Dr.WEB®
ATM Shield

Первый на российском рынке

Централизованная защита встроенных компьютерных систем

(банкоматов, платежных терминалов, мультикиосков, кассовых сетей и др.)

В марте 2009 года в России была обнаружена первая вредоносная программа, заражающая банкоматы.

Инфицированные троянцем **Trojan.Skimer** банкоматы были обнаружены в Москве, а затем и в Санкт-Петербурге.

Первой на эту угрозу отреагировала компания **«Доктор Веб»**, которая сообщила о **Trojan.Skimer**, а затем и создала специализированный антивирус, в режиме реального времени защищающий от вирусов встроенные компьютерные системы (банкоматы, платежные терминалы, мультикиоски, кассовые сети) – **Dr.Web ATM Shield.**

Dr.WEB®
ATM Shield

Признайте, вы ведь тоже это делаете?

- Используете USB-устройства, не проверяя их на вирусы?
- Открываете почту от неизвестных отправителей?
- Работаете под Windows с правами администратора?
- Не производите обновления безопасности всего программного обеспечения, установленного на ПК?
- Выходите в Интернет с рабочего компьютера, на котором стоит ПО, у которого есть уязвимости?
- Используете простые пароли, взлом которых не составляет труда?

Почему вы думаете, что персонал, обслуживающий банкоматы и терминалы, не поступает так же?

А есть ли вирусы для банкоматов?

Специализированных вирусов для банкоматов – вредоносных программ, способных к саморазмножению, – пока не найдено. А вот количество троянских программ увеличивается постоянно! За один только месяц – декабрь 2013 года – появилось 4 новых троянца для банкоматов: Trojan.Ploutus.1, Trojan.Ploutus.2, Trojan.Skimer.19 и Trojan.PWS.OSMP.21.

Некоторые характерные особенности банкоматных троянцев:

- управление вредоносной программой с помощью специальным образом подготовленных мастер-карт, с мобильного устройства;
- перехват и расшифровка PIN-кода после его ввода владельцем **с использованием программного обеспечения самого банкомата!**;
- хищение данных с банковских карт; сохранение похищенных данных на специально подготовленной пластиковой карте злоумышленников или распечатка их на кассовом чеке;
- выдача денежных средств из банкомата по команде злоумышленников, переданной троянцу через клавиатуру банкомата или через специально сформированное СМС-сообщение.

Банкоматы обслуживаются квалифицированными сотрудниками — как туда может попасть что-то вредоносное?

Заражения возможны:

- **со сменных носителей**, предназначенных для проведения регламентных работ на банкомате обслуживающим персоналом, но также используемых ими и в личных целях;
- **со сменных носителей** преступников, для чего аппаратный отсек банкомата вскрывается с помощью специального ключа;
- из-за проникновения вредоносных программ **из зараженной внутренней сети** компании – в случае наличия из нее доступа к встраиваемым системам;
- из-за наличия в программном обеспечении банкомата **уязвимостей**.

Даже если в банкомат попадет «обычная» вредоносная программа, не умеющая работать с денежными средствами и банковскими картами, – «синий экран», шифрование информации с выводом на монитор требования о выкупе и, как результат, фотографии по всему Интернету и потеря репутации – это не только неприятно, но и требует затрат на восстановление работоспособности оборудования.

Dr.Web ATM Shield — это не только антивирус!

Dr.Web ATM Shield включает средства, существенно ограничивающие возможности для умышленного или неумышленного заражения банкоматов:

- файловый монитор обеспечивает невозможность запуска известных вредоносных программ;
- антируткит обеспечивает обнаружение ранее неизвестных угроз;
- Офисный контроль ограничивает возможности работы с локальными каталогами и интернет-ресурсами, что не позволяет вредоносной программе передать данные своему «хозяину» или подключиться к управляющему центру;
- запрет использования сменных носителей исключает внедрение вредоносных программ с неизвестных сменных устройств
- система контроля интернет-трафика обеспечивает выход в Интернет только разрешенных программ и по разрешенным портам.

Dr.WEB®
ATM Shield

Dr.Web ATM Shield специально разработан для противодействия типичным угрозам для встраиваемых устройств

Что говорят регуляторы?

PCI DSS v3. Требование 5: Должно использоваться и регулярно обновляться антивирусное программное обеспечение.

5.1. Антивирусное программное обеспечение должно быть установлено на всех системах, подверженных воздействию вредоносных программ (особенно на персональных компьютерах и серверах).

5.2. Механизмы антивирусной защиты должны регулярно обновляться, постоянно работать и поддерживать ведение журналов аудита.

Применение Dr.Web ATM Shield позволяет полностью выполнить требования стандартов PCI-DSS v2 и v3 в области антивирусной защиты

Зачем использовать специализированное решение, когда можно установить обычный антивирус?

Характерными признаками встраиваемых устройств являются:

- малое количество оперативной памяти и относительно слабый процессор;
- необходимость работать без перезагрузок в круглосуточном режиме;
- использование помимо обычных операционных систем ОС для встраиваемых устройств.

Dr.Web ATM Shield специально разработан для работы на слабых аппаратных конфигурациях

Для нормальной работы Dr.Web ATM Shield достаточно наличия во встраиваемом устройстве 512 МБ оперативной памяти.

Традиционным отличием продуктов Dr.Web, в том числе и Dr.Web ATM Shield, являются компактные вирусные базы и малый размер обновлений, что позволяет защищать удаленные устройства, имеющие «узкий» канал выхода в Интернет или сеть компании.

Dr.Web ATM Shield поддерживает операционные системы для встраиваемых устройств

Dr.Web ATM Shield может использоваться не только на обычных операционных системах – таких как Windows® XP Professional, Windows® Vista и Windows® 7 и Windows® 8, но и на Windows® XP Embedded, Windows® 7 Embedded, Windows® 8 Embedded.

Dr.Web ATM Shield – это не просто антивирус!

Это еще и:

- технологии, позволяющие минимизировать время проверки и загрузки (в том числе за счет многопоточной проверки и отложенной проверки файлов, открываемых «на чтение»);
- стабильная работа системы даже на компьютерах с устаревшей конфигурацией;
- современное антивирусное ядро, позволяющее находить и обезвреживать новейшие вирусы, еще не занесенные в вирусные базы, в том числе и скрытые под неизвестными упаковщиками;
- мощная система самозащиты, которая не дает возможности вирусам вывести систему из строя.

Dr.Web ATM Shield – единственное решение, учитывающее особенности встраиваемых устройств.

Внимание!

Кража средств с помощью вредоносного ПО является противоправным действием, при совершении которого могут присутствовать признаки преступлений, предусмотренных ст. ст. 159, 159.6, 165, 272 и 273 УК РФ.

Компания «Доктор Веб» оказывает услуги по **экспертизе вирусозависимых компьютерных инцидентов**, а также проводит психологическую экспертизу личностей (персонала) с целью выявления фактов причастности к совершению / пособничеству / укрывательству / поощрению противоправных действий в отношении заказчика, фактов бездействия или халатного отношения к служебным обязанностям.

http://antifraud.drweb.com/expertise/

На сайте «Доктор Веб» в разделе «Правовой уголок» http://legal.drweb.com/ размещены образцы заявлений в правоохранительные органы и другие инстанции, а также рекомендации по действиям после обнаружения хищения. Пользуйтесь этой информацией!

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web.

Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Антивирусная защита Dr.Web позволяет информационным системам клиентов эффективно противостоять любым, даже неизвестным угрозам.

«Доктор Веб» стал первой компанией, предложившей на российском рынке инновационную модель использования антивируса в качестве услуги, и по сей день продолжает оставаться безусловным лидером российского рынка интернет-сервисов безопасности для поставщиков ИТ-услуг. Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

Среди клиентов «Доктор Веб» – крупные компании с мировым именем, российские и международные банки, государственные организации, учебные заведения и научно-исследовательские институты, сети которых насчитывают десятки тысяч компьютеров. Антивирусным решениям «Доктор Веб» доверяют высшие органы государственной и исполнительной власти России, компании топливно-энергетического сектора.

«Доктор Веб» — российский разработчик средств информационной безопасности. Антивирусные продукты Dr.Web разрабатываются с 1992 года.
125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Тел.:+7 (495) 789–45–87 (многоканальный);
Факс: +7 (495) 789–45–97.
http://www.drweb.com | http://www.av-desk.com | http://freedrweb.com | http://mobi.drweb.com