber mais sobre o que aconteceu quando o o ESA tentou a entrega, **grep** para o DCID.

3. A fim determinar onde a mensagem foi entregada, procure pelo 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
```

Observe que a mensagem esteve entregada da relação de 192.168.0.199 ao host com endereço IP 10.1.1.112 sobre a porta 25.

Se a entrega não foi tentada, mas a mensagem foi enfileirada para a entrega, indica que o sistema pôde ter a dificuldade em suas comunicações com o servidor de destino. Você pode usar o hoststatus do CLI a fim ver se o estado do host destinatário está abaixo de e para verificar que o fósforo pedido IPs uma ou outra suas rotas S TP para o domínio do destino ou os registros do público MX, como aplicável.