Rapport Spam, verkeerd geclassificeerd, virtuele e-mailberichten

Inhoud

Inleiding

In dit document worden de volgende e-mails naar Cisco verzonden, verkeerd geclassificeerd, virtueel of extra e-mails naar Cisco voor ondersteuning of onderzoek.

Typen e-mailberichten

E-mailberichten met boodschappen over spam, Ham en marketing zijn:

- *Spam*: Onrelevante of ongeschikte e-mailberichten aan een ontvanger.
- *Ham*: Een e-mailbericht dat niet Spam is. Of, "niet-spam", "goede post".
- *Verhandeling*: Direct marketing van een commercieel e-mailbericht.

Cisco accepteert inzendingen voor elke e-mail die onjuist is geclassificeerd:

- fout-negatief (gemiste Spam)
- vals-positief (of "Ham")
- valse negatieve marketingberichten
- vals-positieve marketingberichten
- met phishing verdachte berichten, met phish-positieve berichten
- van het virus verdachte, viruspositieve berichten

Waarom zou u e-mails naar Cisco melden?

Gemiste of niet correct gemarkeerde e-mailberichten die aan Cisco zijn gerapporteerd met contentbevestiging, algemene werkzaamheid en bijbehorende regels en scores. Nadat u een e-mail naar Cisco hebt verzonden, kunt u ook aanvullende waarnemingen en ingesloten bijlagen bekijken via het E-mailstatusportal.

E-mailstatusportal

Met een geldig CCO-id kunt u inloggen op https://talosintelligence.com/tickets/email_submissions. De e-mailstatusportal is een tool om de status van uw e-mailberichten naar Cisco te bekijken. Cisco moedigt inzendingen van spam/phish aan die de huidige detectie-inhoud omzeilden en Ham, wenselijke e-mail die niet correct gefilterd werd, om de algehele effectiviteit te verbeteren. De e-mailstatusportal is een manier om de status van deze inzendingen te volgen. U kunt uw inzendingen controleren en Domain Administrators of Domain Viewers kunnen alle inzendingen uit uw domein(en) controleren.

> **Opmerking**: De bestaande E-mailindienings- en Tracking Portal (ESTP) is sinds 1 september 2020 vervangen door de E-mailstatusportal, gehost door Talosintelligence.com.

E-mailberichten aan Cisco melden

Ondersteunde methoden zijn:

1. Cisco Secure e-mail-invoeging
   Ondersteunt Outlook (Windows, Mac en Web)
2. Cisco e-mail security plug-in Ondersteunt Outlook (alleen Windows)
3. Directe e-mailindiening van de eindgebruiker

Cisco Secure e-mail-invoeging

Cisco Secure Email Submission Add-in ondersteunt Microsoft Outlook voor Windows, Mac en Web. Zie "Ondersteunde configuraties voor Cisco Secure Email Encryption Service Add-in en

Cisco Secure Email Submission Add-in" in de Compatibiliteitstabel voor Cisco Secure E-mailencryptie Service om compatibiliteit voor uw versie van Outlook te garanderen.

Zie Cisco Secure Email Submission Add-in voor downloads en installeren van documentatie.

Cisco e-mail security plug-in

De plug-in van Cisco e-mail security ondersteunt alleen Microsoft Outlook op Windows. Zie "Ondersteunde configuraties voor Cisco Email Reporting Plug-in" in de Compatibiliteitstabel voor Cisco Secure E-mailencryptie Service om compatibiliteit voor uw versie van Outlook te garanderen.

> **Opmerking:** Oudere versies van de plug-in worden aangeduid als "IronPort Email Security Plug-in" of "Encryption plug-in voor Outlook". Deze versie van de stekker bevat zowel rapportage als encryptie. In 2017 heeft Cisco de services gescheiden en twee nieuwe versies uitgebracht van de Plug-in, "Email Reporting plug-in voor Outlook" en de "Email Encryption Plugin voor Outlook". Deze waren beschikbaar met een versie van 1.0.0.x.

Directe e-mail indiening

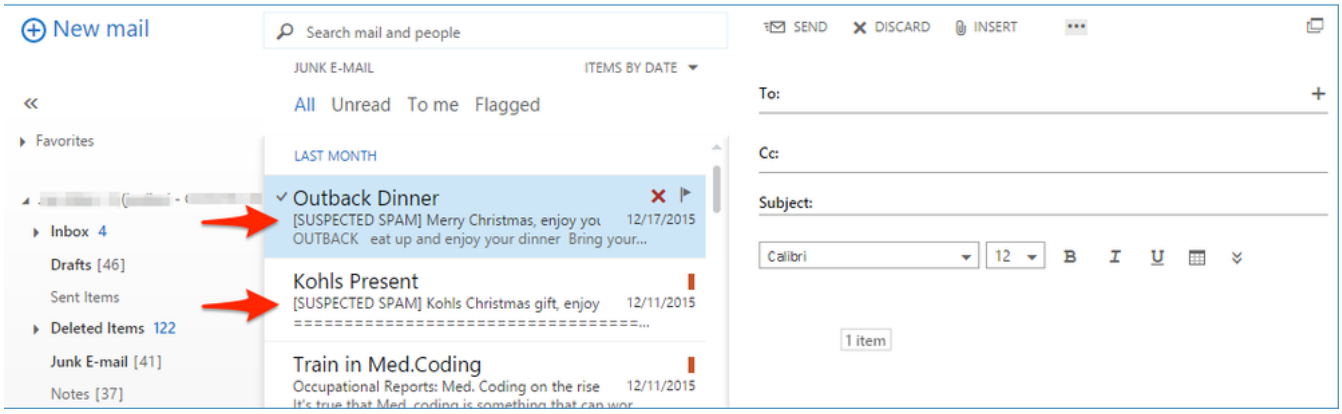
Volg de instructies voor uw e-mailclient die worden meegeleverd om de e-mail als een RFC 822 Multipurpose Internet Mail Extension (MIME) - gecodeerde bijlage aan te voegen. Als een van de voorbeelden uw e-mailcliënt niet weerspiegelt, verwijs dan direct naar uw e-mailgebruikershandleiding of productondersteuning en bevestig dat de e-mailcliënt "Doorsturen als bijlage ondersteunt."

Gelieve e-mailberichten te versturen naar het juiste e-mailadres:

spam@access.ironport.com	De eindgebruiker denkt dat het e-mailbericht spam of de onderwerpregel [VERDACH SPAM] bevat.
ham@access.ironport.com	De eindgebruiker beschouwt het e-mailbericht NIET als spam. De onderwerpregel be [SUSPECTED SPAM] of de onderwerpregel bevat extra tags.
ads@access.ironport.com	De eindgebruiker beschouwt het e-mailbericht als marketinginhoud of grijsmail, of de onderwerpregel bevat [MARKETING], [SOCIAL NETWERK] of [BULK].
not_ads@access.ironport.com	De eindgebruiker beschouwt het e-mailbericht NIET als marketing of grijsmail, of de onderwerpregel bevat [MARKETING], [SOCIAL NETWERK] of [BULK].
phish@access.ironport.com	Het e-mailbericht lijkt phish (bedoeld voor het verkrijgen van naam(en) van de gebrui wachtwoorden, informatie op de kredietkaart of andere persoonlijk identificeerbare informatie) of het e-mailbericht bevat bijlagen bij de software (ook bedoeld voor het verkrijgen van naam(en) of wachtwoorden). De onderwerpregel wordt voorgezet als [VERDACHTE SPAM], [Mogelijk $Threat_Category Fraud] of vergelijkbaar.
virus@access.ironport.com	De eindgebruiker beschouwt het e-mailbericht of een bijlage als viraal, of de onderwerpregel bevat [WAARSCHUWING: VIRUS HERKEND].

Niet alle onderwerpregel's bevatten extra tekst en tags. Raadpleeg voor uw instellingen uw Cisco Secure Email Gateway of Cloud Gateway-configuratie voor anti-spam, anti-virus, Graymail en Outbreak filters, of neem contact op met uw e-mailbeheerder als er problemen zijn.

Voorbeeld van gelabelde onderwerpregel:



Waarschuwing: Stuur je e-mailbericht niet door als inzending. Deze actie behoudt de volgorde van de mail-routing niet en verwijdert de benodigde kopregels voor het verzenden van e-mail die vereist zijn om de oorsprong van de e-mail aan te geven. In plaats daarvan, zorg er altijd voor dat u de betreffende e-mail verstuurt via de optie "verzenden als bijlage".

U kunt een e-mail rechtstreeks vanuit:

- Microsoft Outlook
- Microsoft Outlook-app, Microsoft Office 365
- Microsoft Outlook 2011 en Microsoft Outlook 2016 voor Mac (OS X, macOS)
- Mail (OS X, macOS)
- Mozilla Thunderbird
- Mobiele platforms (iPhone, Android of andere)

Microsoft Outlook

- De voorkeursmethode van Microsoft Outlook is om de Cisco Secure Email Submission Add-in te gebruiken.
- Stuur berichten naar Cisco voor ongevraagde en ongevraagde e-mails, zoals spam, virussen en phish.
- Met de knop Not Spam kan snel de legitieme e-mailberichten die gemarkeerd zijn als Spam, worden geherclassificeerd.

Opmerking: Volg de volgende instructies als u de Cisco e-mail security plug-in niet kunt of liever niet wilt installeren.

Microsoft Outlook-app, Microsoft Office 365

1. Open uw postvak in Microsoft Outlook-webapp.
2. Selecteer het bericht dat u wilt indienen.
3. Klik op "Nieuwe post" linksboven.
4. Sleep het bericht als een bijlage naar het nieuwe bericht.
5. Verzend het e-mailbericht naar het respectieve adres dat in dit document wordt opgegeven.

Microsoft Outlook 2011 en Microsoft Outlook 2016 voor Mac (OS X, macOS)

1. Selecteer het bericht in het deelvenster met berichten.
2. Klik op de knop Bijvoegen.
3. Het bericht doorsturen naar het respectieve adres dat in dit document is vermeld.

Mail (OS X, macOS)

1. Klik met de rechtermuisknop op het e-mailbericht zelf en kies **Voorwaarts als bijlage**.
2. Het e-mailbericht doorsturen naar het respectieve adres dat in dit document is vermeld.

Mozilla Thunderbird

1. Klik met de rechtermuisknop op het e-mailbericht zelf en kies **Voorwaarts als > Bijvoegen**.
2. Het e-mailbericht doorsturen naar het respectieve adres dat in dit document is vermeld.

Opmerking: MailSentry IronPort Spam Reporter is een derde partij plug-in voor Mozilla Thunderbird die de zelfde actie onderneemt als beschreven maar een "Spam/Ham"-knop geeft. **MailSentry IronPort Spam Reporter is geen ondersteunde plug-in uit Cisco.**

Mobiele platforms (iPhone, Android of andere)

- Als uw mobiele platform geen methode heeft om de oorspronkelijke e-mail als bijlage door te sturen, gelieve in te sturen als u toegang hebt tot een van de andere aangeboden methoden.

Hoe u opmerkingen aan Cisco kunt controleren

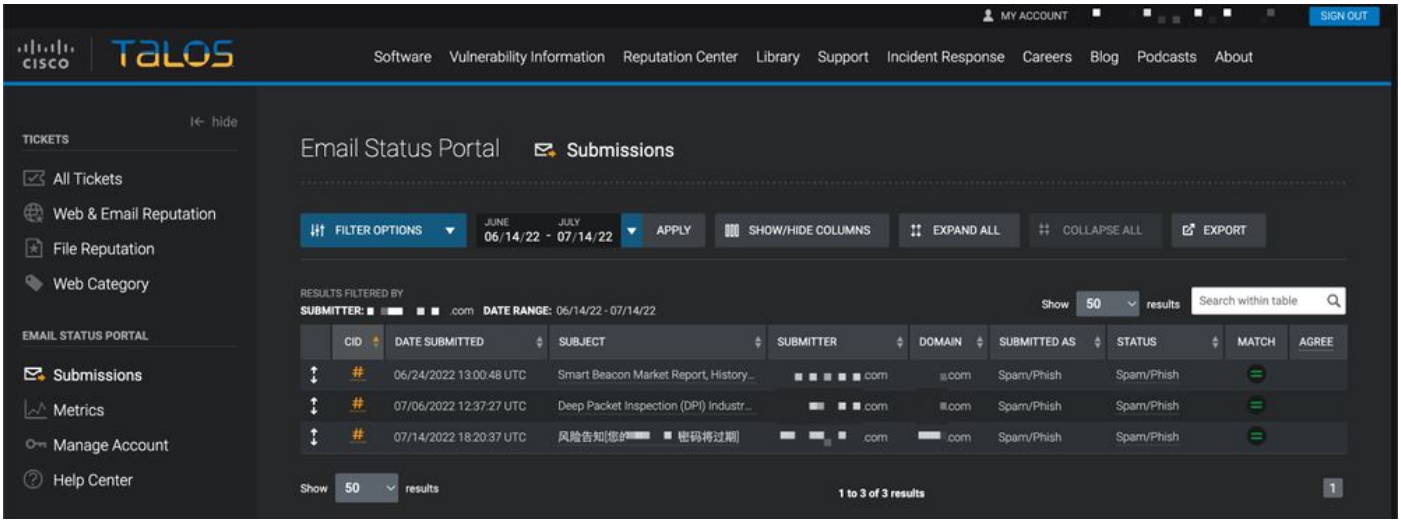
Directe e-mail indiening

Cisco geeft geen bevestigingse-mail of bericht van ontvangst voor e-mailberichten. Bekijk in plaats daarvan uw inzendingen via het e-mailstatusportaal op Talosintelligence.com.

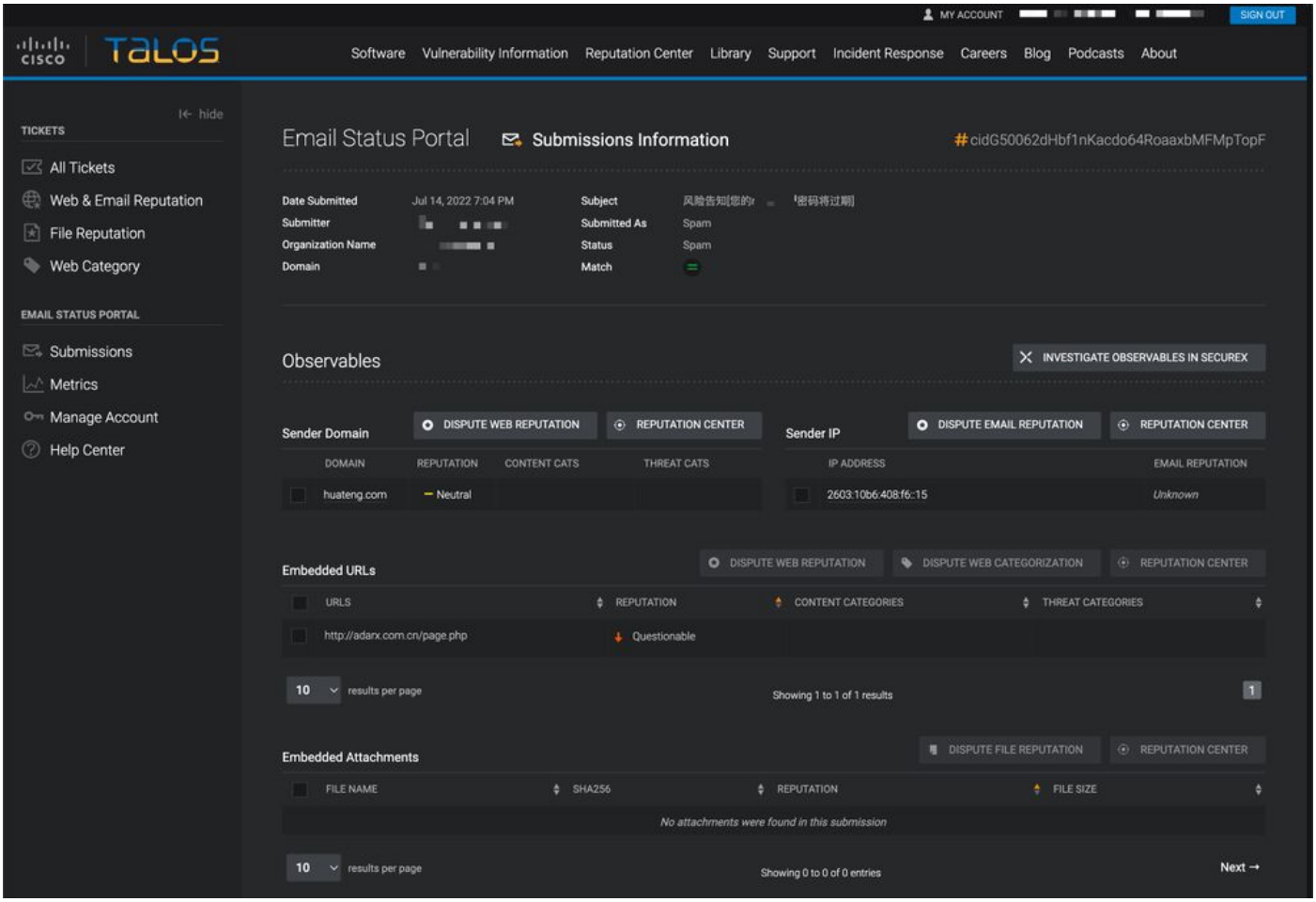
E-mailstatusportal

Bevestig uw inzendingen vanuit het E-mailstatusportaal. Nadat u hebt ingelogd, ontvangt u een lijst met al uw inzendingen binnen het opgegeven datumbereik.

Voorbeeld:



Als u op de unieke CID "#" klikt, kunt u verdere details zien geassocieerd met de gerapporteerde e-mail.



U wordt aangeboden met Sender Domain, Sender IP, Embedded URLs en Embedded Attachments die gekoppeld zijn aan de gerapporteerde e-mail. U kunt verdere actie ondernemen met **disute Web Reputation**, **Dispute Email Reputation** en **Dispute File Reputation**.

Elke geneste informatiestoets bevat maximaal 5 waarnemingen van ingesloten URL's en ingebedde bijlagen. Als een e-mailbericht meer observeermiddelen heeft, kan een gebruiker op de pagina 'Ga naar e-mail met details' klikken om de volledige lijst van geëxtraheerde waarnemingen te zien.

U kunt verdere reputatieschade opzoeken van één enkele waarneembaar met het gewenste waarneembare en dan op de knop "Herstelcentrum" klikken.

U kunt ook meerdere waarnemingen onderzoeken via SecureX. Dit dashboard combineert reputatiegegevens van de volledige reeks van Cisco Secure-producten die op uw Cisco-productportfolio zijn gebaseerd. U kunt maximaal 20 observabels selecteren uit één inzending die u in SecureX tegelijkertijd wilt onderzoeken met de knop 'Investigate obables in SecureX'.

Gebruikers kunnen één reproductievlag (web, e-mail of bestand) indienen of geschillen in bulk toepassen voor een of meer van elk waarneembaar op een inzending. Op URL's en domein kan ook een discussie over webcategorisering worden gestart.

Voor meer informatie over de E-mailstatusportal:
https://talosintelligence.com/tickets/email_submissions/help

Aanvullende informatie

Cisco beveiligde e-mailgateway-documentatie

- Release-opmerkingen
- Gebruikershandleiding
- CLI-referentiegids
- API-programmeerhandleidingen voor Cisco Secure E-gateway
- Open-bron gebruikt in Cisco Secure Email Gateway
- Cisco Content Security Virtual Appliance Installatie-gids (inclusief Virtual Cloud Gateway)

Documentatie over beveiligde e-mail cloudgateway

- Release-opmerkingen
- Gebruikershandleiding

Cisco Secure E-mail en Web Manager-documentatie

- Releaseopmerkingen en -compatibiliteitsmatrix
- Gebruikershandleiding
- API-programmeerhandleidingen voor Cisco Secure E-mail en Web Manager
- Cisco Content Security Virtual Appliance Installatie-gids (inclusief virtuele e-mail en Web Manager)

Cisco beveiligde productdocumentatie

- Cisco Secure-portefeuillenamarchitectuur