

Comment est-ce que je capture et bloque les hyperliens inclus qui ont des executables ?

Contenu

[Question](#)

[Réponse](#)

Question

Comment est-ce que je capture et bloque les hyperliens inclus qui ont des executables ?

Réponse

Vous pouvez utiliser un filtre de message pour balayer le corps et toutes les connexions HTML. Habituellement, ces emails entrés par l'intermédiaire des mails HTML. Pour que l'engine de lecture le détecte, vous devez utiliser corps-contient la condition. Si vous traitez seulement la messagerie sortante, alors vous pouvez utiliser « seulement-corps-contient » la condition.

Le filtre de message suivant recherchera n'importe quel hyperlien de longueur qui finit avec un exécutable. Une fois que la condition est remplie, deux actions lanceront. La première action sera d'informer l'administrateur local en envoyant un email à admin@example.com.

Le deuxième sera une mesure finale de relâcher l'email. L'email n'a pas besoin d'être baisse, mais à la place peut être mis en quarantaine. Enlevant l'action ci-dessous du « drop() ; » peut être remplacé par l'action « de la quarantaine (« stratégie ") ; ».

La quarantaine doit être définie, autrement l'engine de filtre ne permettra pas le filtre. Vous pouvez ou utiliser la quarantaine de stratégie par défaut, ou créez votre propre quarantaine (référez-vous s'il vous plaît aux quarantaines dans le manuel pour créer ou supprimer des quarantaines).

```
Block_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|\\$)")
{
  notify ("admin@example.com");
  drop();
}
```

Vous pouvez également utiliser cette version qui a retiré le mauvais URLs du corps et remplacé leur par l'URL RETIRÉ.

```
remove_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
edit-body-text("://\\S*\\.exe(\\s|\\b|$)", "URL REMOVED");
}
```

Pour des instructions de détail sur la façon dont entrer dans un filtre de message, passez en revue s'il vous plaît [comment j'ajoute un nouveau filtre de message à mon appliance d'IronPort Cisco ?](#)

Veillez se référer au GUIDE d'UTILISATEUR AVANCÉ de^{de} Cisco ESA AsyncOS pour que l'application de Policy appelée par section d'appareils de sécurité du courrier électronique passe en revue des filtres de message.