Segnala messaggi di posta indesiderata, classificati in modo erroneo, virali

Sommario

Introduzione

Questo documento descrive la segnalazione di posta indesiderata, classificata in modo erroneo, virus o altre e-mail a Cisco per il supporto o l'analisi.

Tipi di invio di messaggi di posta elettronica

Posta indesiderata, posta indesiderata e messaggi di marketing:

- *Posta indesiderata*: Messaggi e-mail non pertinenti o inappropriati inviati a un destinatario.
- *Prosciutto*: Messaggio di posta elettronica non indesiderato. Oppure "non-spam", "good mail".
- *Marketing*: Direttamente pubblicizzando un messaggio e-mail commerciale.

Cisco accetta invii per qualsiasi e-mail classificata in modo errato:

- false-negative (posta indesiderata)
- falso positivo (o "Prosciutto")
- messaggi di marketing falsi negativi
- messaggi di marketing falsi positivi
- messaggi sospetti di phishing, messaggi positivi di phishing
- messaggi di sospetto virus, virus positivi

Perché segnalare le e-mail a Cisco?

I messaggi e-mail mancanti o contrassegnati in modo errato vengono segnalati a Cisco per consentire di confermare il contenuto, l'efficacia complessiva, le regole e i punteggi associati. Dopo aver segnalato un'e-mail a Cisco, è possibile visualizzare altri elementi osservabili e allegati integrati tramite il portale di stato delle e-mail.

Portale stato posta elettronica

Se l'ID CCO è valido, è possibile accedere al sito https://talosintelligence.com/tickets/email_submissions. Il portale di stato della posta elettronica è uno strumento per visualizzare lo stato dei tuoi invii di posta elettronica a Cisco. Cisco incoraggia l'invio di posta indesiderata/phishing che ignorano il contenuto di rilevamento corrente e Ham, e-mail desiderabili che sono state filtrate in modo errato, per migliorare l'efficacia complessiva. Il portale dello stato della posta elettronica consente di tenere traccia dello stato di questi invii. È possibile monitorare gli invii e gli amministratori di dominio o i visualizzatori di dominio possono monitorare tutti gli invii dai domini.

> **Nota**: a partire dal 1° settembre 2020, il precedente portale di invio e verifica delle e-mail (ESTP) è stato sostituito dal portale di stato delle e-mail, disponibile su Talosintelligence.com.

Come segnalare i messaggi e-mail a Cisco

I metodi supportati sono:

1. Componente aggiuntivo per l'invio di e-mail sicure Cisco
   Supporta Outlook (Windows, Mac e Web)
2. Plug-in Cisco Email Security Supporta Outlook (solo Windows)
3. Invio diretto di e-mail dall'utente finale

Componente aggiuntivo per l'invio di e-mail sicure Cisco

Il componente aggiuntivo per l'invio di e-mail sicuro di Cisco supporta Microsoft Outlook per Windows, Mac e Web. Per garantire la compatibilità con la versione di Outlook in uso, vedere la sezione "Configurazioni supportate per i componenti aggiuntivi Cisco Secure Email Encryption Service e Cisco Secure Email Submission" nella matrice di compatibilità per i servizi Cisco Secure Email Encryption.

Vedere il componente aggiuntivo Cisco Secure Email Submission per scaricare e installare la documentazione.

Plug-in Cisco Email Security

Il plug-in Cisco Email Security supporta solo Microsoft Outlook su Windows. Vedere "Configurazioni supportate per il plug-in Cisco Email Reporting" nella matrice di compatibilità per il servizio Cisco Secure Email Encryption per garantire la compatibilità con la versione di Outlook in uso.

> **Nota:** Le versioni precedenti del plug-in sono denominate "IronPort Email Security Plug-in" o "Encryption Plug-in for Outlook". Questa versione del plug-in contiene sia Reporting che Encryption. Nel 2017, Cisco ha separato i servizi e rilasciato due nuove versioni del plugin, "Email Reporting Plugin for Outlook" e "Email Encryption Plugin for Outlook". Queste versioni erano disponibili con la versione 1.0.0.x.

Invio diretto tramite posta elettronica

Seguire le istruzioni per il client di posta elettronica fornito per allegare l'e-mail come allegato con codifica MIME (RFC 822 Multipurpose Internet Mail Extension). Se uno degli esempi non riflette il client di posta elettronica, fare riferimento direttamente alla guida per l'utente del client di posta elettronica o al supporto tecnico e confermare che il client di posta elettronica supporta l'inoltro come allegato.

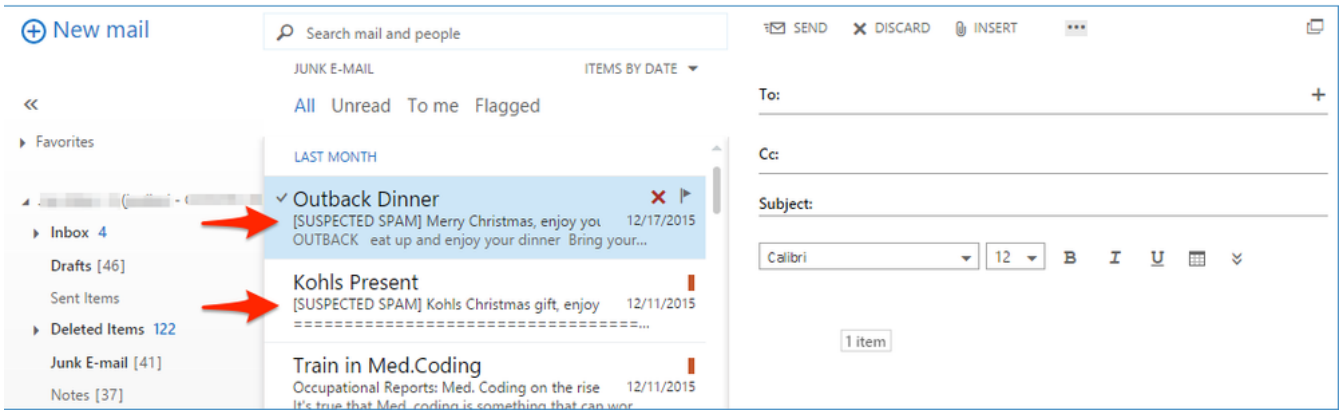
Inviare le e-mail da inviare all'indirizzo e-mail appropriato:

spam@access.ironport.com	L'utente finale considera il messaggio e-mail indesiderato o la riga dell'oggetto contie [SUSPECTED SPAM] (SOSPETTO SPAM).
ham@access.ironport.com	L'utente finale NON considera il messaggio e-mail come posta indesiderata. La riga dell'oggetto contiene [SUSPECTED SPAM] (SOSPETTO SPAM) oppure include tag aggiuntivi.
ads@access.ironport.com	L'utente finale considera il messaggio di posta elettronica come contenuto di marketi posta grigia o la riga dell'oggetto include [MARKETING], [SOCIAL NETWORK] o [BU
not_ads@access.ironport.com	L'utente finale NON considera il messaggio di posta elettronica come messaggio di marketing o di grigi, oppure la riga dell'oggetto contiene [MARKETING], [SOCIAL NETWORK] o [BULK].
phish@access.iron	Il messaggio e-mail sembra essere un phishing (progettato per acquisire nomi utente

port.com	password, informazioni sulla carta di credito o altre informazioni che consentono l'identificazione personale dell'utente) oppure contiene allegati malware (progettato a stesso modo per acquisire nomi utente o password). La riga dell'oggetto viene antep [SUSPECTED SPAM] (SOSPETTO SPAM), [Possible $threat_category Fraud] (Poss frode $threat_category) o simili.
virus@access.iron port.com	L'utente finale considera il messaggio e-mail o un allegato virale oppure la riga dell'o contiene [AVVISO: RILEVATO VIRUS].

Non tutte le righe dell'oggetto contengono testo e tag aggiuntivi. Per le impostazioni, consultare la configurazione di Cisco Secure Email Gateway o Cloud Gateway per i filtri antispam, antivirus, Graymail ed epidemie, o contattare l'amministratore della posta elettronica per qualsiasi problema.

Esempio di oggetto con tag:



Avviso: Non "Inoltrare" il messaggio e-mail come invio. Questa azione non mantiene l'ordine delle intestazioni di routing della posta e rimuove le intestazioni di routing della posta necessarie per attribuire l'origine del messaggio e-mail. Al contrario, accertati di inviare sempre l'e-mail in questione tramite l'opzione "inoltro come allegato".

Puoi inviare un'email direttamente da:

- Microsoft Outlook
- Microsoft Outlook Web App, Microsoft Office 365
- Microsoft Outlook 2011 e Microsoft Outlook 2016 per Mac (OS X, macOS)
- Posta (OS X, macOS)
- Mozilla Thunderbird
- Piattaforme mobili (iPhone, Android o altro)

Microsoft Outlook

- Il metodo di invio preferito da Microsoft Outlook consiste nell'utilizzare il componente aggiuntivo Invio posta elettronica sicuro di Cisco.
- Inviare messaggi a Cisco per ricevere e-mail non richieste o indesiderate, ad esempio posta indesiderata, virus e phishing.
- Il pulsante Non inviare posta indesiderata consente di riclassificare rapidamente i messaggi di posta elettronica legittimi contrassegnati come posta indesiderata.

Nota: Se non è possibile o non si preferisce installare il plug-in Cisco Email Security, attenersi alle istruzioni riportate di seguito.

Microsoft Outlook Web App, Microsoft Office 365

1. Apri la cassetta postale in Microsoft Outlook Web App.
2. Selezionare il messaggio che si desidera inviare.
3. Fare clic su "New mail" in alto a sinistra.
4. Trascinare il messaggio e rilasciarlo come allegato al nuovo messaggio.
5. Invia il messaggio di posta elettronica all'indirizzo fornito nel documento.

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

1. Selezionare il messaggio nel riquadro dei messaggi.
2. Fare clic sul pulsante Allegato.
3. Inoltra il messaggio all'indirizzo fornito nel presente documento.

Posta (OS X, macOS)

1. Fare clic con il pulsante destro del mouse sul messaggio e-mail e scegliere **Inoltra come allegato**.
2. Inoltra il messaggio e-mail all'indirizzo fornito nel presente documento.

Mozilla Thunderbird

1. Fare clic con il pulsante destro del mouse sul messaggio e-mail e scegliere **Inoltra come > Allegato**.
2. Inoltra il messaggio e-mail all'indirizzo fornito nel presente documento.

Nota: MailSentry IronPort Spam Reporter è un plug-in di terze parti per Mozilla Thunderbird che esegue la stessa azione descritta ma fornisce un pulsante "Spam/Ham". **MailSentry IronPort Spam Reporter non è un plug-in supportato da Cisco.**

Piattaforme mobili (iPhone, Android o altro)

- Se la piattaforma mobile non dispone di un metodo per inoltrare l'e-mail originale come allegato, inviarla dopo aver avuto accesso a uno degli altri metodi forniti.

Come verificare gli invii a Cisco

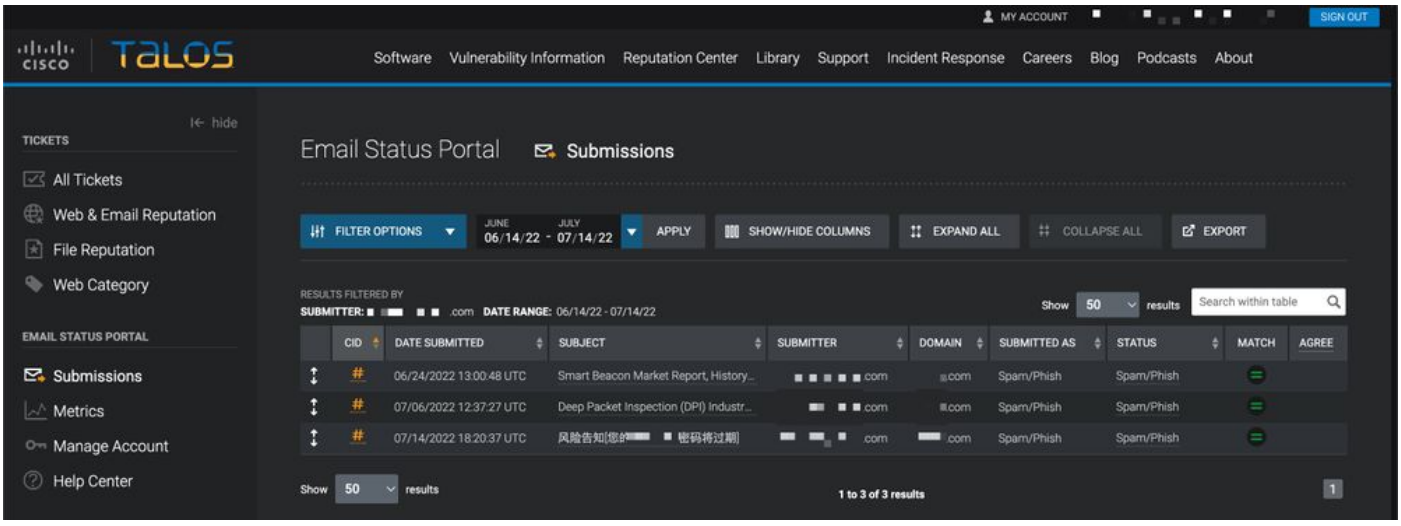
Invio diretto tramite posta elettronica

Cisco non fornisce una conferma tramite e-mail o un avviso di ricezione per l'invio di e-mail. Visualizza i tuoi invii tramite il portale di stato e-mail disponibile su Talosintelligence.com.

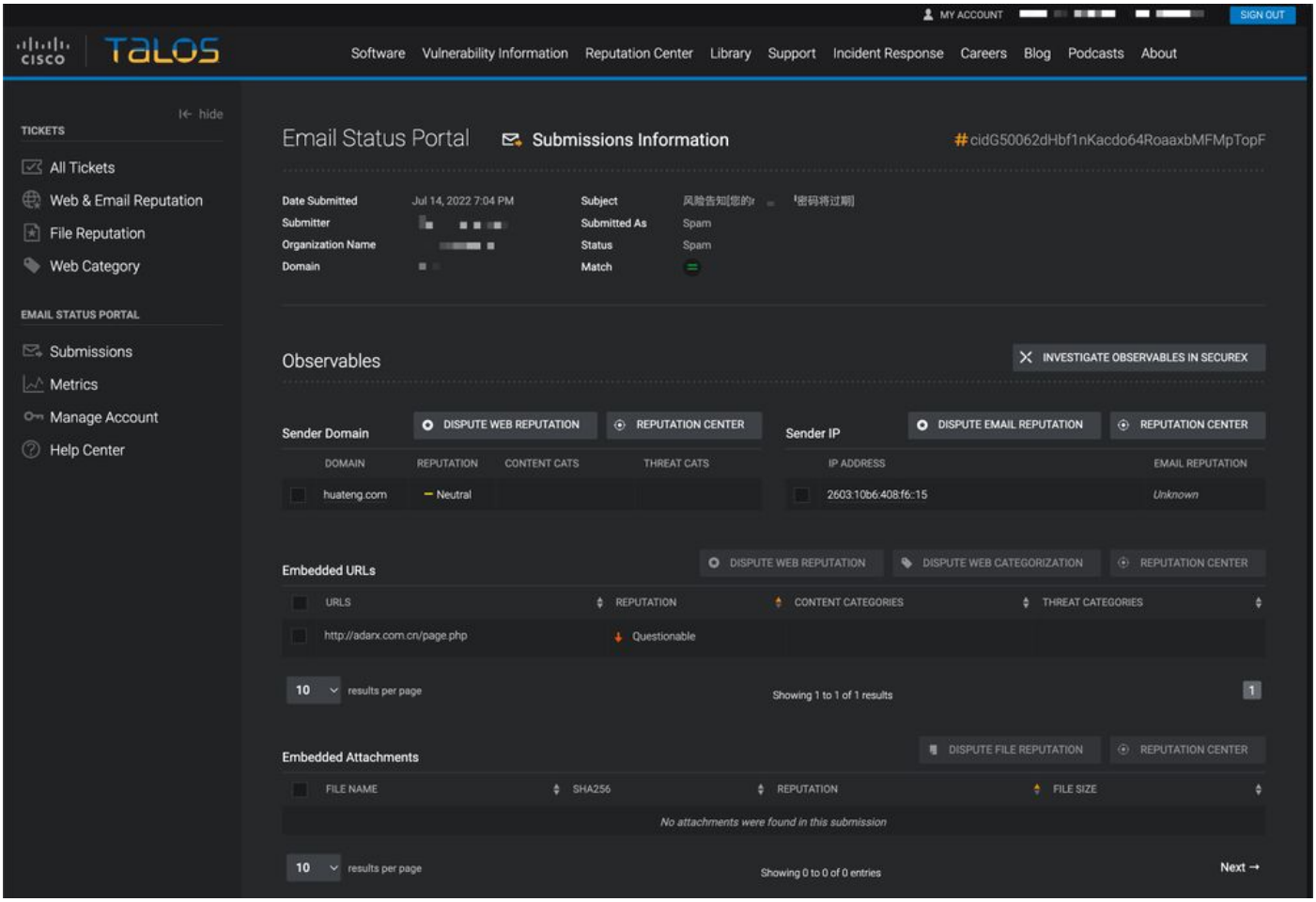
Portale stato posta elettronica

Convalidare i dati inviati dal portale dello stato della posta elettronica. Dopo aver eseguito l'accesso, verrà visualizzato un elenco di tutti gli invii compresi nell'intervallo di data/ora specificato.

Esempio:



Se clicchi sul CID univoco "#", puoi vedere ulteriori dettagli associati all'email segnalata.



Vengono visualizzati il dominio del mittente, l'IP del mittente, gli URL incorporati e gli allegati associati all'e-mail segnalata. Puoi intraprendere ulteriori azioni con la **reputazione Web della controversia**, la **reputazione dell'e-mail della controversia** e la **reputazione del file della controversia**.

In ogni riga di informazioni nidificate vengono visualizzati al massimo 5 elementi osservabili di URL incorporati e allegati incorporati. Se un inoltro e-mail ha più oggetti osservabili, un utente può fare clic su 'Vai a pagina dettagli invio e-mail' per visualizzare l'elenco completo degli oggetti osservabili estratti.

Puoi cercare ulteriori dettagli sulla reputazione di un singolo osservabile con l'osservabile desiderato e poi fare clic sul pulsante 'Centro di reputazione'.

Èinoltre possibile analizzare più oggetti osservabili tramite SecureX. Questo dashboard combina i dati della reputazione della suite completa di prodotti Cisco Secure in base al portafoglio di prodotti Cisco. È possibile selezionare fino a 20 osservabili da un singolo inoltro da analizzare in SecureX alla volta con il pulsante "Analizza osservabili in SecureX".

Gli utenti possono archiviare una singola Controversia relativa alla reputazione (Web, e-mail o file) o applicare le controversie in blocco per uno o più di ogni oggetto osservabile in un invio. Per gli URL e i domini è inoltre possibile che vengano aperte controversie di categorizzazione Web.

Per ulteriori informazioni sul portale dello stato della posta elettronica: https://talosintelligence.com/tickets/email_submissions/help

Ulteriori informazioni

Documentazione di Cisco Secure Email Gateway

- Note sulla release
- Guida dell'utente
- Guida di riferimento CLI
- Guide alla programmazione API per Cisco Secure Email Gateway
- Open Source utilizzato in Cisco Secure Email Gateway
- Guida all'installazione di Cisco Content Security Virtual Appliance (include Virtual Cloud Gateway)

Documentazione su Secure Email Cloud Gateway

- Note sulla release
- Guida dell'utente

Documentazione di Cisco Secure Email e Web Manager

- Note sulla versione e matrice di compatibilità
- Guida dell'utente
- Guide alla programmazione API per Cisco Secure Email e Web Manager
- Guida all'installazione di Cisco Content Security Virtual Appliance (include Virtual Email e Web Manager)

Documentazione del prodotto Cisco Secure

- Architettura di denominazione del portafoglio Cisco Secure