Содержание

Введение

Этот документ описывает, как активировать опцию Предотвращения атаки урожая каталога (DHAP) на Cisco Email Security Appliance (ESA) для предотвращения Атак Урожая Каталога (DHAs).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- ESA Cisco
- AsyncOS

Используемые компоненты

Сведения в этом документе основываются на всех версиях 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.

Общие сведения

DHA является способом, который используется спаммерами для определения местоположения допустимых адресов электронной почты. Существует два основных метода, которые используются для генерации адресов, для которых предназначается DHA:

- Спаммер создает список всех возможных сочетаний букв и номеров, и затем добавляет доменное имя.

- Спаммер использует стандартный подбор пароля по словарю с созданием списка, который комбинирует общие имена, фамилии и начальные буквы.

DHAP является поддерживаемой характеристикой на Устройствах Безопасности содержания Cisco, которые могут быть включены, когда используется приемная проверка Протокола LDAP. Функция DHAP отслеживает количество недопустимых адресов получателя от данного отправителя.

Как только отправитель пересекает определенный порог администратора, отправитель, как считают, недоверяем, и почтовым от того отправителя заблокировано без генерации кода ошибки или Требований к организации сети (NDR). Можно настроить порог, основанный на репутации отправителя. Например, недоверяемые или подозрительные отправители могут иметь низкий порог DHAP и доверяли, или уважаемые отправители могут иметь высокий порог DHAP.

Включите DHAP

Для активации опции DHAP перейдите для **Отправки по почте Политики> таблица доступа к хосту (HAT)** от GUI Устройства Безопасности содержания и выберите **Mail Flow Policies**. Выберите политику, которую вы хотите отредактировать от столбца **Policy Name**.

HAT имеет четыре правила базового доступа, которые используются для реакции на соединения от удаленных хостов:

- **ACCEPT**: соединение принято, и почтовое принятие ограничено далее параметрами настройки слушателя. Это включает Таблицу Доступа Получателя (для общих слушателей).

- **ОТКЛОНЕНИЕ**: соединение первоначально принято, но клиент, который пытается соединиться, получает 4XX или 5XX приветствие. Никакая электронная почта не принята.

- **TCPREFUSE**: соединению отказывают на уровне TCP.

- **РЕЛЕЙНЫЙ**: соединение принято. Получение для любого получателя позволено и не ограничено Таблицей Доступа Получателя. Доменное подписание Ключей доступно только на релейной почтовой политике потока.

В **Почтовом Предельном** разделе **Потока** выбранной политики найдите и установите **Предотвращения атаки урожая каталога (DHAP)** путем установки

Необходимо повторить этот раздел для настройки DHAP для дополнительной политики.

Гарантируйте, что вы отправляете и передаете все изменения в GUI.

> **Примечание:** Cisco рекомендует использовать максимальное число между пять и десять для **Максимального числа недопустимых получателей в час до** значения **удаленного хоста**.

Примечание: Для дополнительных сведений обратитесь к **Руководству пользователя AsyncOS** на Портале поддержки Cisco.