¿Cómo el ESA maneja los mensajes de despedida enviados a 127.0.0.1?

Contenido

Pregunta:

¿Cómo el ESA maneja los mensajes de despedida enviados a 127.0.0.1?

Cuando los spammeres envían el correo electrónico, originan de vez en cuando el correo electrónico de los Domain Name que resolverán a uno de los Loopback Address reservados IP (típicamente 127.0.0.1, aunque cualquier direccionamiento en el bloque 127.0.0.0/8 sea reservado para los propósitos del loopback). Estos direccionamientos también se encuentran de vez en cuando en un gusano de masa-envío, cuando el Domain Name forjado de la fuente nunca fue diseñado para recibir el correo y tiene así una dirección IP ilegal para desalentar el correo electrónico.

El problema con tales Domain Name que resuelven a los Loopback Address es que un MTA confiado pudo intentar conectar con el direccionamiento para entregar el mensaje. Puesto que el Loopback Address conecta de nuevo al mismo MTA, un loop puede ser generado. Dependiendo de cómo las encabezados se forman en un mensaje despedido, el loop puede ser determinado costoso, eventual consiguiendo bastante grande consumir a todos los recursos del sistema.

El ESA evita este síndrome patológico. Cuando una búsqueda de DNS da lugar a una dirección IP en el rango del loopback (127.0.0.0/8), el cliente SMTP de AsyncOS no intentará entregar tal mensaje. Usted puede observar este comportamiento mirando el registro de los mail_logs. El extracto siguiente del registro muestra un mensaje que es enviado con un Domain Name de la dirección de retorno que resuelva a la dirección IP 127.0.0.1. Cuando el mensaje no puede ser entregado, AsyncOS crea un mensaje de despedida, pero no intenta y entrega el mensaje despedido porque el DNS está señalando al Loopback Address.

```
Thu 9 de diciembre 22:06:03 2004 informaciones: Comience MEDIADOS DE 524 ICID 322
Thu 9 de diciembre 22:06:03 2004 informaciones: MEDIADOS DE 524 ICID 322 de: <
loopme@loopback.example.com >
Thu 9 de diciembre 22:06:08 2004 informaciones: MEDIADOS DE 524 ICID 322 LIBRARON 0 a:
<illegal99999@example.com>
Thu 9 de diciembre 22:06:09 2004 informaciones: MEDIADOS DE 524 ID del mensaje
'<3l57rh$gc@mail.example.com>'
Thu 9 de diciembre 22:06:10 2004 informaciones: MEDIADOS DE 524 9 bytes listos de <
loopme@loopback.example.com >
Thu 9 de diciembre 22:06:10 2004 informaciones: MEDIADOS DE 524 correspondieron con a todos los
beneficiarios para por-recipientpolicy el VALOR POR DEFECTO en la tabla entrante
Thu 9 de diciembre 22:06:10 2004 informaciones: MEDIADOS DE negativa de 524 Brightmail
Thu 9 de diciembre 22:06:10 2004 informaciones: MEDIADOS DE negativa del antivirus 524
Thu 9 de diciembre 22:06:10 2004 informaciones: MEDIADOS DE 524 hechos cola para la salida
Thu 9 de diciembre 22:06:10 2004 informaciones: Nuevo direccionamiento 192.245.12.7 de
192.35.195.101 de la interfaz S TP DCID 160
Thu 9 de diciembre 22:06:10 2004 informaciones: Comienzo DCID 160 MEDIADOS DE 524 de la salida A
```

LIBRAR [0]
Thu 9 de diciembre 22:06:10 2004 informaciones: Despedido: DCID 160 MEDIADOS DE 524 PARA LIBRAR 0 - 5.1.0 - errores de dirección desconocidos (usuario desconocido o ilegal '550', ['5.1.1: illegal99999@example.com'])
Thu 9 de diciembre 22:06:10 2004 informaciones: MEDIADOS DE 525 generados para la despedida de MEDIADOS DE 524
Thu 9 de diciembre 22:06:10 2004 informaciones: Comience MEDIADOS DE 525 ICID 0
Thu 9 de diciembre 22:06:10 2004 informaciones: MEDIADOS DE 525 ICID 0 de: <>
Thu 9 de diciembre 22:06:10 2004 informaciones: MEDIADOS DE 525 ICID 0 LIBRARON 0 a: <loopme@loopback.opus1.com>
Thu 9 de diciembre 22:06:10 2004 informaciones: MEDIADOS DE 525 hechos cola para la salida
Thu 9 de diciembre 22:06:10 2004 informaciones: Mensaje acabado MEDIADOS DE 524 hechos
Thu 9 de diciembre 22:06:10 2004 que advierten: puntas del trayecto de resolución del nameserver al direccionamiento 0.x.x.x o 127.x.x.x. domain=loopback.example.com
Thu 9 de diciembre 22:06:10 2004 informaciones: Cierre ICID 322
Thu 9 de diciembre 22:06:15 2004 informaciones: Cierre DCID 160