Troubleshoot Unwanted Outbound Emails on the ESA from Compromised Accounts

Contents

Introduction

This document describes how to troubleshoot and correct the queues on the Email Security Appliance (ESA) in an event that an internal user account has been compromised and sent out unsoliticited emails globally.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on AsyncOS 7.6 and later for ESA.

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.

Troubleshoot

It is advisable to lock down the account that sends the spam if it is known, otherwise lock down the account once discovered via the investigation on the ESA.

Workqueue Checks

When there is a large numbers of emails in the workqueue counter and the rate of emails that

enter the system far exceeds the rate that exit the system, this indicates that there is an impact on the workqueue. You can use the workqueue command to perform the check.

```
C370.lab> workqueue status

Status as of:  Thu Feb 06 12:48:02 2014 GMT
Status:        Operational
Messages:      48654

C370.lab> workqueue rate 5

Type Ctrl-C to return to the main prompt.

Time      Pending    In   Out
12:48:04    48654    48     2
12:48:09    48700    31     0
```

Sender or Subject of Emails in the Workqueue is Known

In order to remove the emails which impact the workqueue, the use of a message filter is recommended. The usage of a message filter will allow the ESA to action these emails at the beginning of the workqueue rather than the end in order to assist with the removal of the emails at a more efficient interval.

This filter can be used to achieve this:

```
C370.lab> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new

Enter filter script.  Enter '.' on its own line to end.

FilterName:
if (mail-from == 'abc@abc1.com')
{
drop();
}
.

OR

FilterName:
if (subject == "^SUBJECT NAME$")
{
drop();
}
.
```

Delivery Queue Check

The **tophosts** command will show the current impacted hosts. In a live environment you will see the recipient host (current active delivery queue) will be impacted with a large number of active recipient. For this output, the example is **impactedhost.queue**.

```
C370.lab> tophosts

Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]>  1

Status as of:                   Thu Feb 06 12:52:17 2014 GMT
Hosts marked with '*' were down as of the last delivery attempt.

                                Active  Conn.     Deliv.       Soft       Hard
#   Recipient Host              Recip.    Out     Recip.    Bounced    Bounced

1   impactedhost.queue          321550     50        440      75568       8984
2   the.euq.queue                    0      0          0          0          0
3   the.euq.release.queue            0      0          0          0          0
```

Should the impacted host be an unfamiliar recipient domain where further information is required before the removal of all emails, the commands **showreceipients**, **showmessage**, and **deleterecipients** can be used. The **showreceipients** command will display the Message ID (MID), Message Size, Delivery Attempts, Envelope Sender, Envelope Recipient(s), and the Subject of the email.

```
C370.lab> showrecipients

Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1

Please enter the hostname for the messages you wish to show.
> impactedhost.queue
```

In the event that the suspected MID in the delivery queue looks legitimate, you can use the **showmessage** command in order to display the message source before you take any action.

```
C370.lab> showmessage

Enter the MID to show.
[]>
```

Once confirmed as spam, in order to remove these emails, proceed and use the **deleterecipient** command. The command will provide three options for email deletion off the delivery queue; By Envelope Sender, By Recipient Host, or All emails in the delivery queue.

```
C370.lab> deleterecipients

Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 2

Please enter the Envelope From address for the messages you wish to delete.
[]>
```

Proactive Monitoring and Action

On version 9.0+ AsyncOS on the ESA, a new message filter condition called Header Repeats Rule is available.

Header Repeats Rule

The Header Repeats rule evaluates to true if at a given point in time, a specified number of messages:

- With the same subject are detected in the last one hour.
- From the same envelope sender are detected in the last one hour.
- header-repeats(<target>, <threshold> [, <direction>])

Further information on this condition is available in your device's Online Help Guide.

Log into the CLI and deploy the filter in order to run this check and action desired. An example filter to drop emails or notify an admin after a threshold is met.

```
C370.lab> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new

Enter filter script.  Enter '.' on its own line to end.

FilterName:
if header-repeats('mail-from',1000,'outgoing')
{
drop();
}
.
```

OR

```
FilterName:
if header-repeats('subject',1000,'outgoing')
{
notify('admin@xyz.com');
}
.
```

Related Information

- **ESA FAQ: How do I manually clear recipients from the email queue?**
- **Technical Support & Documentation - Cisco Systems**