Como permitir campanhas de plataforma de phishing simuladas por meio do Cisco Email Security Appliance

Contents

Introduction

Este documento descreve as etapas de configuração no Cisco Email Security Appliance (ESA) para permitir campanhas de plataformas de phishing simuladas com êxito.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Criação de filtros de mensagens e conteúdo no ESA.
- Configuração da HAT (Host Access Table, tabela de acesso de host).
- Compreensão do pipeline de e-mails de entrada do Cisco ESA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Plataformas de phishing simuladas permitem que os administradores executem campanhas de phishing como parte de um ciclo para gerenciar uma das maiores ameaças que usa os sistemas de e-mail como vetor de ataques de engenharia social.

Problema

Quando o ESA não está preparado para tais simulações, não é raro que os seus motores de pesquisa interrompam as mensagens da campanha de phishing, resultando em falha ou diminuição da eficácia das simulações.

Solução

> **Caution**: Neste exemplo de configuração, a política de fluxo de correio *TRUSTED* é selecionada para permitir que o ESA passe por campanhas de phishing simuladas maiores sem qualquer limitação. A execução contínua de campanhas de phishing de alto volume pode afetar o desempenho do processamento de e-mails.

Para garantir que as mensagens da campanha de phishing não sejam interrompidas por nenhum componente de segurança da configuração do ESA, é necessário implantar.

1. Criar um novo grupo de remetente: **GUI > Políticas de e-mail > Visão geral do HAT** e vinculá-la à política de fluxo de e-mail *TRUSTED* (como alternativa, uma nova política pode ser criada com opções semelhantes em **GUI > Políticas de e-mail > Políticas de fluxo de e-mail**).
2. Adicione o(s) host(s) de envio ou o(s) IP(s) da plataforma de phishing simulada a esse grupo de remetente. Se a plataforma de phishing simulada tiver um grande intervalo de IPs, você poderá adicionar nomes de host parciais ou intervalos de IP, se aplicável.
3. Ordene o grupo de remetente acima do seu grupo de remetente *BLOCKLIST* para garantir que a correspondência está sendo feita estaticamente em vez de SBRS.
4. Desative todo o recurso de segurança da política de fluxo de e-mail *TRUSTED* em **GUI > Políticas de e-mail > Políticas de fluxo de e-mail > TRUSTED** (ou sua política de fluxo de e-mail recém-criada):

Security Features	
Spam Detection:	○ Use Default (On) ○ On ◉ Off
AMP Detection	○ Use Default (On) ○ On ◉ Off
Virus Protection:	○ Use Default (On) ○ On ◉ Off
Sender Domain Reputation Verification:	○ Use Default (On) ○ On ◉ Off
Virus Outbreak Filters:	○ Use Default (On) ○ On ◉ Off
Advanced Phishing Protection:	○ Use Default (On) ○ On ◉ Off
Graymail Detection:	○ Use Default (On) ○ On ◉ Off
Content Filters:	○ Use Default (On) ○ On ◉ Off
Message Filters:	○ Use Default (On) ○ On ◉ Off

5. **Envie essas alterações e confirme.**

AsyncOS v.14 anterior

Caution: Neste exemplo de configuração, a política de fluxo de correio *TRUSTED* é selecionada para permitir que o ESA passe por campanhas de phishing simuladas maiores sem qualquer limitação. A execução contínua de campanhas de phishing de alto volume pode afetar o desempenho do processamento de e-mails.

Para garantir que as mensagens da campanha de phishing não sejam interrompidas por nenhum componente de segurança da configuração do ESA, é necessário implantar.

1. Criar um novo grupo de remetente: **GUI > Políticas de e-mail > Visão geral do HAT** e vinculá-lo à política de fluxo de e-mail *CONFIÁVEL*.
2. Adicione o(s) host(s) de envio ou o(s) IP(s) da plataforma de phishing simulada a esse grupo de remetente. Se a plataforma de phishing simulada tiver um grande intervalo de IPs, você poderá adicionar nomes de host parciais ou intervalos de IP, se aplicável.
3. Ordene o grupo de remetente acima do seu grupo de remetente *BLOCKLIST* para garantir que a correspondência está sendo feita estaticamente em vez de SBRS.
4. **Envie essas alterações e confirme.**
5. Navegue até a CLI e adicione um novo filtro de mensagens, **CLI > filtros,** copie e modifique a sintaxe e adicione o filtro.
6.
```
skip_engines_for_simulated_phishing:
if (sendergroup == "name_of_the_newly_created_sender_group")
{
insert-header("x-sp", "uniquevalue");
log-entry("Skipped scanning engines for simulated phishing");
skip-spamcheck();
skip-viruscheck();
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
skip-filters();
}
.
```
7. Ordene o filtro de mensagens para cima na lista para garantir que ele não seja ignorado por outro filtro de mensagens acima dele, que inclui a ação de ignorar filtros.
8. Pressione a tecla Enter para voltar ao prompt de comando principal do AsyncOS e emita o comando "**commit**" para confirmar as alterações. (não clique em CTRL+C - ele apagará todas as alterações).
9. Navegue até a **GUI> Políticas de e-mail > Filtros de conteúdo de entrada**
10. Crie um novo Filtro de Conteúdo de Entrada com a condição ***"Outro Cabeçalho"*** definida para procurar o cabeçalho personalizado **"x-sp"** e seu *valor exclusivo* configurado no filtro de mensagens e configure a ação ***Ignorar Filtros de Conteúdo Restantes (Ação Final)***.
11. Ordene o filtro de conteúdo para "1" para garantir que outros filtros não atuem contra a mensagem de phishing simulada.
12. Navegue até **GUI > Políticas de e-mail > Políticas de recebimento de e-mail** e atribua o filtro de conteúdo à política necessária.
13. **Enviar e confirmar alterações.**
14. Execute a campanha da plataforma de phishing simulada e monitore os logs de email/Rastreamento de mensagem para verificar a correspondência de fluxo e regra de política.