Dr.WEB®
Антивирус

Информационный бюллетень

Безопасность локальных сетей

Дата составления	18.09.12
Текущий уровень опасности	Высокий

Наиболее актуальные угрозы безопасности компаний*	Типы угроз
Вредоносные программы, способные распространяться в локальных сетях и вмешиваться в штатную работу операционной системы, установленной на инфицированном компьютере	Семейство Trojan.Stuxnet Семейство Win32.HLLW.Autoruner Семейство Trojan.Encoder Семейство Win32.HLLW.Shadow Файловые вирусы

* 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: Защита локальных сетей

Причина выпуска бюллетеня

Развитие вредоносных программ и появление новых методик распространения угроз привели к компрометации средств защиты, ранее рекомендованных для применения.

Типичные представители вредоносных программ

К категории наиболее опасных угроз данного типа можно отнести (для всех версий ОС Microsoft Windows):

1. Семейство **Trojan.Stuxnet**
2. Семейство **Win32.HLLW.Autoruner**
3. Семейство **Trojan.Encoder**
4. Семейство **Win32.HLLW.Shadow**
5. Файловые вирусы **(Win32.Rmnet.12, Win32.Rmnet.16)**

Пути и методы проникновения

Наиболее часто встречающимися методами распространения вредоносного ПО являются:

1. Самореплицирование, то есть способность к самостоятельному копированию без непосредственного участия пользователя, в том числе на съемные носители с созданием файла автоматического запуска — это характерная особенность большинства червей и файловых вирусов (в том числе **Win32.Rmnet.12**, **Win32.Rmnet.16**).
2. Распространение в виде вложений в сообщения, распространяемые в форме спам-рассылки по электронной почте.
3. Распространение с использованием методов социальной инженерии, в том числе с платными архивами **(Trojan.Mayachok.1)**, а также под видом «полезного» ПО — кодеков, обновлений, драйверов и т. д.

Кроме этого, распространение вредоносных программ происходит:

1) с использованием набора эксплойтов — уязвимостей, эксплуатирующих ошибки и недокументированные возможности современного ПО, в частности, браузеров и операционных систем;
2) путем использования ботнетов и троянцев-загрузчиков, предоставляющих возможность внедрения программ на зараженные компьютеры.

Причина актуальности угрозы

Данные вредоносные приложения представляют наиболее высокую опасность для локальных сетей, в первую очередь по той причине, что они способны самостоятельно распространяться по открытым на запись общим ресурсам локальных сетей и сетевым дискам методом самокопирования. При этом вредоносные программы используют несколько различных методов: так, некоторые троянцы «прячут» хранящиеся на диске или в сетевой папке файлы, устанавливая для них атрибут «скрытый» или копируя их в отдельную скрытую папку, а вместо «спрятанных» объектов помещают файл ярлыка с тем же именем и расширением .lnk, запускающим вредоносную программу. Представители семейства **Win32.HLLW.Autoruner** способны размещать на инфицированном сетевом диске файл autorun.inf, вследствие чего при открытии диска в Проводнике происходит автоматический запуск вредоносной программы, если эта функция не отключена в настройках операционной системы. Файловые вирусы, такие как **Win32.Rmnet.12** и **Win32.Rmnet.16**, способны не только к саморепликации, но и к заражению файлов различных типов, в том числе исполняемых. В момент запуска инфицированного приложения встроенный в него вредоносный модуль получает управление.

При этом многие троянские программы, распространяясь по локальной сети, способны нанести серьезный ущерб пользователям. Так, вредоносные программы семейства **Trojan.Encoder** шифруют хранящиеся на дисках файлы (изображения, электронные таблицы, иные документы), требуя у жертвы заплатить определенную сумму за их восстановление. В результате деструктивной деятельности **Trojan.Encoder** могут быть безвозвратно утрачены или повреждены ценные данные.

Следует отметить, что некоторые актуальные угрозы, в частности, представители семейства **Trojan.Stuxnet**, обладают функционалом руткитов, иными словами, способны скрывать следы своего присутствия в инфицированной системе, что заметно усложняет их обнаружение и удаление.

Кроме того:

1. Вредоносные программы перед выпуском тестируются на актуальных антивирусах — и некоторое время после релиза не обнаруживаются ими. Помимо этого, вирусописатели используют различные алгоритмы криптования вредоносных программ с применением всевозможных упаковщиков в целях избежать детектирования вредоносного приложения антивирусным ПО.
2. Огромное количество новейших вирусов появляется ежедневно. При этом ежесуточно в вирусные базы добавляется множество записей, соответствующих уникальным образцам ранее известных угроз, модифицированных злоумышленниками с использованием различных упаковщиков. Системы защиты вредоносных программ также постоянно совершенствуются.
3. Для организации защиты от актуальных угроз, не блокируемых эвристическими механизмами антивирусов, необходимо ограничение прав доступа к различным ресурсам и соблюдение правил работы с конфиденциальной информацией.

Цель проникновения

1. Создание бот-сети, состоящей из инфицированных рабочих станций, с целью осуществления массовых спам-рассылок, проведения DDoS-атак по команде, полученной с удаленных управляющих центров.
2. Вымогательство денег за восстановление зашифрованных данных **(Trojan.Encoder)**, а также за предоставление заблокированного вредоносной программой доступа к Интернету **(Trojan.Mayachok.1)** или операционной системе (троянцы-блокировщики).
3. Похищение конфиденциальных данных, в том числе учетных записей почтовых программ, FTP-клиентов **(Win32.Rmnet.12)**, данных для доступа к системам электронного документооборота и системам дистанционного банковского обслуживания (ДБО).
4. Запуск и удаление различных программ на инфицированном компьютере.
5. Удаленное управление инфицированным компьютером, включая возможность перехвата и передачи на контролируемый злоумышленниками удаленный сервер хранящихся на дисках инфицированного компьютера файлов, создания скриншотов и т. д.
6. Удаление на зараженном ПК операционной системы.

Многие вредоносные приложения имеют сложную многокомпонентную структуру, в которой каждый модуль реализует собственный функционал. Так, файловый вирус **Win32.Rmnet.12** обладает модулем бэкдора, способным осуществлять кражу конфиденциальных данных, собственным FTP-сервером, несколькими другими функциональными модулями. Кроме того, данный вирус (равно как и его модификация **Win32.Rmnet.16**) обладает возможностью заражать исполняемые файлы на съемных накопителях и сетевых дисках, а потому представляет особую опасность для пользователей локальных сетей.

Методы перехвата информации

Некоторые вредоносные программы обладают возможностью кражи конфиденциальных данных пользователя. Среди используемых ими методов перехвата приватной информации можно выделить следующие:

1) запись нажатий пользователем клавиш (кейлоггинг);
2) перехват информации, вводимой пользователем в браузере (в том числе во время работы с системой «Банк-Клиент»);
3) перехват и анализ сетевого трафика в поисках учетных данных и передаваемых значений экранных форм;
4) передача на удаленный сервер злоумышленников файлов cookies;

5) кража и передача на удаленный сервер злоумышленников файлов цифровых сертификатов;
6) встраивание в процессы программ системы «Банк-Клиент» (**Trojan.Carberp** – на данный момент существуют версии программы под большинство систем дистанционного банковского обслуживания);
7) создание скриншотов в моменты ввода важной информации (в том числе через виртуальную клавиатуру);
8) перехват функций, которые могут участвовать в передаче данных;
9) создание дополнительных полей ввода данных каждый раз, когда пользователь посещает сайты банков, что позволяет запрашивать у жертвы номера счетов и паролей доступа.

Методы маскировки от средств контроля и наблюдения

1. Использование специальных драйверов-фильтров файловой системы, способных скрывать присутствие на диске компонентов вредоносной программы **(Trojan.Stuxnet)**.
2. Использование систем криптования в целях избежать детектирования антивирусным ПО по сигнатурам известных угроз.
3. Поиск и закрытие процессов программ-отладчиков, брандмауэров и антивирусных программ.
4. Проверка окружения на предмет выявления факта использования программных средств виртуализации (виртуальных машин).
5. Внедрение в другие работающие приложения – без использования собственного процесса.
6. Подмена цифровых сертификатов, файлов cookies.
7. Блокировка доступа к различным ресурсам сети Интернет, в том числе серверам обновлений систем безопасности.
8. Внедрение на уровень MBR, благодаря чему вредоносная программа может загружаться в оперативную память раньше операционной системы, что затрудняет ее детектирование и удаление.

Обязательные средства защиты

Средство защиты	Необходимость применения
Система ограничения доступа	▪ Позволяет ограничить доступ на запись к общим сетевым ресурсам, предотвратив распространение вредоносных программ, обладающих способностью к саморепликации. ▪ Позволяет ограничить количество посещаемых ресурсов Интернета до необходимого минимума, что минимизирует риск заражения с сайтов, содержащих вредоносные объекты. ▪ Позволяет исключить возможность деактивации пользователями программных средств защиты.
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.
Антивирусный монитор	Позволяет исключить заражение с помощью вредоносных объектов, проникших на машину пользователя без проверки – в том числе в запароленных архивах или с помощью специальных протоколов передачи данных.
Антивирусный сканер	Периодическая проверка дает возможность обнаружения ранее неизвестных вирусов, находящихся в неактивированном виде.
Персональный брандмауэр	Исключение возможности проникновения через открытые порты.

Кроме установки и настройки программных средств защиты, рекомендуется:

1) ограничить права пользователей и запретить для них вход в систему под учетной записью администратора сети или локального компьютера;
2) использовать стойкие пароли;
3) ограничить доступность ресурсов Интернета на отдельных компьютерах сети, содержащих конфиденциальную информацию;
4) ограничить возможность подключения пользователями съемных носителей информации к рабочим станциям, содержащим конфиденциальную информацию или использующим критичные приложения;
5) своевременно устанавливать все обновления системы безопасности и операционной системы.

Внимание! Перечисленные меры защиты позволяют уменьшить риск заражения вредоносными программами, проникающими в локальную сеть через зараженные (в том числе взломанные) сайты, системы показа рекламной информации, а также путем взлома машин пользователей.

Внимание! Перечисленные меры защиты должны быть приняты на всех компьютерах, на которых производится работа с финансовыми средствами, – в том числе в обязательном порядке на компьютерах и мобильных устройствах, функционирующих на ОС Windows и Android, а также на всех смартфонах.

Рекомендуемые средства защиты

Средство защиты	Необходимость применения
Система централизованного управления	▪ 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.
Система сбора и анализа статистики	Дает возможность контролировать уровень защищенности компании в режиме реального времени, определять источники заражения.
Система сбора информации для служб технической поддержки	Позволяет минимизировать время решения тех или иных проблем.
Система установки обновлений безопасности	Позволяет минимизировать возможность проникновения через известные уязвимости.

Скомпрометированные средства защиты

Средство защиты	Методы обхода системы защиты
Виртуальная клавиатура	Снятие скриншотов во время ввода информации
Использование цифровых сертификатов для подписи файлов	Кража и компрометация сертификатов
Отключение входящих соединений на время работы системы ДБО	Использование уязвимостей для проникновения в целевую систему
Использование программ, работающих в защищенном окружении (в том числе Java)	Подмена программных компонентов
Использование внешних средств, гарантирующих соответствие вводимой и отправляемой информации	Подмена программных компонентов, установленных на компьютере, к которому подсоединен внешний модуль
Использование защищенного соединения	Внедрение вредоносных программ, позволяющих перехватить передачу данных
Использование загружаемой операционной системы (LiveCD)	Внедрение вредоносных программ на уровне BIOS (буткиты)

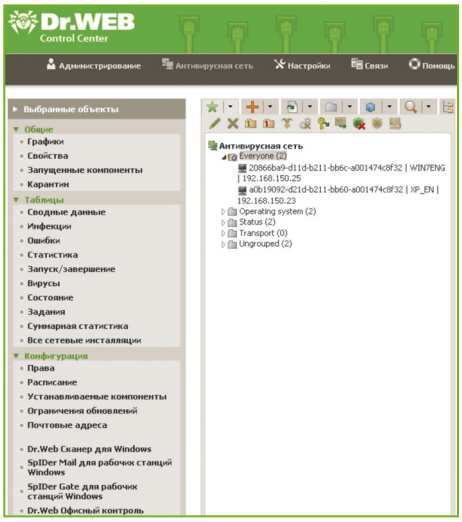
С момента выпуска предыдущего бюллетеня появились сведения о возможности обхода вредоносными программами двухшаговых систем аутентификации (например, включающих использование карты с чипом и пинкода). Кроме этого, был зафиксирован факт перехвата одноразовых паролей, высылаемых банком в виде СМС-сообщений.

Пример настройки средств защиты

В качестве примера рассмотрим настройку системы ограничения доступа для операционной системы Windows.

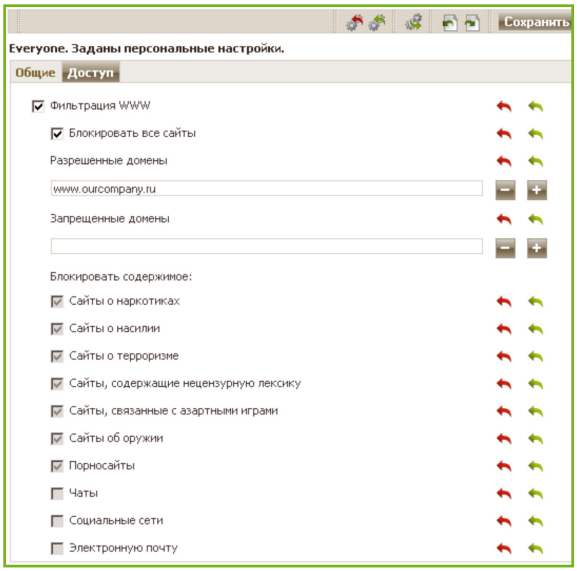
Внимание! Защищена должна быть любая операционная система, с которой переводятся денежные средства или хранится конфиденциальная информация, — в том числе операционные системы семейств Windows, Linux, Android.

Для настройки параметров доступа необходимо в окне системы управления выбрать предустановленную группу **Everyone** или (в случае необходимости задания индивидуальных правил безопасности) любую иную группу или отдельную станцию, а затем выбрать пункт **Офисный контроль**.

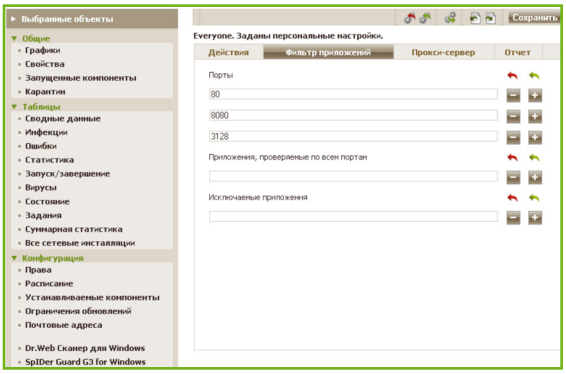


На странице **Офисный контроль** необходимо, выбрав закладку **Доступ**, отметить **Фильтрация WWW**, определить режим блокировки **Блокировать все сайты** и задать список разрешенных сайтов.

Для сохранения настроек необходимо нажать кнопку **Сохранить**.

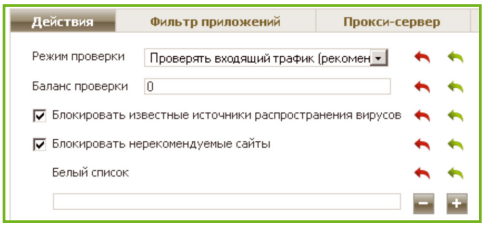


После этого рекомендуется с помощью настроек модулей **SpIDer Gate для рабочих станций Windows** (закладка **Фильтр приложений**) и **Firewall** определить список приложений, которым запрещен выход в Интернет.



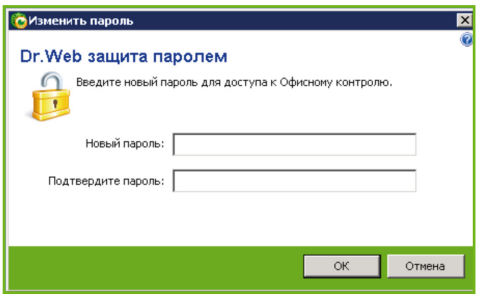
В соседней закладке **Действия** необходимо проверить наличие отметок у пунктов **Блокировать известные источники распространения вирусов** и **Блокировать нерекомендуемые сайты**.

Для сохранения настроек необходимо нажать кнопку **Сохранить**.

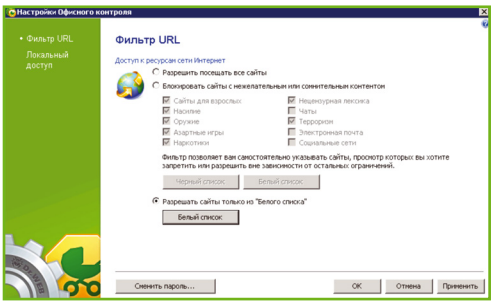


Защита системы ограничения доступа на уровне отдельной рабочей станции

Щелкните правой кнопкой мыши значок в системном трее. Выберите пункт **Настройки Офисного контроля**. Если вы настраиваете права доступа впервые, то вам будет предложено задать пароль и логин доступа. По умолчанию пароль отсутствует. Не рекомендуется не использовать пароли, а также использовать простые, легко поддающиеся взлому пароли — это сводит на нет все усилия по обеспечению безопасности. Задав пароль, нажмите на кнопку **OK**.



Если вы хотите запретить доступ ко всем сайтам, кроме избранных, то на закладке **Фильтр URL** выберите **Разрешать сайты только из «Белого списка»**, нажмите кнопку **Белый список** и введите имена разрешенных ресурсов сети Интернет. После формирования полного списка разрешенных ресурсов нажмите кнопку **Применить** или **OK**.



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.