Como o ESA segura as mensagens de salto enviadas a 127.0.0.1?

Índice

Pergunta:

Como o ESA segura as mensagens de salto enviadas a 127.0.0.1?

Quando os spammer enviam o email, originam ocasionalmente o email dos Domain Name que resolverão a um dos endereços de loopback reservados IP (tipicamente 127.0.0.1, embora todo o endereço no bloco 127.0.0.0/8 seja reservado para finalidades do laço de retorno). Estes endereços são encontrados igualmente ocasionalmente em um worm deenvio pelo correio, quando o Domain Name forjado da fonte foi projetado nunca receber o correio e tem assim um endereço IP de Um ou Mais Servidores Cisco ICM NT ilegal para desanimar o email.

A edição com tais Domain Name que resolvem aos endereços de loopback é que um MTA confiante pôde tentar conectar ao endereço para entregar a mensagem. Desde que o endereço de loopback conecta de volta ao mesmo MTA, um laço pode ser gerado. Segundo como os encabeçamentos são formados em uma mensagem saltada, o laço pode ser particularmente caro, eventualmente conseguindo grande bastante consumir todos os recursos de sistema.

O ESA evita esta síndrome patológica. Quando uma pesquisa de DNS conduzir a um endereço IP de Um ou Mais Servidores Cisco ICM NT na escala do laço de retorno (127.0.0.0/8), o cliente de SMTP de AsyncOS não tentará entregar tal mensagem. Você pode observar este comportamento olhando o log dos mail_logs. O seguinte trecho do log mostra uma mensagem que está sendo enviada com um Domain Name do endereço do remetente que resolva ao endereço IP 127.0.0.1. Quando a mensagem não pode ser entregada, AsyncOS cria uma mensagem de salto, mas não tenta e entrega a mensagem saltada porque o DNS está apontando ao endereço de loopback.

```
Thu o 9 de dezembro 22:06:03 2004 informações: Comece 524 ICID MEADOS DE 322
Thu o 9 de dezembro 22:06:03 2004 informações: 524 ICID MEADOS DE 322 de: <
loopme@loopback.example.com >
Thu o 9 de dezembro 22:06:08 2004 informações: 524 ICID MEADOS DE 322 LIVRARAM 0 a:
<illegal99999@example.com>
Thu o 9 de dezembro 22:06:09 2004 informações: 524 ID de mensagem MEADOS DE
'<3l57rh$gc@mail.example.com>'
Thu o 9 de dezembro 22:06:10 2004 informações: 524 bytes 9 prontos MEADOS DE < de
loopme@loopback.example.com >
Thu o 9 de dezembro 22:06:10 2004 informações: 524 MEADOS DE combinaram todos os receptores para
por-recipientpolicy o PADRÃO na tabela de entrada
Thu o 9 de dezembro 22:06:10 2004 informações: Negativo MEADOS DE de 524 Brightmail
Thu o 9 de dezembro 22:06:10 2004 informações: Negativo MEADOS DE do antivirus 524
Thu o 9 de dezembro 22:06:10 2004 informações: 524 MEADOS DE enfileirados para a entrega
Thu o 9 de dezembro 22:06:10 2004 informações: Endereço novo 192.245.12.7 de 192.35.195.101 da
relação S TP DCID 160
Thu o 9 de dezembro 22:06:10 2004 informações: Começo DCID 160 524 MEADOS DE da entrega PARA
LIVRAR [0]
```

Thu o 9 de dezembro 22:06:10 2004 informações: Saltado: DCID 160 524 MEADOS DE PARA LIVRAR 0 - 5.1.0 - erros de endereço desconhecidos (usuário desconhecido ou ilegal '550', ['5.1.1: illegal99999@example.com'])
Thu o 9 de dezembro 22:06:10 2004 informações: 525 MEADOS DE gerados para o salto de 524 MEADOS DE
Thu o 9 de dezembro 22:06:10 2004 informações: Comece 525 ICID MEADOS DE 0
Thu o 9 de dezembro 22:06:10 2004 informações: 525 ICID MEADOS DE 0 de: <>
Thu o 9 de dezembro 22:06:10 2004 informações: 525 ICID MEADOS DE 0 LIVRARAM 0 a: <loopme@loopback.opus1.com>
Thu o 9 de dezembro 22:06:10 2004 informações: 525 MEADOS DE enfileirados para a entrega
Thu o 9 de dezembro 22:06:10 2004 informações: Mensagem terminada 524 MEADOS DE feitos
Thu o 9 de dezembro 22:06:10 2004 que advertem: pontos do trajeto da definição do servidor de nome ao endereço 0.x.x.x ou 127.x.x.x. domain=loopback.example.com
Thu o 9 de dezembro 22:06:10 2004 informações: Fim ICID 322
Thu o 9 de dezembro 22:06:15 2004 informações: Fim DCID 160