Устраните неполадки нежелательных исходящих электронных почт на ESA от поставивших под угрозу учетных записей

Содержание

Введение

Этот документ описывает, как устранить неполадки и исправить очереди на Email Security Appliance (ESA) в событии, что учетная запись внутреннего пользователя поставилась под угрозу и отослана электронные почты unsoliticited глобально.

Используемые компоненты

Сведения в этом документе основываются на AsyncOS 7.6 для ESA и далее.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Устранение неисправностей

Желательно блокировать вниз, что учетная запись, передавая спам, если это известно, иначе блокируйте вниз учетную запись, однажды обнаруженную через расследование на ESA.

Проверки Workqueue

Когда существует, большие числа электронных почт в счетчике workqueue и скорости электронных почт, вводящих систему далеко, превышают скорость, выходящую из системы, это показательно, что существует влияние на workqueue. Можно использовать workqueue команду для выполнения проверки.

```
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
```

Отправитель или Предмет электронных почт в workqueue известны

Для удаления электронных почт, который влияет на workqueue использование фильтра сообщения рекомендуется. Использование фильтра сообщения позволит ESA действию эти электронные почты в начале workqueue, а не конца помогать с удалением электронных почт в более эффективном интервале.

Следующий фильтр может использоваться для достижения этого:

```
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(); } .
```

Проверка очереди доставки

tophosts команда покажет текущие затронутые хосты. В продуктивной среде вы будете видеть, что на хост получателя (текущая активная очередь доставки) повлияют с большим числом активного получателя. Для этих выходных данных примером является 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
```

Если затронутый хост является незнакомым доменом получателя, где дополнительная информация запрошена перед удалением всех электронных почт могут использоваться команды showreceipients, showmessage и deleterecipients. showreceipients команда отобразит Идентификатор сообщения (MID), Размер сообщения, Попытки Доставки, Отправитель Конверта, Получатель (получатели) Конверта и Предмет электронной почты.

```
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
```

Если подозреваемый MID в очереди доставки может выглядеть легитимным, можно использовать showmessage команду для отображения источника сообщения, прежде чем принято любые меры.

```
C370.lab> showmessage Enter the MID to show. []>
```

После того, как подтвержденный как спам, для удаления этих электронных почт, продолжаются и используют deleterecipient команду. Команда предоставит 3 возможности для почтового удаления от очереди доставки. Отправителем Конверта, Хостом Получателя или Всеми электронными почтами в очереди доставки.

```
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. []>
```

Упреждающий контроль и действие

На версии 9.0 + AsyncOS на ESA, новое условие фильтра сообщения под названием Правило Повторений Заголовка доступно.

Правило повторений заголовка

Правило Повторений Заголовка оценивает к истине если в данный момент времени, заданный номер сообщений:

- С тем же предметом обнаружены за прошлый один час.
- От того же конверта отправитель обнаружены за прошлый один час.
- повторения заголовка (<цель>, <порог> [<направление>])

Дополнительная информация об этом условии доступна в Онлайновом Руководстве Справки вашего устройства.

Войдите в CLI и разверните фильтр для осуществления этой проверки и желаемого действия.

Фильтр в качестве примера, чтобы отбросить электронные почты или уведомить admin после порога встречен.

```
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'); } .
```

Дополнительные сведения

- Часто задаваемые вопросы ESA: Как я вручную очищаю получателей от почтовой очереди?
- Cisco Systems – техническая поддержка и документация