Dr.WEB®
с 1992 года

Защити созданное

Защита касс и терминалов

Недооцененная опасность и защита от нее с помощью Dr.Web

POS-терминалы нескольких сотен заведений крупной сети фаст-фудов Wendy's оказались **заражены** трояном похищающим данные кредитных карт. https://xakep.ru/2016/05/12/wendys/

Это – только один из официально признанных случаев заражения торговой сети. Но огромное количество заражений не получает освещения в СМИ. Какова реальная ситуация с безопасностью устройств в локальных сетях торговых организаций?

Перед вами – иллюстрация результата эпидемии троянца NePetya (он же Лже-Петя) — паралич процесса продаж. Эта вредоносная программа не была направлена специально на торговое оборудование, но заразила и его. Заражение торгового оборудования – это деньги, которые покупатели могли бы оставить в магазине. Но не оставили...

Торговое оборудование (кассы и терминалы) должно быть защищено антивирусом аналогично обычным компьютерам.

Чем кассы и терминалы привлекают злоумышленников?

Trojan.MWZLesson – троянская программа, предназначенная для заражения платежных терминалов и имеющая в своем составе модуль, сканирующий оперативную память инфицированного устройства на наличие в ней треков банковских карт.

Заражение кассовых компьютеров позволяет преступникам получать данные банковских карт, пароли и логины администраторов сети, имеющих доступ к данным устройствам.

Очень часто администраторы используют один и тот же пароль доступа к разным ресурсам, а значит, злоумышленник может отключить антивирусную защиту с сервера сети.

Торговое оборудование также может быть заражено вредоносными программами специальной разработки – с целью сбора статистики продаж в интересах конкурентов или «корректировки» параметров товаров и услуг, продающихся в магазине.

Как вредоносные программы могут проникать в торговые сети?

- Через уязвимости
- С помощью социальной инженерии
- Через сменные носители
- По локальной сети
- Через подмененный POS-терминал

Так компонент нескольких вредоносных программ BackDoor.Neutrino.50 использует для распространения эксплойты для уязвимости CVE-2012-0158.

Защити созданное

! Как правило, кассовое оборудование не обновляется, поэтому содержит множество уязвимостей.

! Вредоносная программа может быть изначально размещена в поставляемом устройстве. Либо ее могут «занести» сотрудники обслуживающей организации. Современные устройства, в том числе POS-терминалы, имеют USB-разъемы, к которым можно подключить зараженный носитель.

Почему кассы и торговые терминалы так легко заразить?

POS-устройства (Point Of Sale — точка продажи), в частности кассы, терминалы, электронные весы – обычные компьютеры. Во многих из них используются процессоры Intel и ОС Windows или Linux.

https://habrastorage.org/files/6b5/663/2e4/6b56632e4a9b4c51bed81246b5c2a8f7.JPG

Кассовые компьютеры весьма производительны. Их конфигурация на основе четырехъядерных процессоров J1900 с частотой 2,4 ГГЦ и более и ОЗУ от 2–4 ГБ отлично подойдет для решения большинства офисных задач.

Поскольку POS-устройства построены на основе стандартных программных и аппаратных компонентов, разработка вредоносных программ для них не представляет труда. Более того, кассы и терминалы легко заражаются и «обычными» вредоносными программами, не предназначенными специально для POS-устройств. Например, шифровальщиками.

Чем защищать POS-устройства?

Если имеется возможность установки антивируса, рекомендуется использовать Dr.Web со следующими активированными компонентами:

- Файловый монитор Dr.Web SpIDer Guard
- Веб-антивирус Dr.Web SpIDer Gate
- Превентивная защита Dr.Web
- Контроль доступа к устройствам в рамках Офисного контроля

Dr.Web – система защиты от вредоносных программ любой сложности и назначения.

- Наличие драйвера самозащиты не позволяет злоумышленникам вывести антивирус из строя.
- Защищенная система обновлений гарантирует получение «лекарства».
- Современные технологии находят троянца, где бы он ни прятался.

Установка Dr.Web позволяет защитить POS-устройства от проникновения вредоносных программ, сканирования по сети с целью поиска незащищенных объектов, а также от запуска ранее неизвестных угроз.

Использование системы контроля доступа к устройствам и Превентивной защиты позволяет ограничить использование сменных устройств, предотвратить доступ к ресурсам компьютера.

! Помимо POS-устройств необходимо защищать также серверы и рабочие станции, с которых имеется доступ к ним. Те устройства, на которые установить защиту невозможно, рекомендуется выделить в отдельную подсеть, отделив их от обычных компьютеров и серверов, и установить систему проверки трафика на входе в эту подсеть.

Рекомендуем продукты

Центр управления Dr.Web — лицензируется бесплатно.

Dr.Web Desktop Security Suite, Комплексная защита

Dr.Web Server Security Suite

Dr.Web Gateway Security Suite

СКИДКА 25%

при покупке лицензии на три продукта Dr.Web.

Централизованное управление антивирусной защитой торговой сети – единственное средство для минимизации потерь при атаке хакеров или случайном заражении!

Защити созданное

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

www.антивирус.рф | www.drweb.ru