Использование Network-Based Application Recognition и ACLs для блокирования вируса "Code Red"

Содержание

Введение

Этот документ предоставляет метод для блокирования червя "Code Red" в точках входа в сеть через Сетевое распознавание приложений (NBAR) и Списки контроля доступа (ACL) в программном обеспечении Cisco IOS на маршрутизаторах Cisco. Это решение должно использоваться в сочетании с рекомендуемыми пакетами исправлений для серверов IIS от Microsoft.

Примечание: Этот метод не работает на маршрутизаторы Cisco серии 1600.

Примечание: Некоторый трафик P2P не может быть полностью заблокирован из-за природы его протокола P2P. Эти протоколы P2P динамично изменяют свои подписи для обхода любой попытки механизмов DPI полностью заблокировать их трафик. Поэтому рекомендуется ограничить пропускную способность вместо того, чтобы полностью блокировать их. Отрегулируйте пропускную способность для этого трафика. Дайте намного меньше пропускной способности; однако, позвольте соединению пройти.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Политика обслуживания качества обслуживания (QoS) с помощью команд интерфейса командной строки (CLI) модульного QoS.
- NBAR
- ACL
- Маршрутизация на основе политик

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования. Конфигурация в этом документе была протестирована на Cisco 3640, который выполняет версию Cisco IOS 12.2 (24a)

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Как заблокировать червя "Code Red" Worm

Первая вещь, которую необходимо сделать для борьбы с "Code Red", применяют исправление, доступное от Microsoft (см. ссылки в Методе раздела A: Используйте ACL ниже). Это защищает уязвимые системы и удаляет червя из зараженной системы. Однако применение исправления к вашим серверам только препятствует тому, чтобы червь заразил серверы, это не мешает HTTP-запросам GET поразить серверы. Существует все еще потенциал для сервера, который будет засыпан лавинной рассылкой попыток заражения.

Решение, детализированное в этих информационных сообщениях, разработано для работы в сочетании с Исправлением от Microsoft для блокирования HTTP-запросов GET "Code Red" в точке входа в сеть.

Это решение пытается заблокировать заражение, однако это не исправит проблемы, вызванные наращиванием больших чисел записей в кэше, смежностей и записей NAT/PAT, так как единственный способ проанализировать содержание HTTP-запроса GET придерживается установления TCP - подключения. Следующая процедура не поможет защищать против просмотра сети. Однако это защитит узел от инвазии от внешней сети или сократит количество попыток заражения, которые должна обслужить машина. В сочетании с фильтрацией входящего потока фильтрация исходящего потока препятствует тому, чтобы зараженные клиенты распространили червя "Code Red" к глобальной сети Интернет.

Поддерживаемые платформы

Решение, описанное в этом документе, требует характеристики маркировки на основе класса в программном обеспечении Cisco IOS. В частности, возможность сопоставлять любую часть HTTP. Адрес URL использует механизм классификации суб-портов HTTP в границах распознавания сетевых приложений (NBAR). Поддерживаемые платформы и минимальные требования к программному обеспечению Cisco IOS приведены ниже:

Платформа	Минимальная версия ПО Cisco IOS
7200	12.1 (5) T
7100	12.1 (5) T
3745	12.2 (8) T
3725	12.2 (8) T
3660	12.1 (5) T
3640	12.1 (5) T
3620	12.1 (5) T
2600	12.1 (5) T
1700	12.2 (2) T

Примечание: Чтобы использовать NBAR, необходимо включить метод коммутации Cisco Express Forwarding (CEF).

Маркировка на основе классов и Распределенный NBAR (DNBAR) также доступны на следующих платформах:

Платформа	Минимальная версия ПО Cisco IOS
7500	12.1 (6) E
Flex WAN	12.1 (6) E

Найдите попытку заражения в веб-журналах IIS

Попытка первой попытки заражения передает большой HTTP-запрос GET к целевому серверу IIS. Исходное место "Code Red" показывают ниже:

```
2001-08-04 16:32:23 10.101.17.216 - 10.1.1.75 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u
7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403
```

"Code Red" II мест показывают ниже:

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090
%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%
u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403 -
```

Заметьте, что запрос GET всегда ищет файл с .ida расширением. Это - общая строка во всех попытках заражения и может поэтому использоваться в качестве условия соответствия

с маркировкой на основе классов в IOS. Остаток от запроса GET не обязательно будет последователен, поскольку это просто пытается создать переполнение буфера. Это может быть замечено путем сравнения этих двух записей выше.

Теперь сообщается, что различие между этими двумя подписями происходит из-за новой версии червя "Code Red", назвал CodeRed.v3 или CodeRed. C . В то время как новая версия содержит "XXXXXXXX", исходная деформация "Code Red" содержит строку "NNNNNNNN" в запросе GET. См. Справочное материалы по Symantec для получения дополнительной информации.

В 18:24 EDT, 6 августа 2001, мы сделали запись нового места. Мы с тех пор узнали, что это - место, которое оставлено позади сканером уязвимости eEye.

```
2001-08-06 22:24:02 10.30.203.202 - 10.1.1.9 80 GET /x.ida AAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X 403 HTTP/1.1 -
```

Способ для блокирования "Code Red", предоставленного в этих информационных сообщениях, может также заблокировать эти попытки сканирования просто путем сжатия определения схемы класса как показано в следующем разделе.

Отметить входящие попытки несанкционированного доступа кодовым красным цветом при помощи функции маркировки класса IOS

Для блокирования червя "Code Red" используйте один из этих трех методов, описанных ниже. Все три метода классифицируют вредоносный трафик, использующий функцию MQC Cisco IOS. Этот трафик тогда отброшен, как описано ниже.

Метод A: Использование ACL

Этот метод использует ACL на выходном интерфейсе для отбрасывания отмеченных пакетов "Code Red". Давайте использовать следующую схему сети для иллюстрирования шагов в этот метод:

Вот шаги в настройку этого метода:

1. Классифицируйте входящие взломы "Code Red" с характеристикой маркировки на основе класса в программном обеспечении Cisco IOS, как показано ниже:
```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*default.ida*"
Router(config-cmap)#match protocol http url "*cmd.exe*"
Router(config-cmap)#match protocol http url "*root.exe*"
```
Вышеупомянутая карта классов смотрит в HTTP URL и соответствиях любая из

заданных строк. Заметьте, что мы включали другие имена файлов помимо default.ida "Code Red". Можно использовать этот способ для блокирования подобных попыток несанкционированного доступа к системе, таких как Вирус sadmind, который объяснен в следующих документах:http://www.microsoft.com/technet/treeview/default.asp? URL =/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.html

2. Создайте политику и используйте команду **набора** для маркировки входящих взломов "Code Red" картой политик. Этот документ использует DSCP-значение 1 (в десятичном числе), так как маловероятно, что любой другой сетевой трафик несет это значение.Здесь мы отмечаем входящие взломы "Code Red" картой политик, названной "mark-inbound-http-hacks".
```
Router(config)#policy-map mark-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#set ip dscp 1
```
3. Примените политику как входящую политику на входном интерфейсе для маркировки поступающих пакетов "Code Red".
```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input mark-inbound-http-hacks
```
4. Настройте ACL, который совпадает на DSCP-значении 1, как установлено политикой обслуживания.
```
Router(config)#access-list 105 deny ip any any dscp 1
Router(config)#access-list 105 permit ip any any
```
Примечание: Cisco IOS Software Release 12.2 (11) и 12.2 (11) T представляют поддержку **регистрационного** ключевого слова на ACL в определении на картах классов для использования с NBAR (CSCdv48172). При использовании более раннего релиза не используйте **регистрационное** ключевое слово на ACL. Выполнение так вынуждает все пакеты быть процессной коммутацией вместо CEF-коммутируемого, и NBAR не будет работать, так как это требует CEF.
5. Примените выходные данные ACL на выходной интерфейс, который соединяется с конечными вебами - серверами.
```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```
6. Проверьте, что ваше решение работает как ожидалось. Выполните команду **show access-list** и гарантируйте, что инкрементно увеличивается значение "соответствий" для инструкции deny.
```
Router#show access-list 105
Extended IP access list 105
 deny ip any any dscp 1 log (2406 matches)
 permit ip any any (731764 matches)
```
В действии настройки можно также отключить передачу IP недостижимых сообщений ни с **какой IP недостижимой** командой interface-level, чтобы избежать заставлять маршрутизатор расходовать избыточные ресурсы.Если вы можете policy-route трафик DSCP=1 к Пустому 0, как описано в Методе B раздел, этот метод не рекомендуется.

Метод B: Использовать маршрутизацию на основе политик (PBR)

Этот метод использует маршрутизацию на основе политик для блокирования отмеченных пакетов "Code Red". Если методы A или C уже настроены, вы не должны применять команды в этом методе.

Вот шаги в реализацию этого метода:

1. Классифицируйте трафик и отметьте его. Используйте команды **команд class-map и policy-map**, показанные в методе A.
2. Используйте **команду service-policy** для применения политики как входящей политики на входном интерфейсе для маркировки поступающих пакетов "Code Red". См. метод A.
3. Создайте ACL расширенного IP, который совпадает на отмеченных пакетах "Code Red".`Router(config)#`**`access-list 106 permit ip any any dscp 1`**
4. Используйте **команду route-map** для построения политики маршрутизации.`Router(config)#`**`route-map null_policy_route 10`**
   `Router(config-route-map)#`**`match ip address 106`**
   `Router(config-route-map)#`**`set interface Null0`**
5. Примените route-map к входному интерфейсу.`Router(config)#`**`interface serial 0/0`**
   `Router(config-if)#`**`ip policy route-map null_policy_route`**
6. Проверьте, что ваше решение работает как ожидалось с командой **show access-list**. При использовании списки ACL для выходных данных и включили Регистрацию ACL, также можно использовать **команды show log**, как показано ниже:`Router#`**`show access-list 106`**

   ```
   Extended IP access list 106
    permit ip any any dscp 1 (1506 matches)

   Router#show log
   Aug 4 13:25:20: %SEC-6-IPACCESSLOGP:
    list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
   Aug 4 13:26:32: %SEC-6-IPACCESSLOGP:
    list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
   ```

   Мы в состоянии сделать решение о сбросе во входном интерфейсе маршрутизатора, вместо того, чтобы нуждаться в списке ACL для выходных данных на каждом исходящем интерфейсе. Снова, мы рекомендуем отключить передающие IP недостижимые сообщения с **командой no ip unreachables** команды.

Метод C: Использование политики на основе классов

Этот метод обычно является самым масштабируемым, поскольку он не зависит или от PBR или от списков ACL для выходных данных.

1. Классифицируйте трафик с помощью **команд class-map**, показанных в методе A.
2. Создайте политику с помощью **команды policy-map** и используйте команду **политики** для определения действия сброса для этого трафика.`Router(config)#`**`policy-map drop-inbound-http-hacks`**
   `Router(config-pmap)#`**`class http-hacks`**
   `Router(config-pmap-c)#`**`police 1000000 31250 31250`**
   `conform-action drop exceed-action drop violate-action drop`
3. Используйте **команду service-policy** для применения политики как входящей политики на входном интерфейсе для отбрасывания пакетов "Code Red".`Router(config)#`**`interface serial 0/0`**
   `Router(config-if)#`**`service-policy input drop-inbound-http-hacks`**

4. Проверьте, что ваше решение работает как ожидалось с **командой show policy-map interface**. Гарантируйте наблюдение инкрементно увеличивающихся значений для класса и отдельных условий соответствия.`Router#`**`show policy-map interface serial 0/0`**

```
Serial0/0

  Service-policy input: drop-inbound-http-hacks

    Class-map: http-hacks (match-any)
      5 packets, 300 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol http url "*default.ida*"
        5 packets, 300 bytes
        5 minute rate 0 bps
      Match: protocol http url "*cmd.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol http url "*root.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      police:
        1000000 bps, 31250 limit, 31250 extended limit
        conformed 5 packets, 300 bytes; action: drop
        exceeded 0 packets, 0 bytes; action: drop
        violated 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps

    Class-map: class-default (match-any)
      5 packets, 300 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Ограничения NBAR

При использовании NBAR с методами в этом документе обратите внимание, что следующие функции не поддерживаются NBAR:

- Обработка соответствий более 24 URL-адресов, сетевых узлов или MIME-типов одновременно
- Соответствие вне первых 400 байтов в URL
- Трафик протоколов, отличных от IP
- Режимы мультиадресной рассылки и другие режимы коммутации, не использующие технологию CEF
- Фрагментированные пакеты
- Постоянные конвейерные HTTP-запросы
- Классификация по URL-адресу, сетевому узлу, MIME-типу с помощью защищенного HTTP
- Асимметричные потоки с протоколами с отслеживанием состояний
- Пакеты, идущие от маршрутизатора с выполняющимся средством NBAR или направляющиеся к нему

Вы не можете настроить NBAR на следующих логических интерфейсах:

- Каналы Fast EtherChannel
- Интерфейсы, которые используют туннелирование или шифрование

- VLAN
- Интерфейсы номеронабирателя
- Multilink PPP

Примечание: NBAR конфигурируем на VLAN с Cisco IOS Release 12.1 (13) E, но поддерживаемый в коммутируемом пути программного обеспечения только.

Так как NBAR не может использоваться для классификации выходного трафика на канале WAN, где туннелирование или шифрование используется, примените его вместо этого к другим интерфейсам на маршрутизаторе, таким как интерфейс LAN (локальной сети), для выполнения классификации входящего трафика, прежде чем трафик будет коммутирован к каналу WAN для выходных данных.

Для большего количества сведений о NBAR посмотрите ссылки в Дополнительных сведениях