Configure Filters to Mitigate against List Bomb (Subscription Email Bomb) Attacks

Contents

Introduction

This document describes how to configure message and content filters using regular expressions to mitigate email bomb attacks on your Cisco Secure Email Gateway (ESA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ESA
- AsyncOS

Components Used

The information in this document is based on all supported versions of AsyncOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

What is an Email Bomb attack?

An email bomb is a form of net abuse that sends large volumes of email to an address to overflow the mailbox, overwhelm the server where the email address is hosted in a denial-of-service attack (DoS attack) or as a smokescreen to distract the attention from important email messages indicative of a security breach.

List bomb attacks (aka subscription bomb, email cluster bomb) can be very disruptive to affected

users. Their inboxes fill up with a large volume of subscription confirmation messages, resulting in difficulty to find desired mail, sometimes overwhelming mail clients or exceeding mailbox quotas. Since the subscription confirmation messages (generally) come from legitimate sources and are sent in response to a sign-up action, Anti-Spam systems can't effectively defend against them without the risk of widespread false positives.

Use Regular Expressions (regex) to Find Body Matches

It is often desirable to cut down the volume delivered to the target's inbox so it remains operational without impact on the mail flow of unaffected users. A message or content filter is the recommended tool for this use case. The provided regular expressions are examples of what has worked well in the past to identify subscription confirmations:

```
(?i)(task=activat|click the confirmation|click on the confirmation|Confirm Subscription|confirm your subscription|Confirm my subscription|activate your subscription|If you did not sign up for|Gracias por suscribirse|cliquez pas sur le lien de confirmation|votre inscription|hiermit Ihre Newsletter-Registrierung|After activation you may|Benutzerkonto zu aktivieren|sie haben den Newsletter|Registrierung auf|start receiving the newsletter)
```

Based on the attack volume and the tolerance for FPs, additional generic terms such as in the following regular expression would help capture messages more aggressively:

```
(?i)(register|registr|subscri|suscri|inscri|confirm|aktiv|activ|newsletter|news.letter)
```

These regular expressions can be used in an **"only-body-contains"** message filter condition or in a **"Message Body > Contains text"** condition in a content filter. The filter can be set up to divert subscription confirmation messages to a different mailbox, a quarantine, or to add a header or subject tag that allows to move the message into a dedicated subfolder within the user's mailbox.

> **Caution**: Please note that these regular expressions are only examples and would have to be adjusted to reflect both, the type of attack seen, as well as account for your regular mail flow to minimize FPs. They are meant to provide some reference point to start with but come without any guarantees.

Message Filter Example

Message filters are created and managed through the CLI with the command **filters**.

For steps to create message filters, please refer to the article here. Sample message filter follows:

```
lab.esa01.local> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> new
Enter filter script. Enter '.' on its own line to end.
Email_Bomb: if (sendergroup != "RELAYLIST" and (only-body-contains("(?i)(task=activat|click the confirmation|click on the confirmation|Confirm Subscription|confirm your subscription|Confirm my subscription|activate your subscription|If you did not sign up for|Gracias por suscribirse|cliquez pas sur le lien de confirmation|votre inscription|hiermit Ihre Newsletter-Registrierung|After activation you may|Benutzerkonto zu aktivieren|sie haben den
```

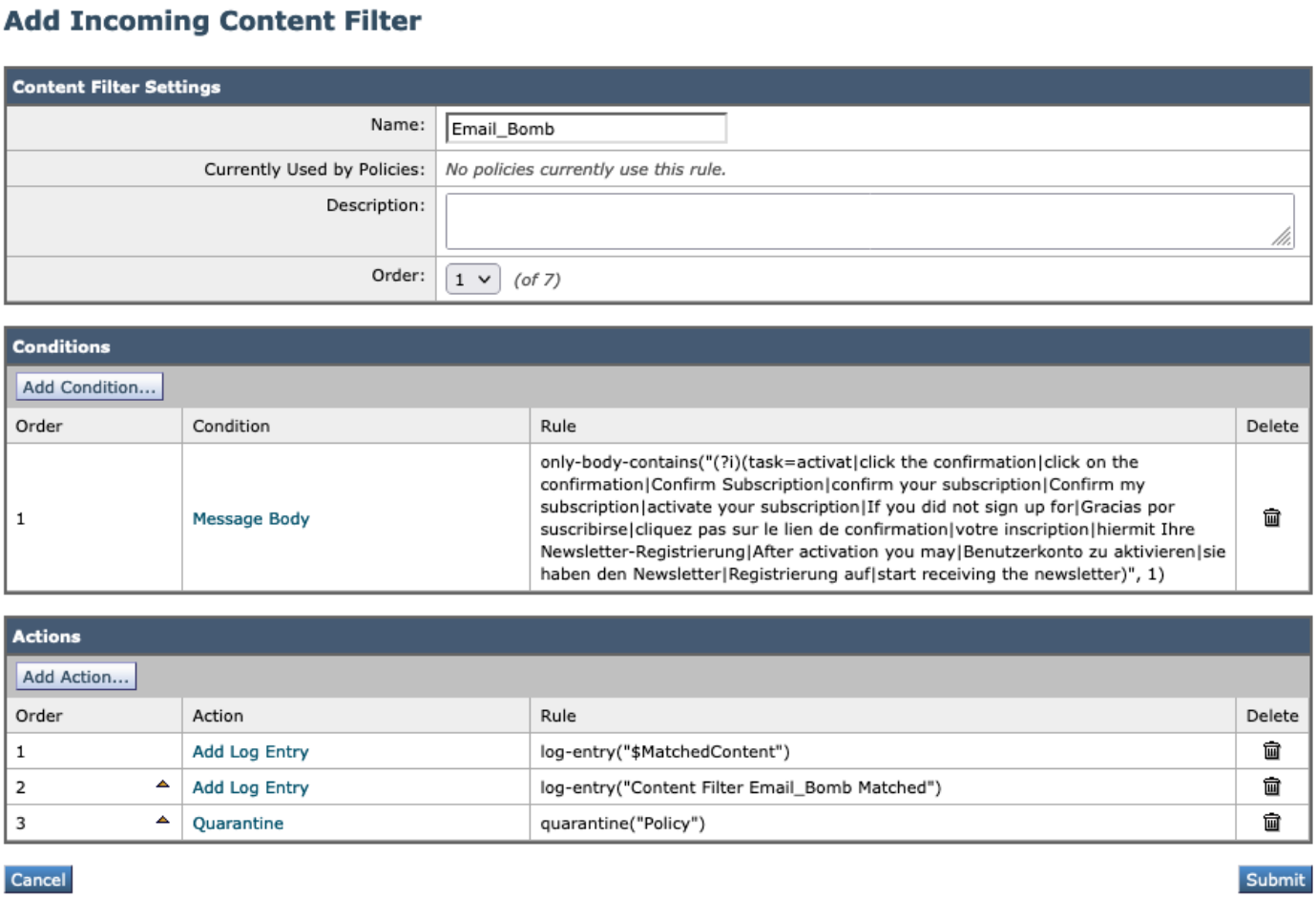
```
Newsletter|Registrierung auf|start receiving the newsletter)", 1))
{
log-entry("$MatchedContent");
log-entry("Message Filter Email_Bomb matched");
quarantine("Policy");
}
.
1 filters added.

lab.esa01.local> commit

Please enter some comments describing your changes:
[]> Added message filter

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Mon Jan 10 22:31:04 2022 EST
```

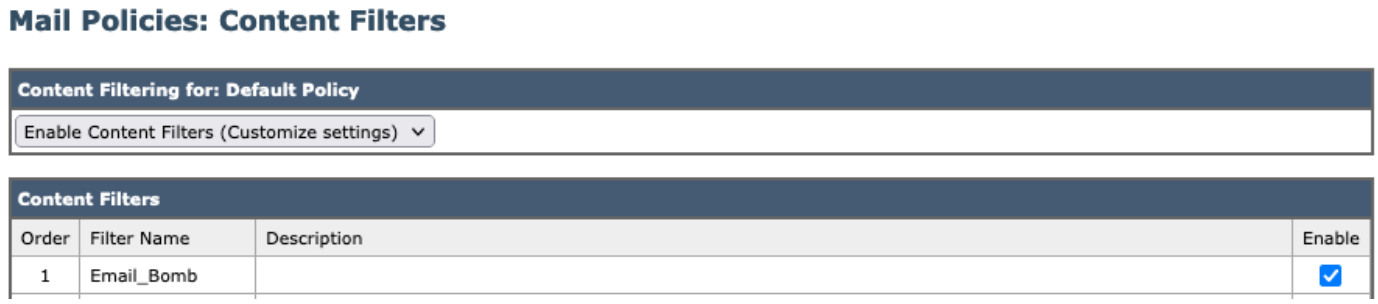
> **Note**: The sendergroup condition in the example is to prevent a filter match against relay/outbound emails. Additional conditions or modifications would be needed based on the device setup.

Incoming Content Filter Example

Content filters for incoming emails can be created directly from the GUI under **Mail Policies > Incoming Content Filters**.

1. Click Add Filter, enter a Filter name such as Email_Bomb.
2. Click Add Condition, select Message Body, radio button Contains text, enter regex you wish to match the email body against. Click Ok when done.
3. Click Add Action, select an action you wish to perform when the filter matches such as quarantine, Add/Edit Header, Notify, and so on. Click Ok when done.
4. Repeat Step 3 to add as many actions as needed, click Submit once done.
5. Navigate to Mail Policies -> Incoming Mail Policies, click the Content Filters column to checkmark and enable the new filter for one or multiple policies.
6. Submit and commit changes.





Note: "(?i)" in regular expressions indicates that the match must be case insensitive.

Related Information

- [Cisco Email Security Appliance - End-User Guides]
- [Working with Message Filters]
- [Best Practices Guide for Incoming and Outgoing Content Filters]
- [Technical Support & Documentation - Cisco Systems]