ESA поддельная почтовая фильтрация

ID документа: 117796

Обновлено: 11 июня 2014

Внесенный Nasir Shakour, специалистом службы технической поддержки Cisco.

Родственные продукты

- Устройство безопасности электронной почты Cisco

Содержание

Введение

Этот документ описывает проблему, с которой встречаются в Cisco Email Security Appliance (ESA), когда спам и мошенническая электронная почта вводят в сеть. Возможные решения к этой проблеме также описаны.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- ESA Cisco
- AsyncOS

Используемые компоненты

Сведения в документе приведены на основе данных версий аппаратного и программного обеспечения:

- Все версии ESA Cisco
- Все версии AsyncOS

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.

Проблема

Мошенники пытаются явиться олицетворением электронной почты. То, когда электронная почта является олицетворением (подразумевает быть от), участник вашего штата компании, это может быть особенно обманчиво и имеет потенциал для порождения беспорядка. В попытке решить эту проблему, почтовые администраторы могли бы попытаться заблокировать входящую почту, которая, кажется, происходит из компании (*имитировавшая* почта).

Могло бы казаться логическим, что при блокировании входящей почты из Интернета, который имеет адрес возврата компании в доменном имени, это решает проблему. К сожалению, при блокировании почты таким образом она может также заблокировать легитимную электронную почту в то же время. Рассмотрите эти примеры:

- Сотрудник перемещается и использует интернет-провайдера (ISP) отеля, который прозрачно перенаправляет весь трафик Протокола SMTP к почтовым серверам интернет-провайдера. Когда почта передается, могло бы казаться, что это течет непосредственно через сервер SMTP предприятия, но это фактически передается через сторонний сервер SMTP, прежде чем это будет отправлено предприятию.

- Сотрудник подписывается на почтовый список рассылки. Когда сообщения передаются списку электронной почты, они возвращены всем абонентам, очевидно от инициатора.

- Внешняя система используется для мониторинга производительности или достижимости внешне видимых устройств. Когда предупреждение происходит, электронная почта имеет доменное имя компании в адресе возврата. Поставщики услуги от стороннего поставщика, такие как WebEx, делают это справедливо часто.

- Из-за ошибки конфигурации временной сети почта изнутри компании передается через входящего слушателя, а не исходящего слушателя.

- Кто-то за пределами компании получает сообщение, что они передают назад в компанию с Почтовым клиентом User Agent (MUA), который использует новые строки

заголовка, а не исходный заголовок.

- Интернет-приложение, такое как федеральные **страницы Экспресс-доставки** или Yahoo **посылает по электронной почте эту** страницу **статьи**, создает легитимную почту с адресом возврата, который указывает назад к компании. Почта легитимна и имеет адрес источника изнутри компании, но это не происходит изнутри.

Эти примеры показывают, что при блокировании входящей почты на основе информации домена она может привести к ошибочным допускам.

Решение

В этом разделе описываются рекомендованные действия, которые необходимо выполнить для решения этой проблемы.

Примените фильтры

Во избежание потери легитимных сообщений электронной почты не блокируйте входящую почту на основе информации домена. Вместо этого можно пометить строку темы этих типов сообщений, поскольку они вводят сеть, которая указывает получателю, что потенциально подделаны сообщения. Это может быть выполнено или с фильтрами сообщения или с фильтрами контента.

Базовая стратегия для этих фильтров должна проверить назад указанные строки заголовка тела (**От** данных, является самым важным), а также отправитель RFC 821 Конверта. Эти строки заголовка обычно показывают в MUAs и являются теми, которые, скорее всего, будут созданы мошенническим человеком.

Сообщение просачивается, следующий пример показывает, как можно пометить сообщения, которые потенциально явлены олицетворением. Этот фильтр выполняет несколько действий:

- Если строка темы уже имеет **"{Возможно Подделанный}"** в ней, то другая копия не добавлена фильтром. Это важно, когда ответы включены в поток сообщений, и строка темы могла бы несколько раз перемещаться через почтовый шлюз, прежде чем поток сообщения будет завершен.

- Этот фильтр ищет Отправителя Конверта или **От** заголовка, который имеет адрес, который заканчивается в доменном имени **@yourdomain.com**. Следует отметить, что почта - от поиска автоматически нечувствительна к регистру, но поиск *от заголовка* не. Если доменное имя найдено в любом местоположении, вставки фильтра **"{Возможно Подделанным}"** в конце строки темы.

Вот пример фильтра:

```
MarkPossiblySpoofedEmail:

   if ( (recv-listener == "InboundMail")      AND
        (subject != "\\{Possibly Forged\\}$") )
   {
       if (mail-from == "@yourdomain\\.com$") OR
```

```
        (header("From") == "(?i)@yourdomain\\.com$")
    {
        strip-header("Subject");
        insert-header("Subject", "$Subject {Possibly Forged}");
    }
}
```

Дополнительные меры

Поскольку нет никакого простого пути для определения имитировавшей почты от легитимной почты, нет никакого способа устранить проблему полностью. Поэтому Cisco рекомендует включить сканер защиты от спама IronPort (интегрированный с AsyncOS), который эффективно определяет мошенническую почту (фишинг) или спам и блокирует его положительно. Использование этого сканера для защиты от спама, когда вместе с фильтрами, описанными в предыдущем разделе, предоставляет лучшие результаты без потери легитимной электронной почты.

Если необходимо определить мошеннические электронные почты, которые входят сеть, то рассматривают использование технологии Доменных ключей определенной почты (DKIM); это требует более установленный, но это - хорошая мера против фишинга и мошеннических электронных почт. Технология DKIM полностью поддерживается в Версиях AsyncOS 5.5 и позже.

> **Примечание:** Для получения дополнительной информации о фильтрах сообщения, обратитесь к **Руководству пользователя AsyncOS** на Системной странице технической поддержки IronPort.

Связанные обсуждения Сообщества Cisco Support

Сообщество Cisco Support является форумом для вас, чтобы спросить и ответить на вопросы, общие предложения, и сотрудничать с вашими узлами.

Обновлено: 11 июня 2014
ID документа: 117796