Защита сети от вируса Nimda

Содержание

Введение

Данный документ описывает способы сведения влияния червя Nimda в сети к минимуму. В документе рассмотрены две темы:

- Сеть заражена, что может быть сделано? Как можно минимизировать повреждение и непредвиденные последствия?
- Сеть еще не заражена или только частично заражена. Что необходимо сделать для минимизации распространения червя?

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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 Технические

рекомендации Cisco. Условные обозначения.

Общие сведения

Для общих сведений на Черве nimda обратитесь к этим ссылкам:

- http://www.cert.org/body/advisories/CA200126_FA200126.html
- http://vil.nai.com/vil/content/v_99209.htm
- http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html

Поддерживаемые платформы

Решение для Сетевого распознавания приложений (NBAR), 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 программного обеспечения Cisco IOS
7200	12.1 (5) T
7100	12.1 (5) T
3660	12.1 (5) T
3640	12.1 (5) T
3620	12.1 (5) T
2600	12.1 (5) T
1700	12.2 (5) T

Примечание: Подключите экспресс-пересылку Cisco, чтобы использовать средство распознавания приложения по сетевым параметрам.

NBAR также поддерживается на некоторых платформах программного обеспечения Cisco IOS начиная с выпуска 12.1E. См. "Поддерживаемые протоколы" в документации средства распознавания приложения по сетевым параметрам.

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

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

Если вы развертываете NBAR, знают об идентификаторе ошибки Cisco CSCdv06207 (только зарегистрированные клиенты). При встрече с этим дефектом может потребоваться обходной путь, описанный в CSCdv06207.

Решение для Списка контроля доступа (ACL) поддерживается во всех текущих релизах программного обеспечения Cisco IOS.

Для решений, где необходимо использовать Модульное качество сервиса (QoS) интерфейс командной строки (CLI) (такой что касается трафика ARP ограничения скорости или внедрять ограничение скорости с ограничителем вместо CAR), вам нужен Модульный интерфейс командной строки для обеспечения качества обслуживания, который доступен в Cisco IOS Software Release 12.0XE, 12.1E, 12.1T, и все версии 12.2.

Для использования согласованной скорости доступа (CAR) вам нужно программное обеспечение Cisco IOS release11.1CC и все версии 12.0 и более позднее программное обеспечение.

Как минимизировать повреждение и ограничить непредвиденные последствия

Этот раздел выделяет векторы заражения, которые могут распространить Вирус nimda и предоставляют советы для сокращения распространения вируса:

- Червь может распространить через Вложения электронной почты MIME audio/x-wav тип.**Советы:**Добавьте правила о своем сервере Протокола SMTP для блокирования любой электронной почты, которая имеет эти прикрепления:readme.exeAdmin.dll
- Червь может распространиться, когда вы просматриваете зараженный Web-сервер с включенным Выполнением JavaScript и использование версии Internet Explorer (IE), который уязвим для использования, обсужденного в MS01-020 (например, IE 5.0 или IE 5.01 без SP2).**Советы:**Используйте Netscape в качестве своего браузера, или отключите Javascript на IE или исправьте IE к SP II.Используйте распознавание приложений на основе сети (NBAR) для Cisco, чтобы фильтровать разрешение на загрузку файлов readme.eml. Вот пример для настройки NBAR:`Router(config)#`**`class-map match-any http-hacks`**
  `Router(config-cmap)#`**`match protocol http url "*readme.eml*"`** После согласования трафика можно выбрать сброс или выполнить маршрутизацию трафика на основе политик для мониторинга инфицированных узлов. Примеры полной реализации найдены в Использовании Сетевого распознавания приложений и Списков контроля доступа для Блокирования Червя "Code Red".
- Червь может распространиться с машины на машину в форме атак IIS (это прежде всего пытается использовать уязвимости, созданные эффектами Code Red II, но также и уязвимостями, ранее исправленными MS00-078).**Советы:**Используйте схемы Code Red, описанные в следующей статье:Решение проблем Mallocfail и высокого уровня загрузки CPU, возникающих вследствие работы червя Code RedИспользование сетевых списков распознавания приложений и управления доступом для блокирования червя Code Red`Router(config)#`**`class-map match-any http-hacks`**
  `Router(config-cmap)#`**`match protocol http url "*.ida*"`**
  `Router(config-cmap)#`**`match protocol http url "*cmd.exe*"`**
  `Router(config-cmap)#`**`match protocol http url "*root.exe*"`**
  `Router(config-cmap)#`**`match protocol http url "*readme.eml*"`** После согласования трафика можно выбрать сброс или выполнить маршрутизацию трафика на основе политик для мониторинга инфицированных узлов. Примеры полной реализации найдены в Использовании Сетевого распознавания приложений и Списков контроля доступа для

Блокирования Червя "Code Red".Ограничение скорости для пакетов синхронизации/старта (SYN) TCP. Это не защищает хост, но он позволяет вашей сети работать в пониженном качестве и все еще оставаться. SYN ограничения скорости вы выбрасываете пакеты, которые превышают определенную скорость, таким образом, некоторые TCP - подключения пройдут, но не все. Для примеров конфигурации обратитесь к "Ограничению скорости для Пакетов TCP SYN" раздел Использования CAR Во время DOS - атак.Рассмотрите протокол преобразования адресов с ограничением скорости (ARP) трафик, если сумма просмотров ARP вызывает проблемы в сети. Чтобы ограничить скорость трафика ARP, выполните следующие действия:

```
class-map match-any arp
   match protocol arp
!
!
policy-map ratelimitarp
   class arp
      police 8000 1500 1500 conform-action transmit exceed-action drop violate-action drop
```

Данная политика должна быть применена для соответствующего интерфейса LAN в качестве выходной политики. Модифицируйте рисунки как соответствующие обслужить количество ARPs в секунду, что вы хотите позволить в сети.

- Червь может распространиться путем выделения или .eml или .nws в Проводнике с включенным Активным рабочим столом (W2K/ME/W98 по умолчанию). По этой причине библиотека THUMBVW.DLL выполняет файл и предпринимает попытку загрузить файл README.EML, ссылка на который имеется в файле (в зависимости от версии Internet Explorer и параметров зоны).**Совет:** Как рекомендуется выше, используйте NBAR для фильтрации readme.eml от того, чтобы быть загруженным.
- Червь может распространяться через подключенные диски. Любой компьютер пораженный вирусом, который имеет подключенные сетевые диски, вероятно, заразит все файлы на сопоставленном дисководе и его подкаталогах**Советы:**Блочный Протокол TFTP (порт 69) так, чтобы компьютеры пораженный вирусом не могли использовать TFTP для передачи файлов незараженным главным компьютерам. Гарантируйте, что TFTP - доступ к маршрутизаторам все еще доступен (поскольку вам, возможно, понадобится путь к коду обновления). Если маршрутизатор выполняет версию программного обеспечения Cisco IOS 12.0 или позже, у вас всегда есть возможность использования протокола передачи файлов (FTP) для передачи образов маршрутизаторам рабочее программное обеспечение Cisco IOS.Блочный NetBIOS. NetBIOS не придется оставить локальную сеть (LAN). Поставщики услуг должны фильтровать вывод NetBIOS, блокируя порты 137, 138, 139 и 445.
- Червь использует собственный механизм SMTP для рассылки электронных сообщений, чтобы инфицировать другие системы.**Совет:** Блочный порт 25 (SMTP) на внутренних частях вашей сети. Пользователи, которые получают их электронную почту с помощью Почтового протокола (POP) 3 (порт 110) или Интернет-протокол доступа почты (IMAP) (порт 143), не должны обращаться к порту 25. Позволяет только порту 25 быть открытым SMTP сервером сети. Это может не быть выполнимо для пользователей, использующих Юдору, Netscape и Outlook Express, среди других, поскольку они имеют свой собственный модуль SMTP и будут генерировать исходящие соединения с помощью порта 25. Возможность использования прокси-серверов или другого механизма требует исследования.
- Уберите Cisco CallManager / Серверы приложений**Совет:** Пользователи с Call Managers и серверами приложений Call Manager в их сетях должны сделать следующее, чтобы

прекратить распространяться вируса. Они не должны переходить к компьютеру пораженный вирусом от Call Manager, и также они не должны совместно использовать дисководы на сервере Call Manager. Следуйте инструкциям, предоставленным в Очистке Вируса nimda от Cisco CallManager 3.x и серверы приложений CallManager для очистки Вируса nimda.

- Фильтруйте вирус nimda на CSS 11000**Совет:** Пользователи с CSS 11000 должны следовать инструкциям, предоставленным в фильтрации Вирус nimda на CSS 11000 для очистки Вируса nimda.
- Cisco Secure Intrusion Detection System (IDS CS) ответ на Вирус nimda**Совет:** IDS CS имеет два других компонента в наличии. Каждый - Узловая система обнаружения сетевых атак (HIDS), который имеет Хост-сенсор и Сетевой IDS (NIDS), который имеет Сетевой датчик, оба из которых другим способом отвечают на Вирус nimda. Для большего количества подробного объяснения и рекомендуемого курса действий, обратитесь к тому, Как Cisco Secure IDS Отвечает на Вирус nimda.

Дополнительные сведения

- Использование сетевых списков распознавания приложений и управления доступом для блокирования червя Code Red
- Решение проблем Mallocfail и высокого уровня загрузки CPU, возникающих вследствие работы червя Code Red
- Использование CAR при атаках DOS
- Информационные сообщения Cisco Security и предупреждения
- Cisco Systems – техническая поддержка и документация