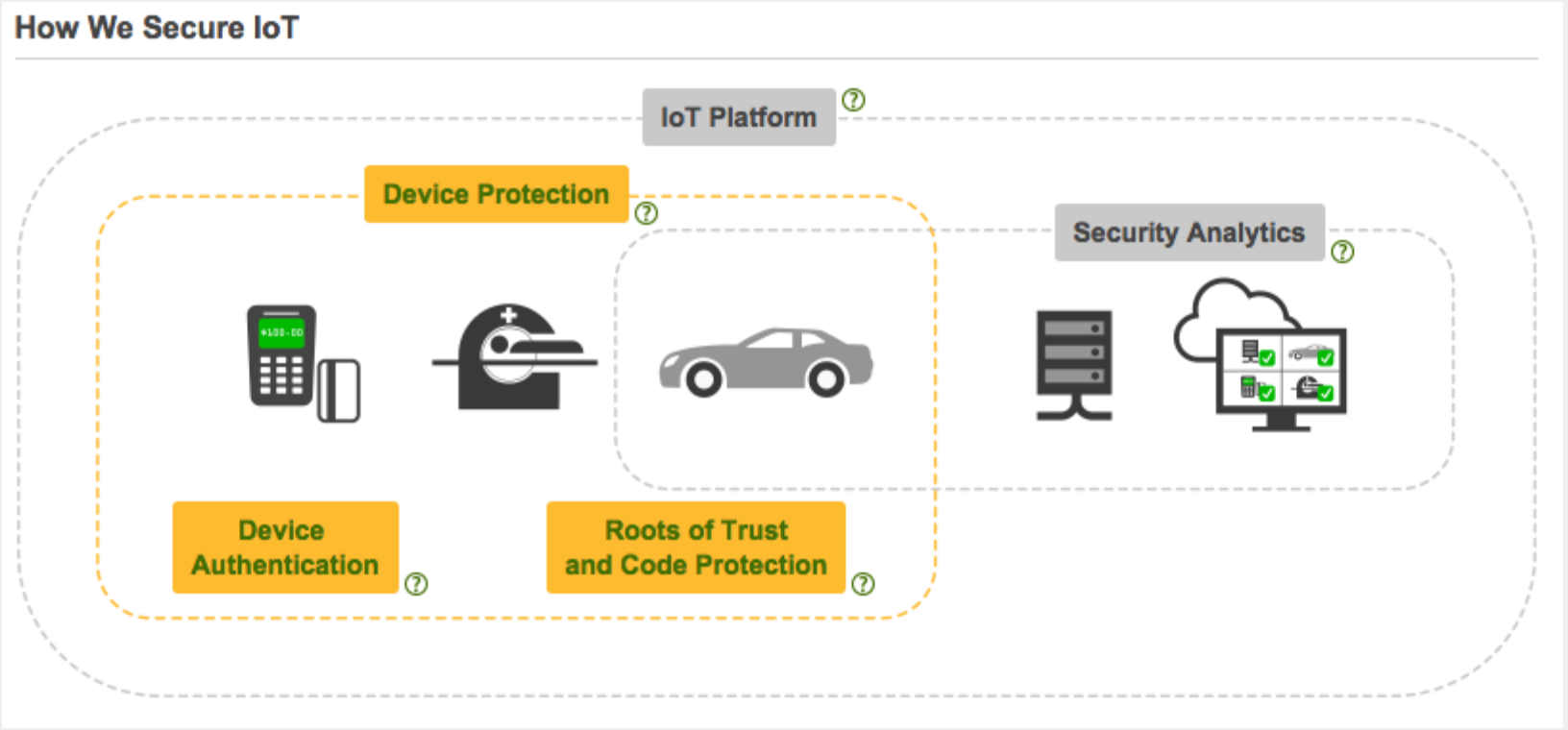
Обеспечение безопасности устройств «Internet of Things» Комплексная защита платежных сервисов от терминалов до центров обработки данных

Петр Сергеев

Symantec Corporation

Защита устройств, имеющих выход в Интернет



- постоянно подключены к сети,
- остающиеся без внимания пользователей,
- часто оставляют неизменными заводские параметры.

Почему стоит доверять Symantec?

Защита разнообразных устройств, имеющих выход в интернет, в том числе банкоматов и платежных терминалов.
Защищаем **более одного миллиарда устройств IoT** (август 2015)

- **Wincor Nixdorf** (Каран Оберой, глобальный продукт-менеджер программное обеспечение безопасности): ключевые технология безопасности Symantec в сочетании с опытом Wincor Nixdorf создали решение, которое предлагает лучшие в своем классе защиту от программных атак на банкоматы.

- **Texas Instruments (TI)** Гил Рейтер, директор по стратегическому маркетингу IoT: чтобы помочь клиентам обеспечить безопасные облачные коммуникации, TI встраивает сертификат Symantec, в устройства ИТН для цифровой подписи и аутентификации обновлений программного обеспечения."

IoT: Архитектура риска

Любой элемент в архитектуре IoT может служить потенциальной угрозой - от примитивных устройств собирающих информацию, до серверов на которых она обрабатывается.

Internet of Things and Privacy

1 in 4 Каждый из четырех человек **не знает** (не помнит, не понимает) какие доступы он предоставляет своим приложениям.

68% Готовы пожертвовать персональными данными, если приложение будет бесплатным

Source: 2015 Norton Global Survey

Backoff: 2014

Backoff: **2014**

- Позволяет удаленно похищать финансовую информацию, в том числе данные банковской карты
- Вирус оснащен модулями обновления и установки вредоносного ПО
- Распространители Backoff контролировали доступность инфицированных POS-терминалов при помощи IP-камер видеонаблюдения
- Атаковали за счет установленных по умолчанию паролей для маршрутизаторов и камер наблюдения, а также путем использования известных уязвимостей

TYUPKIN Март 2014

Цель	Процесс	Действие
Банкоматы без сигнализации, слабо защищенные (физически)	Атакующий запускает загрузочный CD Вредонос блокирует защитное ПО (Mc**e S**e)	Запускается только в ночь воскресенья и понедельника. Блокирует сеть. Опусташает касеты с $$$.

После ввода правильного ключа угроза показывала объем наличных в каждой кассете, позволяя злоумышленникам получить 40 банкнот из кассеты. Угроза самоустраняется по команде.

PLOUTUS Март 2014

Установленный смартфон взаимодействует с Windows Open Service Architecture (WOSA) eXtensions for Financial Services (XFS)

Trojan.Nitovel May 25, 2015

- **Подвержены:** Windows 2000, Windows 7, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Server 2008, Windows Vista, Windows XP. (144,384 bytes)
- После запуска копирует себя с помощью Alternate Data Streams (ADS)
- С помощью ADS создает скриптик
- Создает в автозапуске ссылку на данный скрипт
- Сканирует память устройства на наличие платежных данных карт и отправляет их выгодоприобретателю :o))

FUNCTION4 еще известна как GREENDISPENSER

Середина сентября 2015

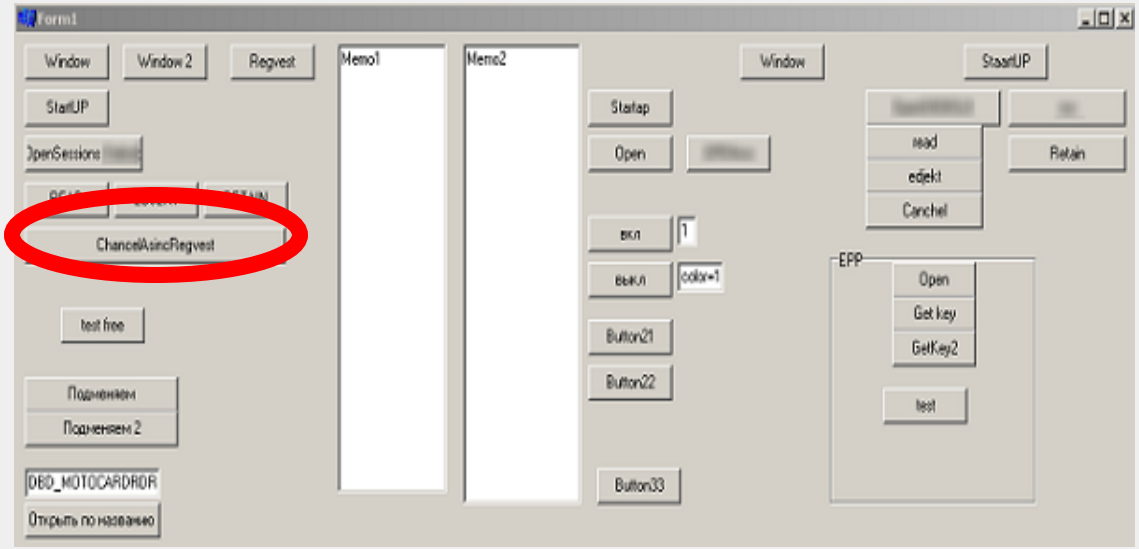
Цель	Описание	Действия
Устройства NCR & Wincor	Соединение с портом периферийных устройств и установка вредоноса	Отдает денньги Удаляет себя

Атакующие вводили команды с устройства ввода пин-кода

Динамический PIN уникален для каждого сеанса запуска, и сгенерирован из QR code, который показывался на пораженном ATM после ввода статического pin.

SUCEFUL

Середина сентября 2015



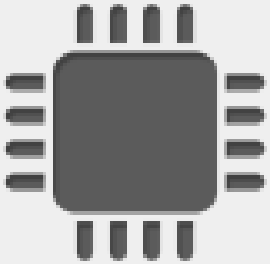
Функционал

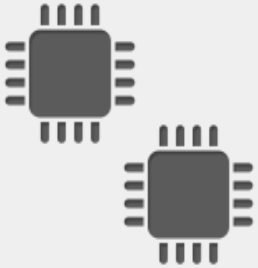
- Удержание карточки
- Считывание данных и ввода PIN
- Взаимодействие с блоками ввода вывода ATM's

Почему данные а не наличные?

- Информацию (Card numbers & PIN) можно использовать на любом банкомате.
- А значит получить больше наличных

ATM Security Контр меры

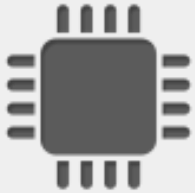


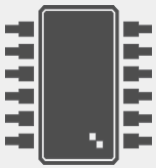


HARDENING	**Авторизованный код и безопасный запуск**	**Аутентификация устройств**	**Аутентификация пользователей**
Sandboxing, контроль поведения, принцип минимума привилегий	Уверенность в запускаемом коде	Не доверять неизвестной периферии	Магнитной линии недостаточно

Защита

Предотвращение исполнения неизвестного кода остановит вредоносную активность





HARDENING	Поведение	Память	Интеграция	Периферия
Политики управления системами	SANDBOXING & WHITELISTING приложений	Политики контроля памяти	Мониторинг в режиме реального времени	Контроль приложений
Применение принципа минимума привилегий для устройств	Ограничить исполнение программ только необходимыми функциями	Защищает от вредоносного кода внедренного или исполненного из памяти	Постоянный мониторинг установок файла и реестра	Доступ к клавиатуре для программ из белых списков Контроль USB & других портов

Многоуровневая защита без сигнатур

Для предотвращения направленных атак и угроз zero-day

СЕТЬ

FIREWALL И ЗАЩИТА ОТ ВТОРЖЕНИЙ

Определение сетевого соединения приложения запущенного на устройстве

HARDENING

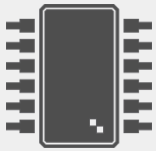
Политики управления системой

Применение минимума привилегий и блокировка внешних интерфейсов

ПОВЕДЕНИЕ

SANDBOXING & WHITELISTING приложений

Ограничить исполнение программ только необходимыми функциями



ПАМЯТЬ

Политики контроля памяти

Защищает от вредоносного кода внедренного или исполненного из памяти

ИНТЕГРАЦИЯ

Мониторинг в режиме реального времени

Постоянный мониторинг установок файла и реестра

Аутентификация пользователей нового поколения

Делает дополнительные факторы прозрачными

Сегодня: ATM, CARD, & PIN.

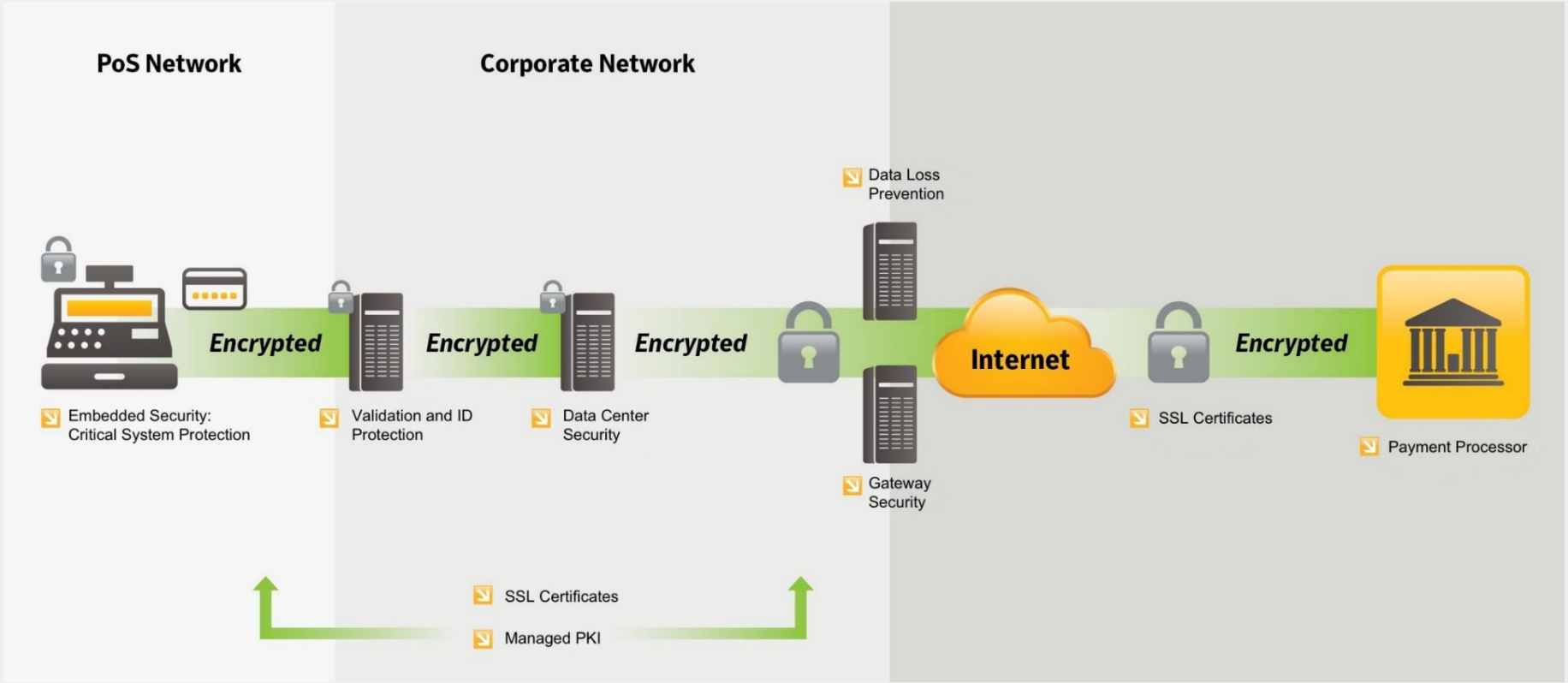
Проверка присутствия владельца карточки возле ATM (через мобильный телефон)

В случае подозрения спросить владельца карточки через мобильный телефон: “Do you authorize this?”

Для транзакций высокого риска использовать биометрию встроенную в смартфон (отпечаток пальца, распознавание лица, радужной оболочки глаза).

Пример эшелонированной защиты

Эшелонированная защита на примере решений Symantec



Спасибо!

Петр Сергеев

Peter_Sergeyev@symantec.com