Dr.WEB®
Антивирус

Информационный бюллетень

Безопасность локальных сетей

Дата составления	02.07.12
Текущий уровень опасности	Высокий

Наиболее актуальные угрозы безопасности компаний*	Дополнительная информация
Вредоносные программы, создаваемые для кражи финансовых средств, в том числе с банковских карт и систем дистанционного банковского обслуживания, используемых компаниями	Тема выпуска
Вредоносные программы, создаваемые для мобильных устройств	Информационный бюллетень от 15.05.12, http://news.drweb.com, https://blogs.drweb.com
Проникновение вредоносных программ с личных компьютеров и устройств пользователей	

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

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 финансовых средств

Причина выпуска бюллетеня

Развитие вредоносных программ и появление новых методик кражи финансовых средств привело к компрометации средств защиты, ранее рекомендованных для применения.

Типичные представители вредоносных программ

К категории наиболее опасных можно отнести:

1) для всех версий Windows: **Trojan.Carberp**, **Trojan.PWS.Ibank**, **Trojan.PWS.Panda** (также известен как Zeus и Zbot) и **Trojan.PWS.SpySweep** (также известен как SpyEye);
2) для ОС Android: **Android.SpyEye.1**.

Пути и методы проникновения

В большинстве случаев заражение происходит автоматически при просмотре инфицированных веб-сайтов (**Trojan.Carberp**). При этом членами криминальных группировок взламываются сайты, наиболее часто посещаемые финансовыми работниками и руководителями компаний в силу должностных обязанностей, – финансовые, информационные, публикующие тексты законов и распоряжений.

Кроме этого, распространение вредоносных программ происходит:

1) с использованием набора эксплойтов Black Hole Exploit Kit – коллекции уязвимостей, эксплуатирующих ошибки и недокументированные возможности современного ПО, в частности, браузеров и операционных систем (**Trojan.Carberp**);
2) путем использования ботнетов и иных вредоносных программ, предоставляющих возможность внедрения программ на зараженные компьютеры.

Причина актуальности угрозы

1. Вредоносные программы перед выпуском тестируются на актуальных антивирусах – и некоторое время после релиза не обнаруживаются ими. В то же время для перевода денег криминальной структурой, имеющей четкую организацию, требуется от одной до трех минут.
2. Огромное количество новейших вирусов появляется ежедневно. По данным http://updates.drweb.com, каждый день выходит несколько десятков экземпляров только **Trojan.Carberp**. Системы защиты вредоносных программ 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.

В 2011 году 40% атак увенчались успехом, при этом средняя сумма хищения составляла 450 тыс. руб.

Цель проникновения

1) похищение сертификатов систем защищенного документооборота и паролей от программ – в первую очередь систем дистанционного банковского обслуживания и торговых платформ (**Trojan.Carberp**, **Trojan.PWS.Panda**);
2) перевод денежных средств компании через системы ДБО;
3) похищение конфиденциальной информации (**Trojan.PWS.SpySweep**, **Android.SpyEye.1**);
4) включение зараженных машин в управляемые ботнеты, координируемые из одного (или нескольких) командных центров (**Trojan.Carberp**);
5) запуск и удаление различных программ на инфицированном компьютере (**Trojan.Carberp**, **Trojan.PWS.SpySweep**, **Trojan.PWS.Panda**);
6) установка сеанса «Удаленного рабочего стола» и выполнение команд злоумышленников (**Trojan.Carberp**, **Trojan.PWS.Panda**, **Trojan.PWS.SpySweep**);
7) удаление на зараженном ПК операционной системы (**Trojan.Carberp**);
8) включение и выключение зараженного компьютера в заданное время (**Trojan.PWS.Panda**).

Кроме того, **Trojan.Carberp**, имея расширяемую архитектуру, дает возможность владельцам криминальной сети загружать специальные встраиваемые дополнения (плагины) для выполнения дополнительных деструктивных действий, в том числе для проведения атаки на целевую компанию.

Методы перехвата информации

1) запись нажатий пользователем клавиш (**Trojan.Carberp**);
2) перехват информации, вводимой пользователем в браузере (в том числе во время работы с банком) (**Trojan.PWS.Panda**);
3) подмена страниц банковских сайтов – в просматриваемую пользователем веб-страницу осуществляется инъекция постороннего содержимого, которое может включать различный текст или веб-формы. Таким образом, ничего не подозревающая жертва загружает в браузере настольного компьютера или ноутбука веб-страницу банка, в котором у нее открыт счет, и обнаруживает сообщение о том, что банком введены в действие новые меры безопасности, без соблюдения которых пользователь не сможет получить доступ к системе «Банк-Клиент», а также предложение загрузить на мобильный телефон специальное приложение, содержащее троянскую программу (**Android.SpyEye.1**);
4) анализатор трафика и вклинивание в интернет-трафик в поисках учетных данных и передаваемых значений экранных форм (**Trojan.Carberp**);
5) встраивание в процессы программ системы «Банк-Клиент» (**Trojan.Carberp** – на данный момент существуют версии программы под большинство систем дистанционного банковского обслуживания);
6) создание скриншотов в моменты ввода важной информации (в том числе через виртуальную клавиатуру);
7) перехват функций, которые могут участвовать в передаче данных;
8) перехват сообщений СМС (**Android.SpyEye.1**);
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) внедрение в другие работающие приложения – без использования собственного процесса (**Trojan.Carberp**, **Trojan.PWS.SpySweep**);
2) шифрование вирусными упаковщиками (**Trojan.Carberp**);
3) деактивация используемых антивирусов (**Trojan.Carberp**);
4) уничтожение «конкурирующих» вредоносных программ (**Trojan.Carberp**);
5) подмена цифровых сертификатов, файлов cookies (**Trojan.PWS.Panda**);
6) подмена домашней страницы в браузерах (**Trojan.PWS.Panda**);
7) блокировка доступа к различным ресурсам сети Интернет, в том числе серверам обновлений систем безопасности (**Trojan.PWS.Panda**);
8) внедрение на уровень MBR, использование руткит-технологий (**Trojan.Carberp**);
9) перехват защищенного протокола HTTPS (SSL/TLS соединения) между браузером и банком (**Trojan.Inject1.147**). На стороне соединения браузера используется поддельный сертификат, вместо сертификата, отправляемого банком, что делает процесс передачи информации недоверенным и позволяет выполнять любые манипуляции вплоть до повторного шифрования, с использованием данных банка перед отправлением в банк для обработки.

Кроме этого, с момента выпуска предыдущего бюллетеня появились сведения о возможности предоставления жертвам фальшивых балансовых отчетов, что позволяет в течение долгого срока скрывать факт хищения и препятствует возврату средств. Внедрение новых методик позволяет переводить средства небольшими суммами, что позволяет обойти как банковские средства контроля, так и средства контроля, основанные на необходимости подтверждения перевода больших сумм с помощью СМС.

Обязательные средства защиты

Средство защиты	Необходимость применения
Система ограничения доступа	▪ Позволяет ограничить количество посещаемых ресурсов до необходимого минимума, что минимизирует риск заражения с сайтов, содержащих вредоносные объекты. ▪ Позволяет исключить возможность отключения пользователями 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) разрешить выход в Интернет только с отдельных компьютеров сети, не содержащих конфиденциальной информации;
3) использовать операционные системы, для которых создано меньшее количество вредоносных программ;
4) своевременно устанавливать все обновления системы безопасности и использовать стойкие пароли.

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.

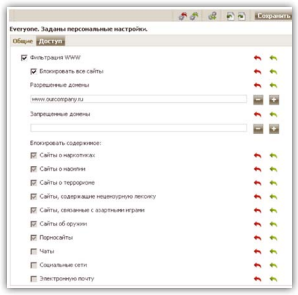
Внимание! Защищена должна быть любая операционная система, с которой переводятся денежные средства или хранится конфиденциальная информация, — в том числе операционные системы Windows, Linux, Android.

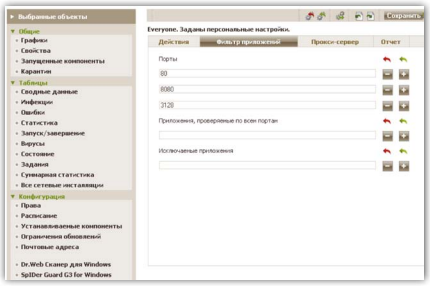
Защита системы ограничения доступа с помощью централизованной системы управления

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**.

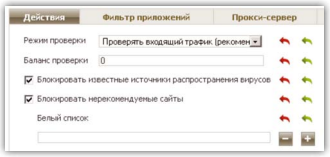




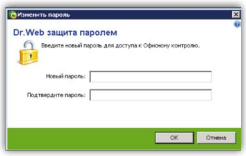
После этого рекомендуется с помощью настроек модулей **SpIDer Gate для рабочих станций Windows** (закладка **Фильтр приложений**) и **Firewall** определить список приложений, которым запрещен выход в Интернет.

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**.