Стратегии для защиты от атак Distributed Denial of Service (DDoS)

Содержание

Введение

Данный технический документ содержит сведения, которые помогут вам разобраться в том, как проводятся атаки DDoS (распределенная атака типа «отказ в обслуживании»), распознать программы, используемые для содействия атакам DDoS, применять меры для предотвращения таких атак, собрать судебные данные, если вы подозреваете атаку, и узнать больше о безопасности хоста.

Общие сведения об атаках DDoS

Обратитесь к следующей схеме:

Клиент — это человек, организующий атаку. Обработчик — это скомпрометированный узел сети со специальной запущенной на нем программой. Каждый обработчик поддерживает управление большим числом агентов. **Агент — это скомпрометированный узел сети, на котором запущена специальная программа.** Каждый агент отвечает за создание потока пакетов, который направляется намеченной жертве.

Известно, что атакующие используют следующие четыре программы для проведения атак DDoS:

1. Trinoo
2. TFN
3. TFN2K
4. Stacheldraht

Для облегчения проведения атаки DDoS, злоумышленники должны иметь от нескольких сотен до нескольких тысяч подконтрольных узлов. Такими узлами оказываются, как правило, компьютеры SUN или с ОС Linux, однако эти программные средства могут взаимодействовать также и с другими платформами. Процесс несанкционированного доступа к узлу и установки программного средства является автоматическим. Этот процесс можно разделить на следующие этапы, когда атакующие:

1. Инициируют процесс сканирования, в ходе которого большое число узлов сети (порядка 100 000 или более) проверяются на известную уязвимость.
2. Получают несанкционированный доступ к уязвимым узлам.
3. Устанавливают программное средство на каждый узел.
4. Используют скомпрометированные узлы сети для дальнейшего сканирования и компрометации.

Поскольку используется автоматизированный процесс, злоумышленники могут получить несанкционированный доступ и установить программное средство на одном узле в течение 5 секунд. Другими словами в течении часа можно получить несанкционированный доступ к нескольким тысячам узлов.

Характеристики типичных программ, используемых для проведения атак

Следующие программы обычно используются хакерами для проведения распределенных атак типа «отказ в обслуживании»:

- TrinooДля связи между клиентами, обработчиками и агентами используются следующие порты:`1524 tcp`
  `27665 tcp`
  `27444 udp`
  `31335 udp`**Примечание:** *Перечисленные выше порты являются портами по умолчанию для этого свойства.* Эти номера портов приведены только для примера, поскольку их легко изменить.
- TFNДля обмена данными между клиентами, обработчиками и агентами используются пакеты ICMP ECHO и ICMP ECHO REPLY.
- StacheldrahtДля связи между клиентами, обработчиками и агентами используются следующие порты:`16660 tcp`
  `65000 tcp`
  `ICMP ECHO`
  `ICMP ECHO REPLY`**Примечание:** Порты, ранее перечисленные, являются портами по умолчанию для этого программного средства. Эти номера портов приведены только для примера, поскольку их легко изменить.
- TFN2KДля связи между клиентами, обработчиками и агентами не используется какой-либо конкретный порт, например, этот порт может быть указан во время выполнения или выбран случайным образом программой, но является комбинацией UDP, ICMP и TCP пакетов.Подробный анализ программ DDoS читайте в следующих статьях.

Примечание: Theaw связывает точку с сайтами внешней web - страницы, не поддерживавшими Cisco Systems.

Средство распределенных DoS-атак DoS Project's "trinoo"

Средство DDoS-атак Tribe Flood Network

"Stacheldraht" – средство распределенной атаки типа "отказ в обслуживании"

Дополнительную информацию относительно инструментов DDoS и их вариантов можно найти на веб-сайте Packet Storm в алфавитном указателе Distributed Attack Tools.

Предотвращение

Ниже предлагаются способы предотвращения распределенных атак, вызывающих отказ в обслуживании.

1. При помощи команды интерфейса ip verify unicast reverse-path на входном интерфейсе маршрутизатора на конце соединения в направлении исходящего трафика.Эта функция проверяет каждый пакет, полученный как входящий на этот интерфейс. Если IP-адрес источника не имеет маршрута в таблице CEF, указывающего обратно на тот же интерфейс, которому поступил пакет, маршрутизатор отбрасывает такой пакет.Эффект однонаправленной проверки передачи по обратному пути (Unicast Reverse Path Forwarding, uRPF) заключается в остановке атак SMURF (и других атак со спуфингом IP-адреса источника) в точке, в которой сеть поставщика услуг Интернета связывается по коммутируемым каналам с сетями других поставщиков услуг Интернета. Такой способ защищает сеть и клиентов, а также остальную часть Интернета. Чтобы использовать uRPF, в маршрутизаторе необходимо включить коммутацию CEF или распределенную коммутацию CEF. Нет необходимости настраивать входной интерфейс для коммутации CEF. В то время как на маршрутизаторе выполняется коммутация CEF, возможна настройка отдельных интерфейсов для работы в других режимах коммутации. RPF — функция входной стороны, включенная на интерфейсе и подчиненном интерфейсе для пакетов, получаемых маршрутизатором.На маршрутизаторе необходимо обязательно включить CEF. RPF не работает без CEF. URPF не поддерживается образами 11.2 и 11.3. URPF включена в версию 12.0 на платформах, поддерживающих CEF, включая AS5800. Поэтому uRPF можно настроить на интерфейсах удаленного доступа PSTN/ISDN на AS5800.
2. Фильтруйте все адресное пространство RFC1918 с помощью Списков контроля доступа (ACL).Пример:
```
access-list 101 deny ip 10.0.0.0    0.255.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0  0.15.255.255 any
access-list 101 permit ip any any

interface xy
   ip access-group 101 in
```
Другой источник информации о специальном пространстве адреса IPv4 использования, которое может фильтроваться, (теперь истек), проект IETF 'Документация Специальных Блоков Адреса IPv4 Использования, которые были зарегистрированы в IANA'
3. Примените входную и выходную фильтрацию (см. RFC 2267), использование ACL.Пример: `{ ISP Core } -- ISP Edge Router -- Customer Edge Router -- { Customer network }`Граничный маршрутизатор поставщика услуг Интернета должен принимать трафик только с исходными адресами, относящимися к сети клиента. Клиентская сеть должна принимать только трафик с исходными адресами, отличными от блока клиентской сети. Ниже приведен пример списка ACL для граничного маршрутизатора поставщика услуг Интернета:
```
access-list 190 permit ip {customer network} {customer network mask} any
access-list 190 deny ip any any [log]

interface {ingress interface} {interface #}
ip access-group 190 in
```
Ниже приведен пример списка ACL для граничного маршрутизатора клиента:`access-list 187 deny ip {customer network} {customer network`

```
mask} any
access-list 187 permit ip any any

access-list 188 permit ip {customer network} {customer network mask} any
access-list 188 deny ip any any

interface {egress interface} {interface #}
ip access-group 187 in
```
`ip access-group 188 out` Если можно включить CEF, длина списка ACL существенно уменьшится, что приведет к увеличению производительности благодаря включению однонаправленной проверки передачи по обратному пути. Для поддержки uRPF требуется только возможность включить CEF на маршрутизаторе в целом; интерфейс, для которого включается эта функция, не обязан быть интерфейсом с коммутацией CEF.

4. Использование CAR для ограничения скорости передачи ICMP-пакетов.Пример:`interface xy`
 `rate-limit` `output access-group 2020 3000000 512000 786000 conform-action transmit exceed-action drop access-list 2020 permit icmp any any echo-reply`
5. Настройка ограничения скорости для SYN-пакетов.Пример:`access-list 152 permit tcp any host eq www`
```
access-list 153 permit tcp any host eq www established

interface {int}
rate-limit output access-group 153 45000000 100000 100000
conform-action transmit exceed-action drop
 rate-limit output access-group 152 1000000 100000 100000
```
`conform-action transmit exceed-action drop` В предыдущем примере замените:**45000000 максимальной пропускной способностью канала1000000 значением из диапазона 50-30% от скорости генерирования синхронизирующих символов (синхронная атака)***нормальную и максимальную скорости пакетов точными значениями*Учтите, если установить скорость пакетов более 30%, то много неподдельных SYN-пакетов могут быть потеряны. Для определения оптимальной скорости пакетов выполните команду show interfaces rate-limit, чтобы отобразить согласованную и запредельную скорости для этого интерфейса. Цель – ограничить скорость SYN-пакетов как можно меньшим значением, лишь бы восстановить работоспособность.**% Warning:** Рекомендуется сначала измерить сумму SYN - пакетов во время нормального состояния (прежде чем атаки произойдут), и используйте те значения для ограничения. Перед применением результатов измерения внимательно их проанализируйте.Если атака SYN нацелена против конкретного узла сети, рассмотрите установку пакета фильтрации IP на этом узле. Одним из таких пакетов является IP Filter. См. Примеры Фильтра IP для сведений о внедрении.

Сбор доказательств и обращение к закону

По возможности получите образец трафика во время атаки для последующего анализа (часто называют «захват пакетов»). Используйте рабочую станцию с ОС Solaris или Linux, имеющую достаточную производительность, чтобы справиться с лавиной пакетов. Для получения такого захвата пакета используйте любого программа tcpdump (доступный для Windows, Solaris и операционных систем Linux) или программа ищейки (доступный только для Операционной системы Solaris). Ниже приведен общий пример использования этих программ:

```
tcpdump -i interface -s 1500 -w capture_file
  snoop -d interface -o capture_file -s 1500
```
В этом примере максимальный размер передаваемого блока данных (MTU) составляет 1500; измените этот параметр, если MTU больше 1500.

Если вы находитесь в США и хотите задействовать правоприменительные акции обратитесь в местное отделение ФБР. Дополнительную информацию см. на веб-сайте Национального центра защиты инфраструктуры. Если вы находитесь в Европе, то конкретного учреждения для обращения не существует. Обратитесь за помощью в местный полицейский орган.

CISCO НЕ МОЖЕТ ОБРАЩАТЬСЯ В ПРАВОПРИМЕНЯЮЩИЕ ОРГАНЫ ОТ ВАШЕГО ИМЕНИ. Группа Cisco PSIRT может взаимодействовать с правоохранительными органами только после вашего первоначального обращения.

Для материалов по безопасности общего узла посетите веб-страницу CERT/CC.

Дополнительные сведения

- Описание и отслеживание лавинной передачи пакетов с помощью маршрутизаторов Cisco
- Технические сведения для борьбы с «червями»
- Повышение уровня безопасности маршрутизаторов Cisco
- Группа реагирования на угрозы безопасности, связанные с уязвимостями решений Cisco (PSIRT)
- Безопасность и Cisco
- Cisco Systems – техническая поддержка и документация