ESA Berichtfilterbeschrijving

Inhoud

Inleiding

Dit document beschrijft de verschillen tussen de vervolgkeuzelijsten per naam, -type, -type en -type van het bericht en -type in de filterhandelingen van Cisco e-mail security applicatie (ESA).

Overzicht van berichtfilter

Berichten die met MIME worden verstuurd kunnen labels hebben toegewezen aan verschillende lichaamsdelen, die vaak als bijlagen worden genoemd. Deze labels kunnen (en doen) in strijd zijn met elkaar in de informatie die ze leveren. Daarnaast kan een lichaamsdeel zijn eigen kenmerken hebben. Een gebruiker kan bijvoorbeeld een JPEG-afbeelding maken, deze aan een e-mailbericht toevoegen, een MIME-type **tekst/html** geven en op de MIME-bestandsnaam **jan.mp3** plaatsen. Al deze labels staan in strijd met de realiteit van wat de bijlage is.

Denk bijvoorbeeld aan dit bericht:

```
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 dit geval zijn de MIME-bestandsnamen en MIME-typen allemaal consistent en komen ze mogelijk wel of niet overeen met het werkelijke formaat van het lichaamsdeel (bijlage). In deze header zitten echter inconsistenties:

```
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.
```

Voor goed gevormde boodschappen is het implementeren van beleid redelijk makkelijk. Maar in het geval van iemand die opzettelijk of onbedoeld probeert het beleid te omzeilen, is extra flexibiliteit nodig.

Netwerkmanagers willen vaak bijlagen van een bepaald type, zoals alle MP3-bestanden, laten

vallen. Maar het implementeren van dit beleid betekent dat je moet beslissen aan welke van de labels je aandacht wilt besteden (of een van hen). AsyncOS geeft u de flexibiliteit om het MIME-type (zoals *tekst/html*), de MIME-bestandsnaam (zoals *jan.mp3*) en de *vingerafdruk* van de bijlage te bekijken om te proberen vast te stellen wat het echte formaat is. Wanneer u uw beleid toepast met berichtfilters of contentfilters, kunt u een of meer van deze labels gebruiken.

Beschrijving van berichtfilter

Hier vindt u de beschrijvingen van de acties van het bericht filter:

- **vervolgkeuzelijsten per naam** - Hiermee controleert u de bestandsnamen van elke bijlage in een bericht om te zien of deze overeenkomt met de gegeven reguliere expressie. De bestandsnaam is afkomstig van de MIME-headers. Deze vergelijking is hoofdlettergevoelig. Als één van de berichtbijlagen de bestandsnaam aanpast, geeft deze regel **waar**. Als een bijlage een archief is, zal het apparaat van de IronPort C-Series de bestandsnamen van binnen het archief oogsten en de **scanconfiguratie** regels toepassen (standaard worden MIME-typen video/*, audio/* en afbeelding/* niet gescand, en er wordt niets meer dan 5 MB gescand) dienovereenkomstig.

- **vervolgkeuzelijsten per type** - druppelt alle bijlagen bij berichten met een MIME-type, bepaald door het gegeven MIME-type of de bestandsextensie. De bijlagen bij het archiefbestand (zip, tar) worden verbroken als ze een bestand bevatten dat overeenkomt met de inhoud.

- **drop-attachments-by-filetype** - onderzoekt bijlagen op basis van de vingerafdruk van het bestand en niet alleen de bestandsextensie met drie letters. Dit lijkt op de UNIX bestandsindeling. Naast de afzonderlijke bestandstypen die kunnen worden gespecificeerd, bevatten de groepsexpressies Compressed, Document, Execteerbaar, Afbeelding en Media alle bestandstypen van het algemene type. De *ExecCan* groep omvat bijvoorbeeld .exe, .java.msi.pif, .dll, .scr, en.com bestanden. Raadpleeg de AsyncOS-gebruikershandleiding voor een volledige lijst met bestandstypen die kunnen worden gespecificeerd.

- **vervolgkeuzelijsten per type** - druppelt alle bijlagen bij berichten met een bepaald MIME-type. Met deze actie wordt niet getracht het MIME-type door middel van bestandsextensie te achterhalen, zodat ook de inhoud van de archieven niet wordt onderzocht.