

Ботнеты: новый характер угроз

Введение

Ботнет представляет собой целую армию зараженных вирусом компьютеров, находящихся под удаленным контролем злоумышленника. Широкое распространение технологий широкополосного доступа привело к значительному расширению возможностей ботнетов по запуску атак типа «отказ в обслуживании», заражению миллионов компьютеров шпионскими программами и другим вредоносным кодом, хищению конфиденциальных данных, широкомасштабной рассылке спама, «накручиванию» кликов, шантажу и вымогательству.

На сегодняшний день ботнеты являются основной угрозой безопасности в Интернете. Атаку с использованием ботнета легко заказать, и хакеры с небывалой скоростью находят и используют новые уязвимости. Как правило, один ботнет состоит из десятков тысяч компьютеров. Ботнеты сложно обнаруживать, поскольку их топология динамична по своей природе, что позволяет обходить наиболее распространенные средства защиты.

Подразделениям обеспечения информационной безопасности необходимо принимать меры по предотвращению заражения корпоративных компьютеров и защите корпоративных ресурсов от атак с использованием ботнетов. В этом официальном документе рассматриваются типичный жизненный цикл ботнета, виды атак с использованием ботнетов, а также наиболее эффективные методы обнаружения ботнетов и борьбы с ними. В конце документа рассматриваются решения, предлагаемые компанией Cisco®.

Как создаются сети «зомби»?

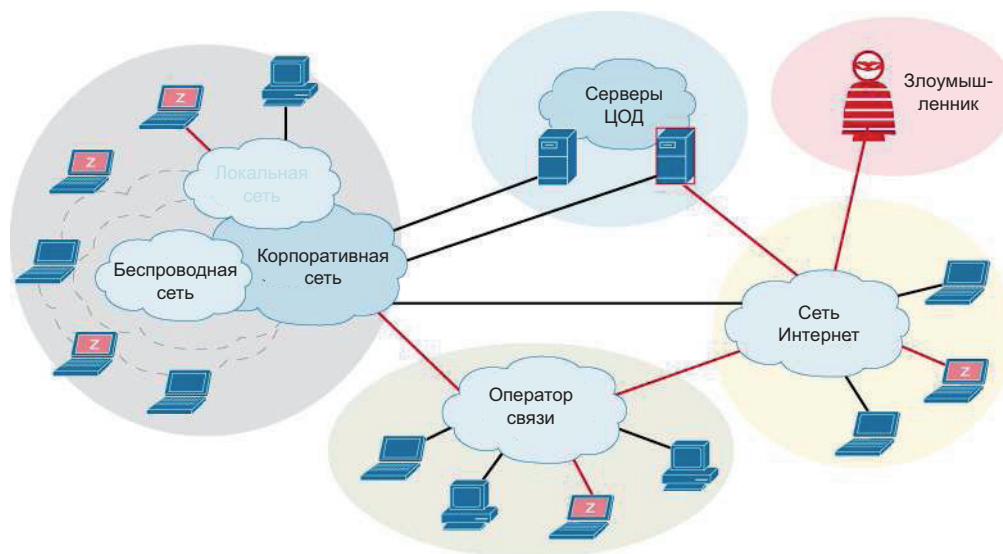
Создание ботнета начинается с загрузки специальной программы – бота (например, IRCBot, SGBot или AgoBot) – со встроенным вредоносным кодом на компьютер ничего не подозревающего пользователя, который открыл зараженное вложение электронной почты либо загрузил вредоносные файлы или бесплатное программное обеспечение из файлообменной сети или с вредоносного web-сайта.

После установки специальной программы и вредоносного кода зараженный компьютер подключается к серверу, который злоумышленник настроил в качестве системы управления для передачи команд ботнету. Зачастую в качестве системы управления используется общедоступный сервер IRC, однако взломанные серверы также могут передавать команды с помощью протоколов HTTPS, SMTP, TCP и UDP. Системы управления не привязываются к одному узлу и часто перемещаются между узлами для предотвращения обнаружения; они запускаются на компьютерах (а подключения к ним осуществляются через прокси-серверы), не принадлежащих злоумышленнику, управляющему сетью.

Используя систему управления, злоумышленник может периодически внедрять новый вредоносный код в установленную на компьютеры ботнета программу. Система управления может также использоваться для изменения кода самой вредоносной программы, чтобы предотвратить обнаружение последней с помощью сигнатур или реализации новых команд и векторов атаки.

Однако первоочередной задачей злоумышленника, управляющего ботнетом, является расширение самого ботнета. Каждый узел ботнета выполняет поиск и заражение уязвимых компьютеров, которые пополняют ботнет и сами начинают поиск потенциальных «новобранцев». Всего за несколько часов ботнет может вырасти до гигантских размеров, иной раз заражая миллионы компьютеров по всему миру. На рис. 1 показан типичный ботнет.

Рисунок 1. Типичный ботнет



Вооружившись армией зараженных компьютеров, злоумышленник приступает к первой массовой атаке.

Фактически, целью этой атаки может стать любая вычислительная система, будь то компьютер малого предприятия, домашней сети, корпоративного офиса или POS-терминал розничного магазина. Определение местоположения злоумышленника, управляющего сетью, является чрезвычайно сложной задачей, поскольку, как правило, он подает команды управления через несколько зараженных компьютеров-посредников, расположенных в различных сетях. Соединения с посредниками, как и сама система управления, часто изменяются, что делает обнаружение хакера практически невозможным.

Виды атак с использованием ботнетов

Ботнеты позволяют хакерам запускать самые разные атаки.

Распределенные атаки типа «отказ в обслуживании» (DDoS)

Используя сеть, состоящую из нескольких тысяч рассредоточенных по всему миру зараженных узлов, злоумышленник может запустить крупномасштабную скоординированную атаку для снижения эффективности работы или вывода из строя популярных сайтов и служб путем лавинной отправки пакетов на целевую систему с целью исчерпания ресурсов и превышения полосы пропускания каналов связи. Атаки с объемами трафика несколько гигабит в секунду не являются редкостью. Наиболее часто используется лавинная отправка пакетов UDP, ICMP и TCP SYN; к другим атакам относится подбор пароля методом перебора и атаки на уровне приложений.

Целями атак могут быть web-сайты коммерческих и государственных учреждений, службы электронной почты, серверы доменных имен (DNS), хостинг-провайдеры, критически важные элементы инфраструктуры сети Интернет и даже серверы разработчиков средств

информационной безопасности и защиты от спама. Атаки могут быть также нацелены на определенные политические и религиозные организации, а также на Интернет-казино, порнографические сайты и игровые порталы. Иногда за этими атаками следует вымогательство.

Применение шпионских программ и вредоносного ПО

Вредоносный код на зараженном компьютере без ведома и согласия пользователя отслеживает его действия и передает отчеты злоумышленнику. Информация, содержащаяся в этих отчетах, используется для непосредственной наживы или вымогательства. Кроме того, на компьютер ботнета может автоматически устанавливаться дополнительное программное обеспечение для отслеживания нажатий клавиш и сбора сведений об уязвимостях систем для последующей продажи этой информации третьим лицам.

Хищение персональной информации

Ботнеты часто применяются для хищения персональной информации, данных о финансовой деятельности или паролей с компьютеров пользователей для последующей продажи или непосредственной наживы.

Применение средств навязывания рекламы

Вредоносный код на зараженном компьютере может автоматически загружать, устанавливать и отображать всплывающие окна с рекламой в зависимости от просматриваемых пользователем страниц в сети Интернет или регулярно открывать в браузере определенные web-сайты.

Рассылка спама

На сегодняшний день большинство нежелательных сообщений электронной почты распространяется с помощью ботнетов. В результате исследования, проведенного компанией IronPort в июне 2006 года, было установлено, что 80% всего спама было отправлено с «зомби» – на 30% больше по сравнению с прошлым годом. На сегодняшний день, этот показатель еще выше – более 95% спама в Интернете, рассылается с использованием ботнетов.

«Накручивание» кликов

Специальный код может имитировать легитимного пользователя web-браузера, переходящего по рекламным модулям, размещенным на web-сайтах, которые принадлежат к рекламной сети с оплатой за каждый клик (например, Google Adwords), с целью заставить платить определенного рекламодателя (или привлечь его к ответственности).

Фишинг

Ботнеты позволяют выполнять поиск уязвимых серверов, которые могут использоваться для размещения сайтов фишинга, имитирующих реально существующие ресурсы (например, PayPal или web-сайты Интернет-банков), с целью хищения паролей и других конфиденциальных данных.

Обнаружение и борьба с ботнетами

Ботнеты используют множество векторов атаки; применение одной технологии обеспечения безопасности не может обеспечить защиту от них. Например, целью DDoS-атаки является

вывод из строя сервера. Целью фишинга – привлечение пользователей на вредоносный web-сайт, замаскированный под реально существующий ресурс, чтобы выведать у них персональную информацию. Вредоносное ПО может применяться в самых различных целях – от сбора персональных данных и показа рекламы на зараженном компьютере до рассылки с него спама. Для обнаружения и отражения атак с использованием ботнета необходим подход, реализующий глубокую эшелонированную оборону.

Традиционные методы фильтрации пакетов, анализа трафика на основе используемых портов и проверки с использованием сигнатур не позволяют эффективно бороться с атаками ботнетов, которые динамично и быстро изменяют вредоносный код, систему управления и используемые порты (или используют стандартные порты HTTP/S, такие как 80 и 443).

В настоящее время для обнаружения ботнетов применяются разнообразные свободно распространяемые и коммерческие средства. Многие из них выполняют анализ данных о трафике, передаваемых с маршрутизаторов (например, Cisco® NetFlow). Другие средства используют методы анализа поведения; например, определение базовых показателей сетевого трафика в обычных условиях и выявление аномальных всплесков трафика, которые могут указывать на DDoS-атаку. Для обнаружения ботнетов также используются анализ журналов DNS-серверов и создание систем-приманок (honeypot), однако эти методы не всегда могут быть масштабированы.

К наиболее распространенным методам обнаружения ботнетов относятся:

- **Анализ телеметрии.** Этот метод заключается в использовании сводной информации сетевого и транспортного уровня от сетевых устройств. Технология Cisco NetFlow часто применяется Интернет-провайдерами и отделами информационной безопасности предприятий для обнаружения трафика DDoS-атак, всплесков трафика SMTP, характерного для массовой рассылки спама и управляющего трафика контроллера ботнета.
- **Обнаружение аномалий.** Если подходы на основе сигнатур заключаются в сопоставлении каждой атаки с имеющейся базой данных сигнатур, то обнаружение аномалий (или поведенческие подходы) заключается в обратном: описываются характеристики обычного трафика, а затем выполняется поиск отклонений. При использовании такого подхода обеспечивается обнаружение и блокировка DDoS-атак и попыток массового сканирования, предпринимаемых ботнетом. Метод обнаружения аномалий может эффективно применяться в сети, а также на оконечных узлах (таких как серверы и портативные компьютеры). При использовании на оконечных узлах этот метод позволяет обнаруживать подозрительные действия и нарушения политик безопасности и предотвращать заражение узла.
- **Анализ журнала сервера DNS.** Ботнеты часто используют бесплатные службы DNS, чтобы разместить адрес поддомена серверов IRC, захваченных управляющим ботнетом злоумышленником и содержащих специальные программы и соответствующий вредоносный код. Свойственный ботнетам код содержит жестко заданные ссылки на DNS-сервер, которые могут быть легко найдены любым средством анализа журнала DNS-запросов. При обнаружении таких служб администратор DNS-сервера может нейтрализовать ботнет путем переадресации поддоменов, нарушающих действующую политику, на несуществующий IP-адрес (так называемая «маршрутизация в никуда»). Хотя данный метод является эффективным, его сложнее всего применять, поскольку для этого требуется сотрудничество со сторонними хостинг-провайдерами и службами регистрации доменных имен.

- Система-приманка. «Приманка» – замкнутая, защищенная и контролируемая область, имитирующая уязвимую сеть, ресурс или службу. Ее основная цель – приманить и обнаружить вредоносные атаки и попытки вторжения. Функционируя больше как система наблюдения и раннего предупреждения, она также позволяет исследователям в области информационной безопасности анализировать развитие угроз. Из-за сложности установки и необходимости активного анализа, использование «приманок» в сетях крупного масштаба ограничено.

Продукты и решения Cisco

Cisco предлагает широкий ассортимент решений для обнаружения ботнетов и предотвращения создаваемых ими атак. Ниже представлено описание данных продуктов.

Устройства обнаружения и подавления DDoS-атак Cisco Guard и Cisco Anomaly Detector

Устройства Cisco Guard являются самыми функциональными и мощными из существующих решений для подавления наиболее опасных на сегодняшний день угроз, исходящих от ботнетов, а именно DDoS-атак.

Устройства Cisco Guard основаны на уникальной архитектуре множественной верификации и работают в тесном взаимодействии с системами обнаружения DDoS-атак Cisco Traffic Anomaly Detector. Такое сочетание позволяет реализовать самые современные технологии обнаружения аномалий и разнообразной проверки источников пакетов, позволяющие в режиме реального времени обнаруживать и блокировать отдельные вредоносные потоки, пропуская легитимный трафик. Тем самым, доступность сети и непрерывность бизнес-процессов обеспечиваются даже во время атаки.

Cisco Guard обрабатывает трафик со скоростью несколько гигабит в секунду для защиты операторов связи и крупных предприятий от DDoS-атак посредством анализа каждого потока и обнаружения и блокирования вредоносных пакетов. Более подробную информацию см. на странице http://www.cisco.com/en/US/products/ps5879/Products_Sub_Category_Home.html

Cisco Service Control Engine

Решение Cisco Service Control Engine (Cisco SCE) обладает возможностью контроля трафика абонентов сети ШПД. Используя технологии глубокого анализа пакетов с учетом состояния соединений, решение Cisco SCE вооружает операторов мощным инструментом борьбы с угрозами, исходящими от зомби-компьютеров в сети ШПД. Обнаружение зараженных абонентов, производится за счет мониторинга трафика и выявления признаков работы бота, таких как рассылка спама, сканирование и DDoS-атаки. Все эти признаки говорят о заражении компьютера абонента вредоносным ПО и его причастности к ботнету. После того как зараженные компьютеры выявлены, оператор ШПД может поместить их в карантин (отказать в доступе в сеть), чтобы защитить сеть, а также уведомить пользователя о заражении, для того чтобы он мог принять меры по очистке своего компьютера от вирусов.

Дополнительная информация о Cisco SCE: <http://www.cisco.com/go/servicecontrol/>

Cisco IronPort

Устройство IronPort S-series имеет возможность мониторинга трафика на 4 уровне со скоростью 1Гбит/с, обнаруживая и блокируя попытки соединений с вредоносными ресурсами в сети Интернет. Отслеживая активность на всех 65 535 сетевых портах, IronPort S-series эффективно блокирует вредоносное ПО, пытающееся обойти порт 80, а также

предотвращает мошеннические действия, связанные с использованием клиентов файлообменных сетей и IRC. Это позволяет обнаруживать зараженные вредоносным ПО компьютеры, пытающиеся установить исходящие соединения с контроллером ботнета, передачи конфиденциальных данных и пр.

Дополнительный уровень защиты предоставляется фильтрами web-репутации IronPort. Эти фильтры работают на основе репутационной информации, накопленной сетью IronPort SenderBase, самой первой и крупной в мире системой мониторинга почтового и web-трафика, которая осуществляет сбор данных из более чем 100 000 сетей по всему миру. Отслеживая значения более чем 40 параметров, относящихся к web-трафику, SenderBase делает очень точные выводы о каждом URL-адресе. Если сайт внезапно начинает распространять вредоносный код (что свидетельствует о его заражении), его репутация снижается, в результате чего он подвергается сканированию антивирусной системой IronPort S-series.

Обширная информация SenderBase позволяет фильтрам web-репутации IronPort блокировать как известные, так и новые угрозы, что обеспечивает гораздо более высокую эффективность обнаружения вредоносных программ по сравнению с решениями web-безопасности на основе сигнатур. Эти методы предотвращают загрузку ПО бота и другого вредоносного кода, например, средств навязывания рекламы, троянских программ, программ для отслеживания нажатий клавиш, файлов cookies для отслеживания особенностей просмотра пользователем страниц в сети Интернет, программ для перехвата управления браузером с целью открытия определенных web-страниц и средств фишинга. Более подробную информацию см. на сайте <http://www.ironport.com>

Cisco Security Agent

Cisco Security Agent защищает серверы, персональные компьютеры и POS-терминалы от наиболее распространенных атак с использованием ботнета: установки ПО бота, шпионских программ, ПО для скрытого удаленного управления, а также целенаправленных и совершенно новых атак. Cisco Security Agent обеспечивает превентивную защиту от неизвестных и новых угроз, а также модификаций известных угроз, в которых используются опубликованные и неопубликованные уязвимости системы.

Cisco Security Agent обеспечивает видимость выполняющихся на хостах процессов, которые взаимодействуют с узлами вне корпоративной сети, и создает соответствующие отчеты. Он выполняет глобальный корреляционный анализ информации об угрозах и динамически принимает меры по отражению. Кроме того, Cisco Security Agent может обнаруживать аномальную активность, например, лавинную посылку TCP SYN пакетов, и влиять на действующие в сети политики безопасности. Это достигается путем передачи информации об агрессивном поведении хостов (указывающей на то, что они являются зараженными) на системы предотвращения вторжений Cisco IPS (установленные на пути прохождения трафика), что приводит к блокированию доступа этих хостов к сети. Cisco Security Agent также может контролировать доступ к файлам ключей, приложениям и серверам, осуществляемый с неавторизованных хостов. Более подробную информацию см. на странице <http://www.cisco.com/go/csa>

Системы предотвращения вторжений Cisco

Системы Cisco IPS используют алгоритмы обнаружения аномалий для обнаружения и блокирования атак с использованием ботнетов. В основе этих алгоритмов лежит предположение о том, что быстро распространяющиеся Интернет-черви и предпринимаемые

ботнетами попытки сканирования приведут к изменению общепринятых шаблонов трафика в сети (например, в результате поиска дополнительных уязвимых хостов).

Для обнаружения аномалий Cisco IPS использует два режима: обучения и обнаружения. В режиме обучения Cisco IPS исследует обычное поведение вашей сети и создает набор профилей для каждой сетевой службы на гистограмме. В режиме обнаружения Cisco IPS выявляет отклонения от обычных профилей поведения и отмечают соответствующую активность. Сенсоры контролируют такие события, как:

- отсутствие ответа SYN-ACK на запрос TCP SYN;
- отсутствие ответа в виде UDP-пакетов на отправленные UDP-пакеты;
- отсутствие ответов на ICMP-запросы или запросы, переданные с использованием других протоколов.

Системы Cisco IPS отличают события, вызванные сбоем соединений, от попыток сканирования, выявляют отклонения, а затем на основе имеющихся шаблонов классифицируют аномальную активность как поведение Интернет-червя или программы для поиска уязвимых хостов. После этого Cisco IPS вырабатывает ответные действия, например, «Блокировать атакующего» или «Подать сигнал тревоги». Данный поведенческий подход позволяет мгновенно обнаруживать быстро распространяющихся Интернет-червей даже без наличия последнего набора сигнатур. Применение систем Cisco IPS в сочетании с Cisco Security Agent позволяет получить еще более мощное решение для обнаружения и отражения совершенно новых атак с использованием ботнетов.

Cisco NetFlow

Cisco NetFlow – это лучшая из представленных в отрасли реализация Flow-протоколов с функцией телеметрии, позволяющей получать данные о работе маршрутизаторов под управлением Cisco IOS®. Благодаря своей масштабируемости и возможности предоставления отчетов о трафике в сетях любых размеров технология Cisco NetFlow стала стандартным методом получения полезной информации для управления трафиком и обеспечения безопасности в сетях как предприятий, так и операторов связи. Телеметрические данные Cisco NetFlow можно использовать для обнаружения ботнетов, расследования инцидентов и выполнения аудита.

После включения NetFlow на конкретном сетевом устройстве его телеметрические данные можно просматривать с помощью интерфейса командной строки или передавать на внешние средства сбора и анализа NetFlow. Более подробную информацию см. на странице <http://www.cisco.com/go/netflow>

Cisco Global Site Selector

Cisco Global Site Selector – это устройство глобального распределения нагрузки, которое может также использоваться в качестве DNS-сервера, предоставляющего масштабируемые службы имен и адресации для сетей предприятий и операторов связи. Выполняя функции распределения нагрузки или DNS-сервера, данное устройство позволяет снижать воздействие DDoS-атак на DNS-сервер. Такая функция самозащиты может быть развернута для обеспечения безопасности любой DNS-инфраструктуры, включающей службы BIND, клиентские устройства на основе ПО Microsoft, а также Microsoft Active Directory.

Cisco Global Site Selector использует ряд функций уникальной архитектуры множественной верификации, применяемых в устройствах подавления DDoS-атак Cisco Guard. Global Site Selector блокирует вредоносный трафик, продолжая передавать легитимный DNS-трафик.

К функциям Cisco Global Site Selector относится ограничение скорости потока, фильтрация и предотвращение подмены адреса источника. Более подробную информацию см. на странице <http://www.cisco.com/go/gss>

В таблице 1 приводится сравнение описанных выше решений Cisco.

Таблица 1. Матрица угроз ботнетов и решений Cisco

Технология Cisco	Угрозы ботнетов			
	DDoS-атака	Распространение вредоносного кода	Фишинг	Рассылка спама
Устройства Cisco Guard и Cisco Traffic Anomaly Detector	Обнаружение и подавление атак	—	—	—
Cisco SCE	Обнаружение и блокирование атакующих узлов	Обнаружение и блокирование зараженных узлов	—	Обнаружение и блокирование источников спама
Cisco NetFlow	Обнаружение атак	Обнаружение	—	Обнаружение источников спама
IronPort S-series	—	Обнаружение и блокирование вредоносного ПО в Web трафике. Блокирование попыток соединений с вредоносными ресурсами сети Интернет.	Блокирование попыток посещения фишинговых сайтов.	—
IronPort C-series	—	Обнаружение и блокирование вредоносного ПО в E-mail трафике.	Блокирование фишинговых писем	Детектирование и фильтрация спама
Cisco Security Agent	—	Предотвращение заражения	—	—
Cisco IPS	—	Обнаружение и предотвращение распространения вредоносного кода в сети	—	—
Cisco Global Site Selector	Предотвращение атак на службу DNS	—	—	—

Заключение

На сегодняшний день ботнеты представляют наиболее опасную угрозу безопасности в Интернете. Ботнеты используют множество векторов заражения и атак, поэтому применение одной технологии не может обеспечить защиту от всех исходящих от них угроз. Cisco является единственной компанией в отрасли информационной безопасности, предлагающей самый полный набор продуктов для защиты от атак с использованием ботнетов. Более подробную информацию см. на странице <http://www.cisco.com/go/tcc>.



Cisco
Россия, 115054, Москва,
бизнес-центр
«Риверсайд Тауерс»
Космодамианская наб., 52,
стр. 1, этаж 4
Тел.: +7 (495) 961-14-10
Факс: +7 (495) 961-14-60
www.cisco.ru
www.cisco.com

Cisco
Россия, 191186,
Санкт-Петербург,
бизнес-центр «Регус»
Невский проспект, 25,
этаж 2, офис 30
Тел.: +7 (812) 346-77-17
Факс: +7 (812) 346-78-00
www.cisco.ru
www.cisco.com

Cisco
Казахстан, 480099,
Алматы,
бизнес-центр «Самал 2»
Ул. О. Жолдасбекова, 97,
блок А2, этаж 14
Тел.: +7 (327) 244-21-01
Факс: +7 (327) 258-46-60
www.cisco.ru
www.cisco.com

Cisco
Украина, 03038, Киев,
бизнес-центр
«Горизонт Парк»
(Horizon Park)
Ул. Николая Гринченко, 4В
Тел.: +38 (044) 391-36-00
Факс: +38 (044) 391-36-01
www.cisco.ua
www.cisco.com

Cisco
Азербайджан,
AZ 1065, Баку,
бизнес-центр «Карат»
Ул. М. Мухтарова, 201,
этаж 2
Тел.: +994 (50) 250-99-94
Факс: +994 (12) 437-48-20
www.cisco.ru
www.cisco.com

Cisco
Узбекистан, 100000,
Ташкент, бизнес-центр
«Инконель»
Ул. Пушкина, 75,
офис 605,
Тел.: +998 (71) 140-44-60
Факс: +998 (71) 140-44-65
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2007 Cisco Systems Inc. All rights reserved. Printed in Russia. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)