Relatar spam, mensagens de e-mail de vírus com classificação incorreta

Contents

Introduction
Tipos de Envios de Mensagens de Email
Por que relatar e-mails à Cisco?
Portal de status de e-mail
Como relatar mensagens de e-mail à Cisco
Suplemento de envio de e-mail seguro da Cisco
Plug-in do Cisco Email Security
Envio de mala direta
Microsoft Outlook
Microsoft Outlook Web App, Microsoft Office 365
Microsoft Outlook 2011 e Microsoft Outlook 2016 para Mac (OS X, macOS)
Correio (OS X, macOS)
Thunderbird Mozilla
Plataformas móveis (iPhone, Android ou outro)
Como verificar envios à Cisco
Envio de mala direta
Portal de status de e-mail
Additional Information
Documentação do Cisco Secure Email Gateway
Documentação do Secure Email Cloud Gateway
Documentação do Cisco Secure Email and Web Manager
Documentação do produto Cisco Secure

Introduction

Este documento descreve o relato de e-mails de spam, classificados incorretamente, virais ou adicionais à Cisco para suporte ou exame.

Tipos de Envios de Mensagens de Email

Spam, Ham e mensagens de e-mail de marketing são:

- *Spam*: Mensagens de e-mail irrelevantes ou inadequadas para um destinatário.
- *Presunto*: Uma mensagem de e-mail que não é spam. Ou "não spam", "e-mail bom".
- *Marketing*: Marketing direto de uma mensagem de e-mail comercial.

A Cisco aceita envios de e-mails classificados incorretamente:

- falso-negativo (spam perdido)
- falso-positivo (ou "Presunto")
- mensagens de marketing falso-negativo
- mensagens de marketing falso positivo
- mensagens suspeitas de phishing, mensagens positivas de phishing
- mensagens com suspeita de vírus e positivas para vírus

Por que relatar e-mails à Cisco?

Mensagens de e-mail perdidas ou marcadas incorretamente relatadas à Cisco ajudam na confirmação do conteúdo, na eficácia geral e nas regras e pontuações associadas. Depois de relatar um e-mail para a Cisco, você também poderá visualizar outros objetos de observação e anexos incorporados por meio do Portal de status de e-mail.

Portal de status de e-mail

Com uma ID CCO válida, você pode fazer login em https://talosintelligence.com/tickets/email_submissions. O Portal de status de e-mail é uma ferramenta para visualizar o status de seus envios de e-mail à Cisco. A Cisco incentiva envios de spam/phishing que ultrapassam o conteúdo de detecção atual e Ham, e-mails desejáveis que foram filtrados incorretamente, para melhorar a eficácia geral. O Portal de status de e-mail fornece uma maneira de controlar o status desses envios. Você pode monitorar seus envios, e os administradores de domínio ou visualizadores de domínio podem monitorar todos os envios de seus domínios.

> **Observação**: o portal de rastreamento e envio de e-mail (ESTP) legado foi substituído pelo portal de status de e-mail, hospedado em Talosintelligence.com, a partir de 1º de setembro de 2020.

Como relatar mensagens de e-mail à Cisco

Os métodos suportados são:

1. Suplemento de Envio de Email do Cisco Secure
   Oferece suporte ao Outlook (Windows, Mac e Web)
2. Plug-in do Cisco Email Security Suporte ao Outlook (somente Windows)
3. Envio de mala direta por email do usuário final

Suplemento de envio de e-mail seguro da Cisco

O Add-in Cisco Secure Email Submission oferece suporte ao Microsoft Outlook para Windows, Mac e Web. Consulte "Configurações suportadas para o Add-In Cisco Secure Email Encryption Service e o Add-in Cisco Secure Email Submission" na Matriz de Compatibilidade do Cisco Secure Email Encryption Service para garantir a compatibilidade da sua versão do Outlook.

Consulte o Add-in Cisco Secure Email Submission para baixar e instalar a documentação.

Plug-in do Cisco Email Security

O plug-in do Cisco Email Security é compatível apenas com o Microsoft Outlook no Windows. Consulte "Configurações suportadas para o plug-in do Cisco Email Reporting" na Matriz de compatibilidade do Cisco Secure Email Encryption Service para garantir a compatibilidade da sua versão do Outlook.

> **Note**: As versões mais antigas do plug-in são denominadas "Plug-in do IronPort Email Security" ou "Plug-in de criptografia para Outlook". Esta versão do plug-in continha o Reporting and Encryption em conjunto. Em 2017, a Cisco separou os serviços e lançou duas novas versões do plug-in, "Email Reporting Plugin for Outlook" e "Email Encryption Plugin for Outlook". Eles estavam disponíveis com uma versão 1.0.0.x.

Envio de mala direta

Siga as instruções para seu cliente de e-mail fornecido para anexar o e-mail como um anexo codificado RFC 822 Multipurpose Internet Mail Extension (MIME). Se um dos exemplos não refletir o cliente de e-mail, consulte diretamente o guia do usuário do cliente de e-mail ou o suporte ao produto e confirme se o cliente de e-mail suporta "Encaminhamento como anexo".

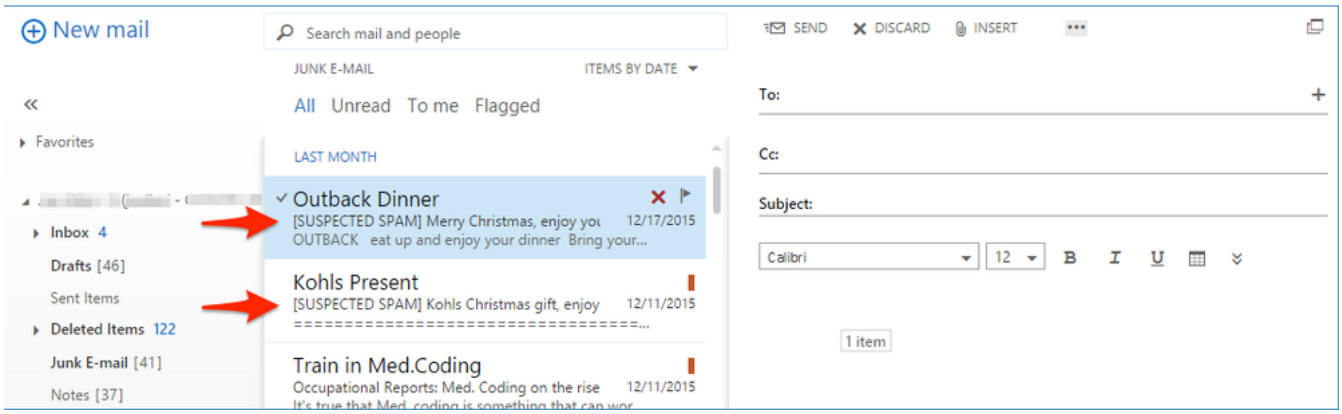
Envie os emails enviados para o endereço de email apropriado:

spam@access.ironport.com	O usuário final considera o spam de mensagem de e-mail ou a linha de assunto cont [SPAM SUSPEITO].
ham@access.ironport.com	O usuário final NÃO considera a mensagem de e-mail como spam. A linha de assunt contém [SPAM SUSPEITO] ou a linha de assunto inclui marcas adicionais.
ads@access.ironport.com	O usuário final considera a mensagem de e-mail como sendo ou contendo conteúdo marketing ou mensagens em cinza, ou a linha de assunto inclui [MARKETING], [RED SOCIAL] ou [BULK].
not_ads@access.ironport.com	O usuário final NÃO considera a mensagem de e-mail como marketing ou em cinza, linha de assunto contém [MARKETING], [REDE SOCIAL] ou [BULK].
phish@access.ironport.com	A mensagem de e-mail parece ser um phishing (projetado para adquirir nome(s) de usuário, senhas, informações de cartão de crédito ou outras informações de identific pessoal), ou a mensagem de e-mail contém anexos de malware (da mesma forma, projetado para adquirir nome(s) de usuário ou senhas.) A linha de assunto é precedi [SPAM SUSPEITO], [Possível $threat_category Fraud] ou semelhante.

virus@access.ironport.com	O usuário final considera a mensagem de e-mail ou um anexo como viral ou a linha d assunto contém [AVISO: VÍRUS DETECTADO].

Nem todas as linhas de assunto contêm texto e marcas adicionais. Para suas configurações, consulte a configuração do Cisco Secure Email Gateway ou do Cloud Gateway para obter filtros antisspam, antivírus, de mensagens de cinza e epidemia, ou entre em contato com o administrador de e-mail se tiver alguma preocupação.

Exemplo de linhas de assunto marcadas:



aviso: Não 'Encaminhar' sua mensagem de e-mail como envio. Esta ação não retém a ordem dos cabeçalhos de roteamento de email e remove os cabeçalhos de roteamento de email necessários para atribuir a origem do email. Em vez disso, certifique-se sempre de enviar o e-mail em questão através da opção "encaminhamento como anexo".

Você pode enviar um e-mail diretamente de:

- Microsoft Outlook
- Microsoft Outlook Web App, Microsoft Office 365
- Microsoft Outlook 2011 e Microsoft Outlook 2016 para Mac (OS X, macOS)
- Correio (OS X, macOS)
- Thunderbird Mozilla
- Plataformas móveis (iPhone, Android ou outro)

Microsoft Outlook

- O método preferencial de envio do Microsoft Outlook é usar o Add-in Envio de Email Seguro da Cisco.
- Envie mensagens para a Cisco para e-mails não solicitados e indesejados, como spam, vírus e phishing.

- O botão Não é spam pode reclassificar rapidamente mensagens de e-mail legítimas marcadas como spam.

Note: Siga as próximas instruções se não conseguir ou preferir não instalar o plug-in do Cisco Email Security.

Microsoft Outlook Web App, Microsoft Office 365

1. Abra sua caixa de correio no Microsoft Outlook Web App.
2. Selecione a mensagem que deseja enviar.
3. Clique em "Novo email" na parte superior esquerda.
4. Arraste a mensagem e solte-a como um anexo para a nova mensagem.
5. Envie a mensagem de email para o respectivo endereço fornecido neste documento.

Microsoft Outlook 2011 e Microsoft Outlook 2016 para Mac (OS X, macOS)

1. Selecione a mensagem no painel de mensagens.
2. Clique no botão Anexo.
3. Encaminhe a mensagem para o respectivo endereço fornecido neste documento.

Correio (OS X, macOS)

1. Clique com o botão direito do mouse na própria mensagem de e-mail e escolha **Encaminhar como anexo**.
2. Encaminhe a mensagem de e-mail para o respectivo endereço fornecido neste documento.

Thunderbird Mozilla

1. Clique com o botão direito do mouse na própria mensagem de e-mail e escolha **Encaminhar como > Anexo**.
2. Encaminhe a mensagem de e-mail para o respectivo endereço fornecido neste documento.

Note: MailSentry IronPort Spam Reporter é um plugin de terceiros para Mozilla Thunderbird que toma a mesma ação como descrito, mas fornece um botão "Spam/Ham". **MailSentry IronPort Spam Reporter não é um plugin suportado da Cisco.**

Plataformas móveis (iPhone, Android ou outro)

- Se sua plataforma móvel não tiver um método para encaminhar o e-mail original como um anexo, envie-o assim que tiver acesso a um dos outros métodos fornecidos.

Como verificar envios à Cisco

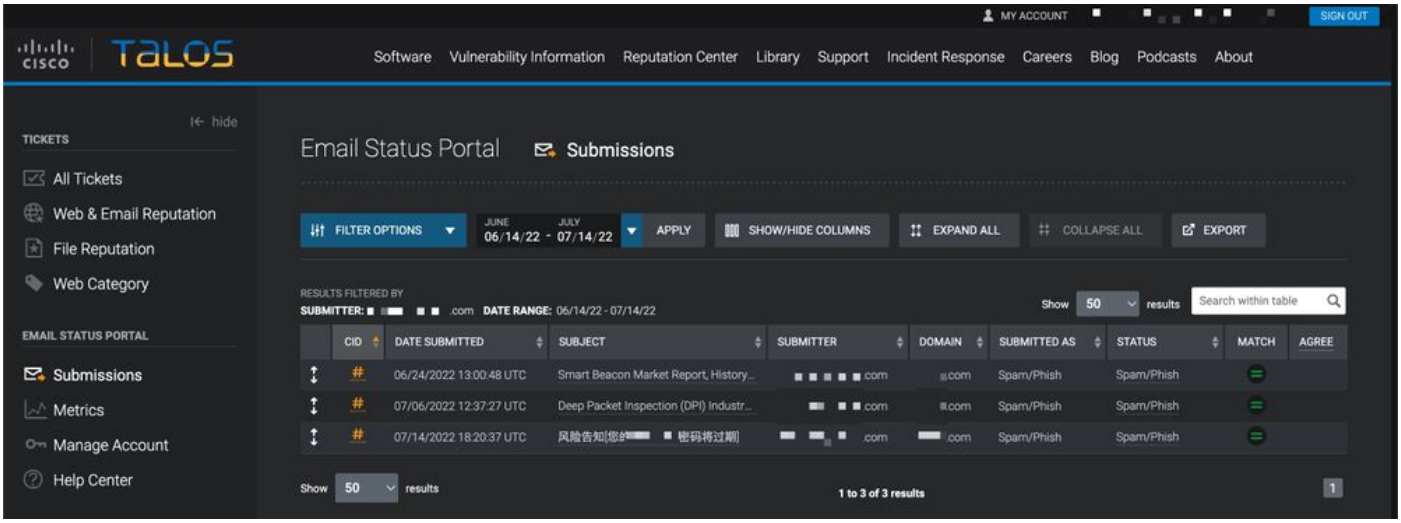
Envio de mala direta

A Cisco não fornece um e-mail de confirmação ou aviso de recebimento para envios por e-mail. Em vez disso, visualize seus envios por meio do Portal de status de e-mail hospedado em Talosintelligence.com.

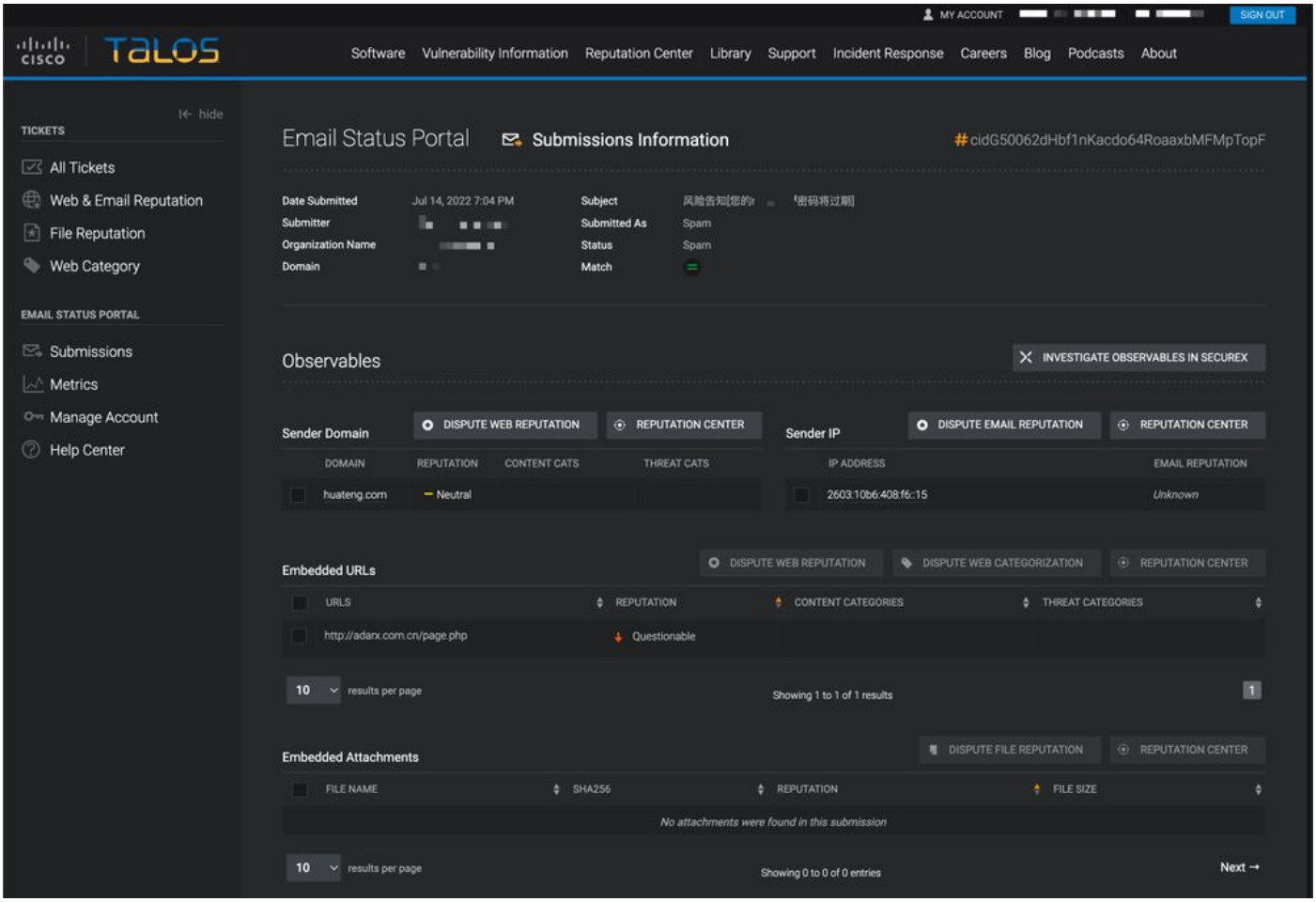
Portal de status de e-mail

Valide seus envios do Portal de status de e-mail. Após fazer login, você recebe uma lista de todos os seus envios dentro do intervalo de data/hora especificado.

Exemplo:



Se você clicar no CID exclusivo "#", poderá ver mais detalhes associados ao e-mail relatado.



Você verá os campos Domínio do remetente, IP do remetente, URLs incorporados e Anexos incorporados associados ao e-mail relatado. Você pode tomar outras medidas com **Dispute Web Reputation**, **Dispute Email Reputation** e **Dispute File Reputation**.

Cada linha de informação aninhada mostra um máximo de 5 observáveis de URLs incorporados e anexos incorporados. Se um envio de e-mail tiver mais observáveis, um usuário poderá clicar em "Ir para a página de detalhes do envio de e-mail" para ver a lista completa de observáveis extraídos.

Você pode pesquisar mais detalhes de reputação de um único observável com o observável desejado e, em seguida, clicar no botão "Centro de reputação".

Você também pode investigar vários observáveis via SecureX. Esse painel combina dados de reputação do conjunto completo de produtos Cisco Secure com base no portfólio de produtos da Cisco. Você pode selecionar até 20 observáveis de um único envio para investigar no SecureX de uma vez com o botão 'Investigar observáveis no SecureX'.

Os usuários podem arquivar uma única Disputa de reputação (Web, e-mail ou arquivo) ou aplicar disputas em massa para um ou mais de cada um dos itens observáveis em um envio. URLs e domínios também podem ter Disputas de categorização da Web arquivadas contra eles.

Para obter mais informações sobre o Portal de status de e-mail: https://talosintelligence.com/tickets/email_submissions/help

Additional Information

Documentação do Cisco Secure Email Gateway

- Notas de versão
- Guia do usuário
- Guia de referência CLI
- Guias de programação de API para Cisco Secure Email Gateway
- Fonte aberta usada no Cisco Secure Email Gateway
- Guia de instalação do Cisco Content Security Virtual Appliance(inclui Virtual Cloud Gateway)

Documentação do Secure Email Cloud Gateway

- Notas de versão
- Guia do usuário

Documentação do Cisco Secure Email and Web Manager

- Notas de versão e matriz de compatibilidade
- Guia do usuário
- Guias de programação de API para Cisco Secure Email e Web Manager
- Guia de instalação do Cisco Content Security Virtual Appliance(inclui Virtual Email e Web Manager)

Documentação do produto Cisco Secure

- Arquitetura de nomenclatura do portfólio Cisco Secure