АТАКА НА ПОСЛЕДНИЕ РУБЕЖИ.
КАК СПАСТИ БАНКОМАТЫ ОТ КИБЕР МОШЕННИКОВ

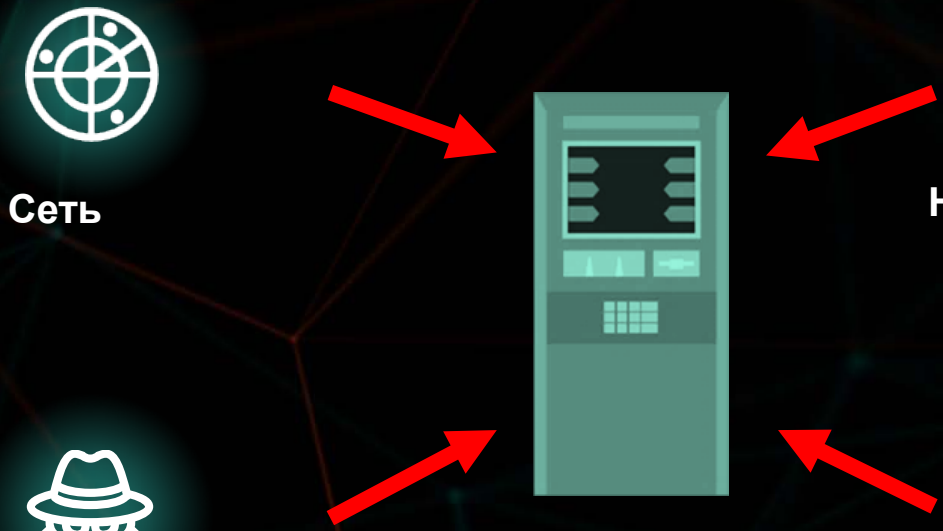
Зачем вообще нужно защищать банкоматы и так все работает?

KASPERSKY lab

Векторы атак на банкоматы

ТАК БЫЛО РАНЬШЕ

В НАШЕ ВРЕМЯ МЕТОДЫ ВЗЛОМА БОЛЕЕ ИНТЕЛЕКТУАЛЬНЫЕ



Сеть

Недоверенные устройства

Внутренние пользователи

Физические интерфейсы

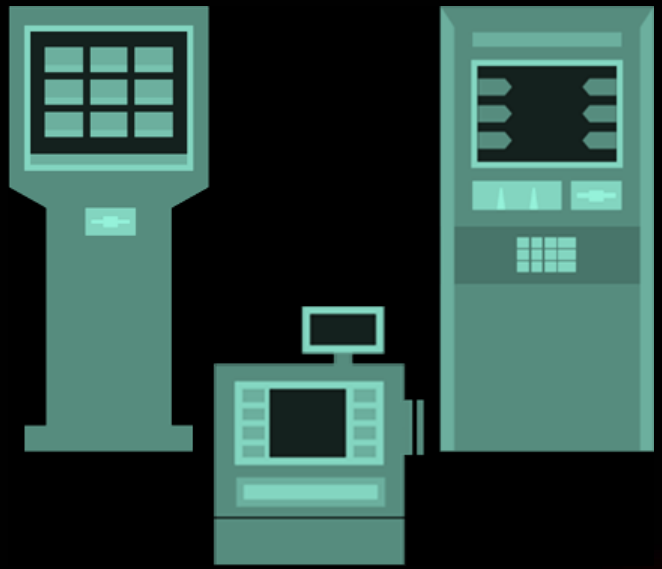
Почему так произошло?

- Windows XP без официальной поддержки
- Системный блок в зоне легкого доступа
- активные USB порты и CD-ROM
- Банкоматы подключены к доверенной сети
- Такие атаки стали очень дешёвыми. В 2017 году впервые появилась услуга ATM Malware-as-a-service

Почему традиционная защита не пригодна?

Применение

— Отсутствует классический пользователь
— Публичный доступ
— Обслуживается сторонними компаниями



Технические характеристики

— Низкая производительность
— Ограниченный канал связи

Специальное назначение

• Финансовые транзакции
• Обработка персональных данных

Программное обеспечение

— Операционная система Windows Embedded
— Фиксированный набор программ
— Редкие изменения конфигурации

Kaspersky Embedded Systems Security

СПЕЦИАЛИЗИРОВАННАЯ ЗАЩИТА БАНКОМАТОВ

Низкие требования к аппаратным ресурсам

От 256 MB RAM

Совместимость со всеми встраиваемыми системами Windows, в том числе с Windows XP
XP Embedded, POS Ready 2009

Ограниченное или полное отсутствие подключения к интернету

Работа даже на слабых каналах связи

В основном мобильные сети (3G в лучшем случае)

KASPERSKY EMBEDDED SYSTEMS SECURITY

Контроль устройств

Файловый антивирус
(опционально доступен)

Защита памяти
— Защита процессов в памяти от эксплойтов

Режим «Запрет по умолчанию»

—Низкие системные требования (256MB системной памяти)

—Низкое потребление трафика (не нужно регулярных обновлений антивируса)

—Не требуется соединение с интернетом

—Запрет исполняемых файлов, DLL, драйверов

Контроль целостности файлов
— Отслеживает действия с выбранными файлами и папками

Гибкое управление

Kaspersky Embedded Systems Security

Соответствие требованиям PCI DSS v3.2

ТРЕБОВАНИЯ PCI DSS 3.2

1.4 Установить персональный брандмауэр или аналогичное ПО на все устройства, которые имеют доступ к интернету.

5.1 Развернуть антивирусное ПО на всех системах, обычно подверженных воздействию вредоносного ПО.

5.1.1 Убедиться, что антивирусное ПО способно обнаруживать и устранять все известные типы вредоносного ПО и обеспечивать защиту от них.

5.2 Гарантировать, что все антивирусные механизмы поддерживаются в актуальном состоянии, выполняют периодическое сканирование, создают журналы регистрации событий, которые хранятся согласно требованию 10.7 стандарта PCI DSS.

5.3 Убедиться, что антивирусные механизмы постоянно запущены, и пользователи не могут их ни отключить, ни изменить без явного разрешения, которое выдается руководством на каждый конкретный случай и на ограниченный период времени.

ТРЕБОВАНИЯ PCI DSS 3.2

6.2 Все системные компоненты и программное обеспечение должны быть защищены от известных уязвимостей путем установки необходимых обновлений системы безопасности, выпущенных поставщиком. Критичные обновления безопасности должны быть установлены в течение месяца с момента их выпуска производителем.

10.5.5 Следует использовать приложения контроля целостности файлов для защиты журналов регистрации событий от несанкционированных изменений.

11.5 Следует внедрить механизм защиты от изменений (например, мониторинг целостности файлов) для оповещения персонала о несанкционированных изменениях критичных системных файлов, конфигурационных файлов и файлов данных.

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- ✓ **Kaspersky Embedded Systems Security**
- ✓ **Физическая безопасность банкоматов**
- ✓ **Обучение персонала**

ЖИВОЙ КЕЙС ЕВРАЗИЙСКОГО БАНКА

- Почему необходимо защищать банкоматы?
- С чего необходимо начать?
- Как не повлиять на бизнес процессы компании?

Eurasian Bank

Спасибо!

KASPERSKY lab