

O Spam obtém perto Cisco envia por correio eletrônico a ferramenta de segurança (ESA) em sua organização

Índice

[Introdução](#)

[Métodos](#)

1. [Correio legítimo da mensagem/mercado](#)
2. [O Anti-Spam não está sendo atualizado corretamente](#)
3. [Filtro da política ou da mensagem do correio](#)
4. [Política do fluxo de correio](#)
5. [A mensagem é Spam](#)

Introdução

Este documento descreve cinco métodos que os email do Spam podem incorporar sua organização.

Métodos

1. Correio legítimo da mensagem/mercado

A mensagem legítima foi optada dentro pelo usuário ou seu nome foi vendido a uma outra organização. No primeiro caso o usuário precisará de tomar etapas ao cancelar assinatura da lista. Se é o último, submeta a mensagem outra vez a spam@access.ironport.com assim que as definições do antispam podem ser atualizadas globalmente, melhorando a taxa total da captação do Spam de seu ESA. Permitir o correio do mercado na política do correio recebido pode ajudar a mudar a percepção desta mensagem “que introduz no mercado” sobre o “Spam”.

2. O Anti-Spam não está sendo atualizado corretamente

O Anti-Spam é desabilitado ou a chave de recurso expirou. Para verificar e ver se o Anti-Spam está atualizando, vá aos **serviços do > segurança GUI > ao Anti-Spam de IronPort**. Dentro deste painel você deve ver atualizações aos grupos das regras ou motor dentro das últimas horas 6. Igualmente de dentro desta aba na parte superior você pode assegurar-se de que o serviço do Anti-Spam esteja permitido. Para a revisão do estado da chave de recurso você pode ir à aba > à chave de recurso da administração do sistema a verificar no estado da chave do Anti-Spam.

3. Filtro da política ou da mensagem do correio

O Spam pode obter em sua organização se o motor da Segurança do Anti-Spam é desabilitado para um remetente ou um receptor específico por uma política do correio do cliente. Uma outra maneira de saltar a filtração do Spam é através da mensagem filtra (CLI: comando dos **filtros**).

4. Política do fluxo de correio

Uma mensagem é classificada usando o ICID da mensagem. Nesta situação é provável que os recursos de segurança do Anti-Spam estão desligados, que cancelam a política do correio. Você pode determinar este olhando os logs do correio, dentro dos logs que você precisará primeiramente de rever o ICID para compreender que SenderGroup a mensagem foi classificada. Lá da revisão da política associada do fluxo de correio. Se você tem uma grande quantidade de entradas em seu WhiteList, você pode precisar de rever algumas das mensagens que estão conseguindo dentro considerar se foram feitas a varredura pelo motor de AntiSpam. Abra os encabeçamentos de uma mensagem e procure o X-IronPort-Spam do encabeçamento, a presença deste encabeçamento significa que a mensagem atravessou o motor.

5. A mensagem é Spam

A mensagem é Spam real. Você confirmou a mensagem foi feito a varredura pelo motor do antispam usando a característica do rastreamento de mensagem (no rastreamento de mensagem, procure o "CASO"). Se a sentença do caso é negativa e você julga a mensagem para ser Spam, submeta o mensagem original a spam@access.ironport.com. Este poderia ser um exemplo de uma ameaça nova do Spam que estão sendo liberadas apenas ou de uma ameaça mais velha que re-fosse projetada.

O processamento das submissões do Spam é um automático e o processo manual e lá não é nenhum feedback para sua submissão específica. Em qualquer momento você pode contactar o tac Cisco e pedir uma avaliação e uma resposta.