O ESA experimenta uma tempestade do salto (NDR)

Índice

Introdução

Este documento descreve um problema encontrado onde sua ferramenta de segurança do email (ESA) experimenta uma tempestade do salto e oferece uma solução ao problema.

Informações de Apoio

Uma tempestade do salto é um efeito secundário de um trabalho de Joe ou de um backscatter do Spam do email.

Trabalho de Joe

Um trabalho de Joe é um ataque do Spam que dados falsificado e alvos do remetente dos usos para manchar a reputação do remetente aparente e/ou para induzir os receptores tomar a ação contra o remetente aparente.

Backscatter

Um backscatter é um efeito secundário do Spam do email, vírus, e worms onde os servidores de e-mail que recebem o Spam e o outro correio enviam mensagens de salto a um partido inocente. Isto ocorre porque o remetente do envelope do mensagem original é forjado a fim conter o endereço email da vítima. Desde que estas mensagens não foram solicitadas pelos receptores, são substancialmente similares entre si, e são entregadas em quantidades maiorias, qualificam como o email ou o Spam maioria espontâneo. Como tal, os sistemas que gerenciem o backscatter do email podem tornar-se listados em várias listas negras do Domain Name System

(DNSBLs) e ser em violação dos termos dos provedores de serviço da Internet de serviço.

Problema

Seu ESA experimenta uma tempestade do salto onde haja um dilúvio das mensagens injetadas no ESA. Os pontos da contagem da conexão recebida durante tal ataque. O dispositivo pôde desenvolver um backup do workqueue. A fim verificar se o dispositivo é sujeito a tal ataque, grep que o correio registra para o correio do endereço. Salta (relatórios da NON-entrega - Os NDR) têm um correio vazio do envelope do endereço.

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

Um dispositivo que seja sujeito a uma tempestade do salto terá a maioria das mensagens com o correio do envelope do endereço do "**<>**".

Solução

Há um número de opções para controlar uma tempestade do salto.

Verificação do salto

A fim combater estes ataques orientados mal do salto, AsyncOS inclui a verificação do salto de Cisco. Quando permitida, esta característica etiqueta o endereço do remetente do envelope para as mensagens enviadas através do ESA. O receptor do envelope para toda a mensagem de salto recebida pelo ESA é verificado então para ver se há a presença desta etiqueta. Quando as mensagens de salto legítimas são recebidas, a etiqueta que foi adicionada ao remetente que do envelope o endereço é removido e o salto estão entregados ao receptor. As mensagens de salto que não contêm a etiqueta podem ser seguradas separadamente.

AsyncOS considera saltos como o correio com um correio nulo do endereço (**<>**). As mensagens que são dos endereços tais como mailer-daemon@example.com ou postmaster@example.com não são consideradas saltos pelo sistema e não são sujeitas saltar a verificação.

Configurar o endereço da verificação do salto que etiqueta chaves

O endereço da verificação do salto que etiqueta a enumeração das chaves mostra que seus chave e algum atuais unpurged o fecha se usou no passado. A fim adicionar uma chave nova, termine estas etapas:

1. Na página da **verificação das políticas >** do **salto do correio**, clique a **chave nova**.
2. Incorpore uma sequência de caracteres de texto e o clique **submete-se**.
3. Comprometa suas mudanças.

Removendo chaves

Você pode remover seu endereço velho que etiqueta chaves se você seleciona uma regra removendo do menu de destruição e clica a **remoção.**

Configurar ajustes da verificação do salto de Cisco

Os ajustes da verificação do salto determinam que ação a tomar quando um salto inválido é recebido.

- Escolha **políticas do correio > verificação do salto**.
- O clique **edita ajustes**.
- Selecione se rejeitar saltos inválidos ou adicionar um encabeçamento feito sob encomenda à mensagem. Se você quer adicionar um encabeçamento, incorpore o nome e o valor do encabeçamento.
- Opcionalmente, permita exceções espertas. Este ajuste permite as mensagens do correio recebido e as mensagens de salto geradas pelos servidores de e-mail interno a ser isentados automaticamente do processamento da verificação do salto (mesmo quando um único ouvinte é usado para o correio entrante e que parte).
- Submeta e comprometa suas mudanças.

Configurar a verificação do salto de Cisco com o CLI

Você pode usar os comandos do **bvconfig** e do **destconfig no** CLI a fim configurar a verificação do salto. Estes comandos são discutidos no guia de referência de Cisco AsyncOS CLI.

Cisco salta a verificação e a configuração de grânulos

A verificação do salto trabalha em uma configuração de grânulos enquanto ambos os dispositivos de Cisco usam a mesma do “chave salto.” Quando você usa a mesma chave, um ou outro sistema deve poder aceitar um bounceback legítimo. A etiqueta/chave alteradas do encabeçamento não é específicas a cada dispositivo de Cisco.

Filtro de correio

Se você não pode usar a verificação do salto porque você usa dispositivos separados para o recibo e a entrega, você pode estabelecer um filtro da mensagem a fim obstruir as mensagens que têm um correio vazio do endereço.

Bloco do correio

Desde que estas mensagens de salto terão muito provavelmente um endereço destinatário do envelope inexistente, você pode endereços inválidos de bloco através da validação destinatária do Lightweight Directory Access Protocol (LDAP) da conversação a fim ajudar mais baixo o impacto de tais mensagens.