Dr.WEB®
Антивирус

Информационный бюллетень

Ботнеты

Дата составления	4.10.12
Текущий уровень опасности	Высокий

Наиболее актуальные угрозы безопасности компаний*	Типы угроз
Вредоносные программы, способные организовывать бот-сети — распределенные системы, состоящие из инфицированных компьютеров и управляемые одним или несколькими командными серверами.	Win32.Rmnet.12 Win32.Rmnet.16 Backdoor.Flashback.39 Backdoor.Andromeda.22 Trojan.WinSpy

* Актуальность угроз определяется не только количеством и разнообразием вредоносных программ, но и уровнем защиты от них в компаниях и организациях различного типа.

© ООО «Доктор Веб», 2003–2012
125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Телефон: +7 (495) 789-45-87 (многоканальный)
Факс: +7 (495) 789-45-97

www.drweb.com
www.freedrweb.com
www.av-desk.com

Тема выпуска: Ботнеты

Ботнет — это сеть компьютеров, зараженных вредоносной программой, которая позволяет преступным группировкам удаленно управлять зараженными машинами без ведома пользователя. Как правило, большинство современных ботов являются многофункциональными вредоносными приложениями, позволяющими злоумышленникам реализовывать широкий ассортимент различных угроз.

Типичные представители

- Win32.Rmnet.12 — файловый вирус, в сети насчитывается более 4 миллионов инфицированных узлов, работающих под управлением Microsoft Windows;
- Win32.Rmnet.16 — файловый вирус, в сети насчитывается более 400 000 инфицированных узлов, работающих под управлением Microsoft Windows;
- Backdoor.Flashback.39 — троянская программа для Mac OS X; в пиковый период более были заражены более 800 000 машин;
- Backdoor.Andromeda.22 — чрезвычайно распространенный троянец-бот, обладающий широким вредоносным функционалом, однако используемый в основном для загрузки на инфицированный компьютер других троянских программ;
- Trojan.WinSpy — обширное семейство вредоносных программ, некоторые версии используют руткит-технологии. Часто используется для загрузки на инфицированный компьютер других вредоносных приложений.

Цели организации ботнетов

Преступные группировки организуют и используют ботнеты в следующих целях:

- Загрузка и установка на инфицированный компьютер по команде с удаленного сервера других вредоносных программ (так называемые троянцы-загрузчики, или даунлоадеры). Ярким представителем данного семейства является Backdoor.Andromeda.22. Услуга по загрузке на компьютеры пользователей вредоносных программ пользуется высоким спросом среди вирусописателей и успешно монетизируется злоумышленниками.
- Проведение DDoS-атак (Distributed Denial-of-Service) на отдельные сайты и веб-сервисы. Данная услуга также широко востребована среди злоумышленников, промышляющих киберпреступлениями. Сетевые атаки могут использоваться в целях вымогательства, давления на конкурентов, дискредитации перед потенциальными клиентами.
- Распространение спама с использованием инфицированных рабочих станций. При этом спам рассылается не только в виде электронной почты, но и в социальных сетях, форумах, блогах.
- Удаленное управление инфицированными компьютерами, возможность хищения хранящихся на локальных дисках файлов.
- Прямое вымогательство финансовых средств у пользователя инфицированного компьютера (Trojan.Mayachok.1).
- Хищение конфиденциальной информации (в том числе логинов и паролей) методом анализа трафика, осуществления веб-инжектов, похищения файлов cookies, кейлоггинга (перехвата нажатий клавиш), пересылки злоумышленникам снимков экрана, иных методов (Win32.Rmnet.12, Win32.Rmnet.16).
- Хищение информации для доступа к системам дистанционного банковского обслуживания (ДБО), что позволяет злоумышленникам получить доступ к банковским счетам предприятия (Trojan.PWS.Panda, Trojan.Carberp).
- Перенаправление браузера пользователя на принадлежащие злоумышленникам веб-страницы. При этом могут преследоваться различные цели: фишинг, загрузка на компьютер пользователя вредоносного ПО с использованием уязвимостей, «накрутка» посещаемости некоторых интернет-ресурсов.
- Использование инфицированных компьютеров в качестве прокси-серверов для анонимизации доступа злоумышленников в Интернет.

Получив несанкционированный доступ к инфицированному компьютеру, злоумышленники могут:

- установить на инфицированную рабочую станцию любую другую (в том числе вредоносную) программу;
- просматривать любые хранящиеся на компьютере файлы, копировать и передавать их на собственный управляющий сервер;
- работать в Интернете, используя инфицированный компьютер в качестве промежуточного узла, в том числе совершая различные противоправные действия, например сетевые атаки. В файлах журналов атакованных узлов при этом останется IP-адрес инфицированного компьютера;
- перехватывать пароли от различных приложений, FTP-клиентов, интернет-сервисов, служб электронной почты;
- получать снимки экрана и перехватывать изображение с подключенной к компьютеру веб-камеры;
- анализировать и перенаправлять сетевой трафик, в том числе с целью извлечения паролей. Перенаправление может происходить в зависимости от заданных условий — в том числе в зависимости от введенных пользователем поисковых запросов;
- подменять открываемые в браузере веб-страницы, в том числе для получения несанкционированного доступа к системам дистанционного банковского обслуживания (ДБО);
- отдавать установленной на инфицированном ПК вредоносной программе различные команды;
- полностью уничтожить операционную систему на зараженном компьютере.

Хищение персональных данных может вызвать такие последствия для жертвы, как:

- Рассылка от имени жертвы спам-сообщений по электронной почте и в социальных сетях.
- В случае дискредитации паролей к FTP-клиентам и панелям управления веб-сайтами (CMS) — установка злоумышленниками на принадлежащие жертве веб-сайты скриптов, осуществляющих перенаправление посетителей на принадлежащие злоумышленникам веб-страницы или загрузку на их компьютеры вредоносного ПО.
- Получение злоумышленниками несанкционированного доступа к системам «Банк-Клиент» и другим системам ДБО.
- Получение злоумышленниками несанкционированного доступа к счетам пользователя в электронных платежных системах (WebMoney, «Яндекс. Деньги» и т. д.).

Кроме вышеописанного, попадание в ботнет может привести к:

- отключению провайдером доступа в Интернет при выявлении фактов распространения из инфицированной сети вредоносного ПО, спама или массового DDoS-трафика;
- значительному снижению быстродействия инфицированных рабочих станций и локальной сети;
- отказу ОС на отдельных инфицированных компьютерах.

Типичные пути заражения

Как правило, заражение происходит:

- Путем самореплицирования вредоносной программы: самостоятельного (без участия пользователя) копирования вредоносной программы на сменные носители и общедоступные ресурсы локальной сети с заражением исполняемых файлов, динамических библиотек и других типов файловых объектов. Подобным образом распространяются файловые вирусы, такие как Win32.Rmnet.16 или Win32.Rmnet.12, заразивший более 4 млн компьютеров по всему миру.
- Путем загрузки на инфицированный компьютер другими вредоносными программами (Backdoor.Andromeda.22).
- При посещении инфицированных веб-сайтов и в момент просмотра веб-страниц, содержащих известные уязвимости браузеров или ОС. При этом жертва может даже не заметить самого момента заражения (Backdoor.Flashback.39).
- При открытии вложений в сообщения электронной почты, полученные в спам-рассылке.
- С использованием методов социальной инженерии. Например, для просмотра размещенного на сайте видеоролика

пользователю предлагается загрузить кодек или обновление, под видом которого распространяется вредоносная программа.

- С применением специально «забытых» и заранее инфицированных флешек либо других носителей информации.

Методы противодействия обнаружению

Некоторые вредоносные программы могут использовать следующие методы противодействия их обнаружению:

- **Антиотладка.** Вредоносная программа пытается определить, не запущена ли она в виртуальной машине, не загружен ли на инфицируемом компьютере отладчик или антивирусная программа (например, методом перечисления запущенных процессов).
- **Использование руткит-технологий.** В частности, с применением специальных драйверов файловой системы вредоносная программа может скрыть присутствие своих компонентов на диске зараженного компьютера.
- **Заражение главной загрузочной записи (MBR), хранение компонентов за пределами таблиц разделов.** Некоторые вредоносные программы могут инфицировать главную загрузочную запись (MBR) и сохранять свои компоненты в свободной области дискового пространства. Получив управление в процессе загрузки ОС, троянец считывает хранящиеся за пределами файловых таблиц модули непосредственно в оперативную память инфицированного компьютера.
- **Исполнение в контексте других запущенных процессов.** Некоторые вредоносные программы имеют возможность встраиваться в запущенные процессы (в том числе в процессы операционной системы) и работать «внутри» данных процессов.
- **Обфускация и криптование.** Нередко злоумышленники шифруют тело вредоносной программы с использованием различных программных упаковщиков с целью сбития сигнатурного детекта антивирусной программой. Иногда насчитывается до нескольких сотен зашифрованных различными упаковщиками модификаций одной и той же вредоносной программы.
- **Организация шифрованного виртуального диска (BackDoor.Tdss).**
- **Блокировка и обход файерволов** (в том числе Windows Firewall), что обеспечивает беспрепятственное получение управляющих сообщений. В том числе использование протокола SOCKS для получения доступа к сервисам.
- **Постоянное изменение реальных адресов управляющего сервера**, а также генерация доменных имен по псевдослучайному принципу, благодаря чему все боты одновременно формируют один и тот же перечень имен — и обращаются к ним.

Методы перехвата информации

- Перехват нажатий клавиш, а также получение скриншотов в реальном времени — для перехвата ввода с виртуальной клавиатуры **(Trojan.PWS.Panda)**.
- Получение скриншота в области экрана, где была нажата левая кнопка мыши, после захода на нужный URL **(Trojan.PWS.Panda)**.
- Анализ трафика и перехват интересующих данных **(Trojan.PWS.Panda)**.
- Получение любых импортируемых сертификатов, а также использованных при удачной авторизации логинов/паролей. В том числе к приложениям, использующим протоколы POP3 и FTP вне зависимости от порта **(Trojan.PWS.Panda)**.
- Перехват HTTP/HTTPS запросов **(Trojan.PWS.Panda)**.
- Анализ и подмена страниц, используемых для ввода банковской информации. Кража TAN-кода (кода активации для проведения платежной операции) **(Trojan.PWS.Panda)**.
- Анализ передаваемых (POST) на определенные адреса данных **(Trojan.PWS.Panda)**.
- Получение данных из буфера обмена **(Trojan.PWS.Panda)**.
- Поиск интересующих файлов и данных с дальнейшим их удалением или закачкой на удаленный сервер **(Trojan.PWS.Panda)**.
- Анализ файлов cookie (данных, связанных с определенным веб-сервером и хранимых на компьютере) и данных сохраненных форм **(Trojan.PWS.Panda)**.
- Веб-инжекты — встраивание в веб-страницы постороннего кода.
- Сбор и отправка на удаленный сервер информации о программно-аппаратной конфигурации ПК.

Обязательные средства защиты

Средство защиты	Необходимость применения
Постоянная антивирусная защита	Позволяет гарантированно обнаруживать вредоносные файлы известных типов, а также вредоносные файлы, неизвестные антивирусу, но действующие в соответствии с известными антивирусному ядру алгоритмами действия.
Антивирусный сканер	Периодическая глубокая проверка дает возможность обнаружения угроз, отсутствовавших в вирусных базах на момент проникновения.
Система ограничения доступа	Позволяет ограничить количество посещаемых интернет-ресурсов до необходимого минимума, что минимизирует риск заражения с сайтов, заведомо содержащих вредоносные объекты.
Система ограничения использования внешних устройств	Позволяет исключить риск заражения с внешних устройств, в том числе флеш-накопителей.
Формирование списка разрешенных приложений	Позволяет уменьшить риск запуска неизвестных приложений без их предварительной проверки на безопасность.
Система проверки интернет-трафика	Позволяет исключить использование уязвимостей клиентского ПО за счет проверки трафика до его поступления в приложения.
Система поверки интернет-ссылок	Позволяет исключить возможность перехода на зараженные и мошеннические ресурсы.
Корпоративный брандмауэр	Позволяет минимизировать риск организации сетевой атаки на ресурсы компании.
Персональный брандмауэр	Исключение возможности атаки через открытые порты.
Система установки обновлений безопасности	Позволяет минимизировать возможность проникновения через известные уязвимости.

* Перечисленные меры защиты должны быть реализованы для всех компьютеров организации, в том числе не имеющих разрешения на выход в Интернет.

Кроме установки и настройки программных средств защиты, рекомендуется:

1) ограничить права пользователей и запретить для них вход в систему с правами администратора;
2) использовать стойкие пароли.

Рекомендуемые средства защиты

Средство защиты	Необходимость применения
Система защиты каналов передачи данных	Обеспечивает безопасный доступ к внешним ресурсам компании, в том числе облачным.
Использование системы удаленного управления мобильным устройством в случае его утери или кражи	Система Антивор позволяет исключить риск утечки конфиденциальной информации (включая пароли доступа к внутренним ресурсам) в случае кражи устройства.
Система сбора информации для служб технической поддержки	▪ Позволяет исключить возможность отключения пользователями систем защиты. ▪ Позволяет устанавливать единые для всей компании или групп пользователей правила информационной безопасности. ▪ Позволяет в случае возникновения той или иной угрозы мгновенно менять настройки системы безопасности.

Корпоративная система защиты от атак	Позволяет обеспечить бесперебойную работу ресурсов компании, а также доступ к внешним, в том числе облачным сервисам.
Система резервного копирования и архивирования	Обеспечивает восстановление поврежденных ресурсов.*
Система защиты от спама	Позволяет обеспечить защиту от проникновения вредоносных программ через спам-сообщения, а также защиту от фишинга.
Система выявления уязвимостей	Периодическое применение системы позволяет находить и устранять возможные уязвимости защищаемой системы.
Система сбора и анализа статистики	Дает возможность контролировать уровень защищенности компании в режиме реального времени, определять источники заражения.

* Восстанавливаемые ресурсы должны проверяться на наличие ранее неизвестных вредоносных программ.

Рекомендуется установить системы защиты — в первую очередь антивирусные — не только на компьютеры и серверы компании, но и на мобильные и домашние компьютеры ее сотрудников, а также их смартфоны.

Причина актуальности угроз

Вышеперечисленные угрозы имеют крайне высокий уровень опасности в связи с:

- наличием прямого неконтролируемого доступа к ресурсам сети Интернет;
- уверенностью большинства пользователей в том, что сам факт использования антивируса является гарантией непроникновения вредоносного кода.

Скомпрометированные средства защиты*

Средство защиты	Методы обхода системы защиты
Использование антивируса в качестве единственного средства защиты от вирусов	Некоторые современные вредоносные программы обладают эффективными средствами обхода антивирусной защиты. Использование методов криптования вредоносного ПО позволяет злоумышленникам оперативно создавать образцы уже известных угроз, сигнатуры которых добавляются в вирусные базы спустя некоторое время после появления троянца.
Парольная защита	Использование методов социальной инженерии.
Ограничение прав пользователей и списка используемых приложений	▪ Проникновение через уязвимости используемых целевой группой приложений, в том числе Adobe Reader, Adobe Flash, приложения для работы с финансовыми средствами. ▪ Внедрение вредоносных программ во время работы под административным аккаунтом обслуживающего персонала.
Использование операционных систем, для которых имеется относительно небольшое количество вредоносных программ	▪ Использование методов социальной инженерии. ▪ Внедрение вредоносных программ через малоизвестные уязвимости.

Пример настройки средств защиты

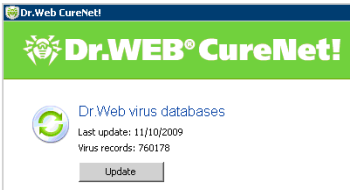
Для периодической проверки системы можно, кроме сканера, входящего в состав используемого антивируса, использовать утилиту Dr.Web CureNet!.

Для получения Dr.Web CureNet! необходимо зарегистрировать серийный номер на данный продукт на странице http://products.drweb.com/register. Непосредственно дистрибутив формируется в момент регистрации — с последними вирусными базами. Если серийный номер Dr.Web CureNet! уже был зарегистрирован, то просто нужно зайти в «Личный кабинет» Dr.Web CureNet! и скачать актуальную версию дистрибутива.

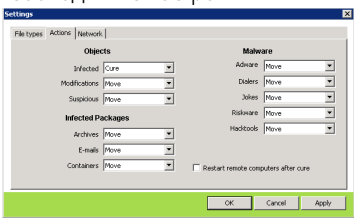
Все проверяемые компьютеры должны быть настроены на работу в той же сети, в которой находится компьютер, с которого будет осуществляться проверка.

После запуска и развертывания продукта:

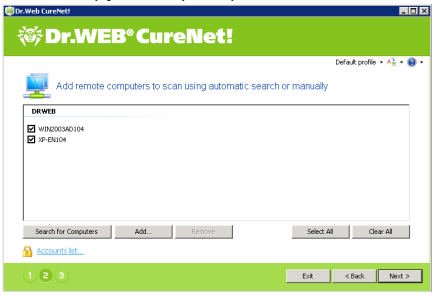
1. Обновите вирусные базы



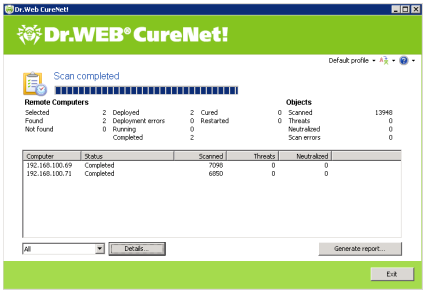
2. Укажите необходимые настройки



3. Создайте список станций сети, на которых будет проводиться антивирусная проверка



4. Запустите проверку



О компании «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности и лидер российского рынка интернет-сервисов безопасности. Антивирусные продукты Dr.Web разрабатываются с 1992 года и имеют сертификаты ФСТЭК России, ФСБ России и Министерства обороны РФ.

Наличие в нашем штате экспертов по различным вопросам, связанным с информационной безопасностью, позволяет нам максимально учитывать особенности работы компаний самого разного размера и профиля деятельности. Мы предлагаем нашим клиентам оптимальный выбор продуктов, имеющих минимальную совокупную стоимость, и, как разработчик этих продуктов, гарантируем их высокое качество. Проверить качество работы наших решений вы можете как с помощью бесплатных лечащих утилит Dr.Web CureNet! и Dr.Web CureIt!, так и с помощью сервиса тестирования наших решений — Dr.Web LiveDemo.