Come è possibile acquisire e bloccare i collegamenti ipertestuali incorporati che dispongono di file eseguibili?

Sommario

Domanda

Come è possibile acquisire e bloccare i collegamenti ipertestuali incorporati che dispongono di file eseguibili?

Risposta

Èpossibile utilizzare un filtro messaggi per analizzare il corpo e gli eventuali allegati HTML. In genere, queste e-mail vengono inviate tramite e-mail HTML. Affinché il motore di scansione possa rilevarlo, è necessario utilizzare la condizione body-contains. Se si elabora solo la posta in uscita, è possibile utilizzare la condizione 'only-body-contains'.

Il filtro messaggi seguente cercherà tutti i collegamenti ipertestuali lunghi che terminano con un eseguibile. Una volta soddisfatta la condizione, verranno attivate due azioni. La prima azione consiste nel notificare l'amministratore locale inviando un messaggio di posta elettronica a admin@example.com.

La seconda azione sarà l'eliminazione definitiva dell'e-mail. L'e-mail non deve essere eliminata, ma può essere messa in quarantena. La rimozione dell'azione seguente di '`drop();`' può essere sostituita con l'azione di '`quarantine('Policy');`'.

Ènecessario definire la quarantena, altrimenti il motore di filtro non consentirà il filtro. È possibile utilizzare la quarantena predefinita o creare una quarantena personalizzata (consultare le quarantene nel manuale per creare o eliminare le quarantene).

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

Èinoltre possibile utilizzare questa versione per rimuovere gli URL non validi dal corpo e sostituirli con URL REMOVE (RIMOSSO).

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

Per istruzioni dettagliate su come immettere un filtro messaggi, consultare How do I add a new message filter to my Cisco IronPort Appliance? (Come aggiungere un nuovo filtro messaggi all'accessorio Cisco IronPort).

Per la revisione dei filtri messaggi, consultare la sezione Cisco ESA AsyncOS ADVANCED USER GUIDE for Email Security Appliance (Applicazione delle policy).