Содержание

Введение

Этот документ описывает пять методов, что электронные почты спама могут ввести вашу организацию.

Методы

1. Легитимное сообщение / Торгующий Почтой

Легитимное сообщение было выбрано в пользователем, или их название было продано другой организации. В первом случае пользователь должен будет предпринять шаги для отмены подписки из списка. Если это - последний, отправьте сообщение снова spam@access.ironport.com, таким образом, определения для защиты от спама могут быть обновлены глобально, улучшив полную скорость захвата спама вашего ESA. Включение Торгующий почтой в политике Входящей почты может помочь изменять восприятие этого сообщения, являющегося "Торгующим" по "Спаму".

2. Защита от спама не обновляется правильно

Защита от спама отключена, или Характерная черта истекла. Чтобы проверить и видеть, обновляет ли Защита от спама, перейдите **к> Security GUI Сервисы> Защита от спама IronPort**. В этой панели необходимо видеть обновления наборов правил или механизма в течение прошлых 6 часов. Также из этой вкладки наверху можно гарантировать, что включен сервис Для защиты от спама. Для анализа статуса Характерной черты можно перейти к вкладке System Administration> Характерная черта для проверения статуса ключа Для защиты от спама.

3. Почтовая политика или сообщение фильтр

Если механизм безопасности Для защиты от спама отключен для определенного отправителя или получателя на Политику Почты клиента, спам может войти в вашу

организацию. Другой способ пропустить фильтрацию спама через фильтры сообщения (CLI: **фильтрует** команду).

4. Почтовая политика потока

Сообщение классифицировано с помощью ICID сообщения. В этой ситуации вероятно, что Характеристика безопасности Для защиты от спама выключена, который отвергает Почтовую Политику. Можно определить это путем рассмотрения почтовых журналов в журналах, которые необходимо будет сначала рассмотреть ICID для понимания, в который SenderGroup классифицировалось сообщение. Оттуда анализ связанной Почтовой Политики Потока. Если у вас есть большое количество записей в вашем WhiteList, вы, возможно, должны рассмотреть некоторые сообщения, которые входят, чтобы видеть, были ли они просмотрены механизмом AntiSpam. Откройте заголовки сообщения и ищите заголовок X-IronPort-Spam, присутствие этого заголовка означает, что сообщение действительно проходило механизм.

5. Сообщением является Спам

Сообщение является фактическим спамом. Вы подтвердили, что сообщение было просмотрено механизмом для защиты от спама, использующим функцию Отслеживания сообщений (в отслеживании сообщений, ищите "CASE"). Если вердикт случая отрицателен, и вы считаете сообщение, чтобы быть спамом, отправить исходное сообщение spam@access.ironport.com. Это могло быть случаем новой угрозы Спама, просто освобождаемой или более старой угрозы, которая была повторно спроектирована.

Обработка представлений Спама является и автоматическим и ручным процессом и нет никакого отзыва для вашего определенного представления. В любой точке можно связаться с Центром технической поддержки Cisco и запросить оценку и ответ.