Ativação de recursos de DHAP ESA

Contents

Introduction

Este documento descreve como ativar o recurso de prevenção de ataque de coleta de diretório (DHAP) no Cisco Email Security Appliance (ESA) para evitar ataques de coleta de diretório (DHAs).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ESA
- AsyncOS

Componentes Utilizados

As informações neste documento são baseadas em todas as versões do AsyncOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

Um DHA é uma técnica usada por spammers para localizar endereços de e-mail válidos. Há duas técnicas principais que são usadas para gerar os endereços que o DHA tem como alvo:

- O remetente de spam cria uma lista com todas as combinações possíveis de letras e números e, em seguida, anexa o nome de domínio.

- O remetente de spam usa um ataque de dicionário padrão com a criação de uma lista que combina nomes, sobrenomes e iniciais comuns.

O DHAP é um recurso com suporte nos Cisco Content Security Appliances que pode ser

habilitado quando a validação de aceitação do Lightweight Diretory Access Protocol (LDAP) é usada. O recurso DHAP rastreia o número de endereços de destinatário inválidos de um determinado remetente.

Quando um remetente ultrapassa um limite definido pelo administrador, ele é considerado não confiável e o e-mail desse remetente é bloqueado sem nenhum requisito de projeto de rede (NDR) ou geração de código de erro. Você pode configurar o limite com base na reputação do remetente. Por exemplo, remetentes não confiáveis ou suspeitos podem ter um limite de DHAP baixo, e remetentes confiáveis ou confiáveis podem ter um limite de DHAP alto.

Ativar DHAP

Para habilitar o recurso DHAP, navegue para **Políticas de e-mail > Tabela de acesso de host (HAT)** na GUI do Content Security Appliance e selecione **Políticas de fluxo de e-mail**. Escolha a política que deseja editar na coluna **Nome da política**.

O HAT tem quatro regras básicas de acesso que são usadas para agir em conexões de hosts remotos:

- **ACEITO:** A conexão é aceita e a aceitação de e-mail é ainda mais restrita pelas configurações de ouvinte. Isso inclui a tabela de acesso de destinatário (para ouvintes públicos).
- **REJECT:** A conexão é aceita inicialmente, mas o cliente que tentar se conectar receberá uma saudação 4XX ou 5XX. Nenhum e-mail é aceito.
- **TCPREFUSE**: A conexão é recusada no nível TCP.
- **RETRANSMISSÃO:** A conexão é aceita. O recebimento de qualquer destinatário é permitido e não é restrito pela tabela de acesso de destinatário. A assinatura de Chaves de Domínio está disponível apenas em políticas de fluxo de e-mail de retransmissão.

Na seção **Limites de fluxo de e-mail** da política selecionada, localize e defina a configuração **Prevenção de ataque de coleta de diretório (DHAP)** definindo a **Máx.** Destinatários Inválidos Por Hora. Você também pode optar por personalizar o Máx. Destinatários inválidos por código de hora e máximo. Texto de destinatários por hora inválido se desejar.

Você deve repetir esta seção para configurar o DHAP para políticas adicionais.

Certifique-se de enviar e confirmar todas as alterações na GUI.

> **Note**: A Cisco recomenda que você use um número máximo entre cinco e dez para o **número máximo de destinatários inválidos por hora de uma** configuração de **host remoto**.

> **Note**: Para obter informações adicionais, consulte o **Guia do usuário do AsyncOS** no Portal de suporte da Cisco.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.