Descrizioni delle azioni del filtro messaggi ESA

Sommario

Introduzione

In questo documento vengono descritte le differenze tra le operazioni filtro messaggi drop-attachments-by-name, -type, -filetype e -mimetype su Cisco Email Security Appliance (ESA).

Panoramica dell'azione filtro messaggi

I messaggi inviati tramite MIME possono avere etichette assegnate a varie parti del corpo, che vengono spesso denominate allegati. Queste etichette possono essere in conflitto tra loro nelle informazioni che forniscono. Inoltre, una parte corpo può avere le proprie caratteristiche. Ad esempio, un utente può acquisire un'immagine JPEG, allegarla a un messaggio di posta, assegnarle un tipo MIME **testo/html** e contrassegnarla con un nome file MIME **jan.mp3**. Tutte queste etichette sono in conflitto con la realtà dell'allegato.

Si consideri ad esempio la seguente intestazione del messaggio:

```
Boundary_(ID_n6BU1raweF+4UwCeweFmVQ)
Content-type: application/msword; name="eval form.doc"
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename="eval form.doc"
Content-description: eval form.doc
```

In questo caso, i nomi di file MIME e i tipi MIME sono tutti coerenti e possono corrispondere o meno al formato effettivo della parte corpo (allegato). Tuttavia, in questa intestazione sono presenti incoerenze:

```
Boundary_(ID_n6BU1raweF+4UwCeweFmVQ)
Content-type: image/jpeg; name="eval form.doc"
Content-transfer-encoding: BASE64
Content-disposition: attachment; filename="evaluation.zip"
Content-description:  These are the latest warez, d00d.
```

Per messaggi ben formati, l'implementazione delle regole è abbastanza semplice. Ma nel caso in cui qualcuno, intenzionalmente o meno, cerchi di aggirare la politica, è necessaria maggiore flessibilità.

I gestori di rete spesso desiderano eliminare allegati di un particolare tipo, ad esempio tutti i file

MP3. Tuttavia, l'implementazione di questo criterio implica che è necessario decidere a quale delle etichette si desidera prestare attenzione (se presenti). AsyncOS offre la flessibilità di esaminare il tipo MIME (ad esempio *text/html*), il nome file MIME (ad esempio *jan.mp3*) e di *imprimere effettivamente* l'allegato per cercare di determinare il formato reale. Quando si implementano i criteri utilizzando filtri messaggi o filtri contenuti, è possibile utilizzare una o più di queste etichette.

Descrizioni delle azioni filtro messaggi

Descrizioni delle operazioni filtro messaggi:

- drop-attachments-by-name: controlla i nomi file di ciascun allegato in un messaggio per verificare se corrisponde all'espressione regolare specificata. Il nome del file viene ricavato dalle intestazioni MIME. Per questo confronto viene fatta distinzione tra maiuscole e minuscole. Se uno dei messaggi allegati corrisponde al nome del file, questa regola restituisce true. Se un allegato è un archivio, l'accessorio IronPort serie C raccoglierà i nomi dei file dall'interno dell'archivio e applicherà le regole di scanconfig (per impostazione predefinita, non vengono scansionati i tipi MIME di video/*, audio/* e immagine/* e non viene scansionato nulla oltre 5 MB).

- drop-attachments-by-type: elimina tutti gli allegati nei messaggi di tipo MIME, determinato dal tipo MIME specificato o dall'estensione del file. Gli allegati di file di archivio (zip, tar) verranno eliminati se contengono un file corrispondente.

- drop-attachments-by-filetype: esamina gli allegati in base all'impronta digitale del file e non solo all'estensione di tre lettere del nome del file. È simile al comando UNIX file. Oltre ai singoli tipi di file che è possibile specificare, le espressioni di gruppo Compressed, Document, Executable, Image e Media includono tutti i tipi di file del tipo generale. Ad esempio, il gruppo *Executable* include file con estensione exe, java, msi, pif, dll, scr e and.com. Per un elenco completo dei tipi di file che è possibile specificare, consultare la Guida dell'utente di AsyncOS.

- drop-attachments-by-mimetype - Elimina tutti gli allegati dei messaggi che hanno un determinato tipo MIME. Questa azione non tenta di determinare il tipo MIME per estensione di file, quindi non esamina il contenuto degli archivi.