Инфозащита

Как кибермошенники воруют деньги у банков: анализ случаев из практики

О компании «Инфозащита»

Инфозащита

KASPERSKY lab

1 СПЕЦИАЛИЗАЦИЯ - **защита информации**

30+ **вендоров**

ЛИЦЕНЗИИ **ФСТЭК ФСБ**

СИСТЕМНЫЙ ПРОЕКТНЫЙ **ПОДХОД**

ISO 9001 **СЕРТИФИКАЦИЯ**

2000+ клиентов в 2014 году

>50% **ЕЖЕГОДНЫЙ РОСТ ВЫРУЧКИ**

УНИКАЛЬНЫЕ КОМПЕТЕНЦИИ

ШИРОКИЙ СПЕКТР **ИБ-услуг**

2008 **год основания**

100+ ДЕЙСТВУЮЩИХ СЕРТИФИКАТОВ В ОБЛАСТИ ИБ

Краткое содержание

Инфозащита

KASPERSKY lab

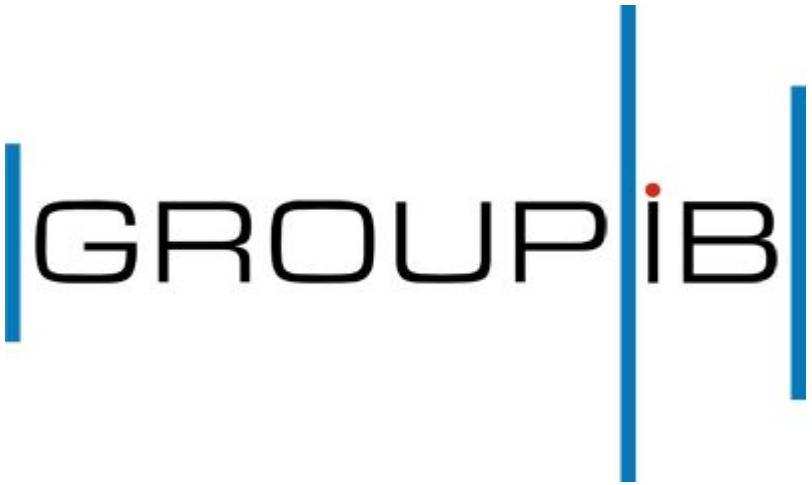
- 2 случая из практики
- Алгоритмы атак
- Варианты предотвращения

Наши партнеры

Инфозащита

KASPERSKY lab

При подготовке данной презентации мы сотрудничали с нашими партнерами



Инфозащита

KASPERSKY lab

Что случилось

Сеть партнера платежной системы была скомпрометирована, 2013 г.

Инфозащита

KASPERSKY lab

Последствия

В результате манипуляций с балансами клиентов платежной системы было украдено более 75 миллионов рублей

Алгоритм атаки

Инфозащита

KASPERSKY lab

Взлом веб-сервера и размещение бэкдора

Запуск бэкдора на компьютере пользователя

VPN соединение с сетью платежной системы

#1

Алгоритм атаки

Инфозащита

KASPERSKY lab

Компрометация пароля root

SSHd-бэкдор, сбор данных

Бэкдор на ПК администратора

#2

Алгоритм атаки

Инфозащита

KASPERSKY lab

Доступ к СУБД и ее анализ

Разработка процедур работы с БД

Манипуляции со счетами клиентов

#3

Инфозащита

KASPERSKY lab

Что случилось

На компьютер рядового пользователя банка попала вредоносная программа

Инфозащита

KASPERSKY lab

Последствия

Со счетов банка было похищено более 100 миллионов рублей

Алгоритм атаки

Инфозащита

KASPERSKY lab

СПАМ-вирус с легального сайта

Обмены данным между хакерами

Дополнительное вредоносное ПО

#1

Алгоритм атаки

Инфозащита

KASPERSKY lab

Доступ в ЛВС банка и взлом серверов

Взлом ПК операторов АБС

Похищение денежных средств

#2

Какие выводы?

Инфозащита

KASPERSKY lab

- Атаки сложные и многоходовые
- Атака может начаться различных точках
- Различные хакеры тесно взаимодействуют
- Банальное заражение может превратиться в направленную атаку

Как можно было защититься?

Инфозащита

KASPERSKY lab

- Контроль целостности и антивирусная защита для Linux
  - ✓ Антивирус Касперского для Linux File Servers
- Анализ трафика в реальном времени
  - ✓ Bot-Trek Threat Detection Service (TDS)
  - ✓ Bot-Trek Cyber Intelligence

Инфозащита

KASPERSKY lab

#1

От атак на 100% никто не застрахован

Инфозащита

KASPERSKY lab

#2

Нужно применять комбинацию разноплановых средств защиты

Инфозащита

KASPERSKY lab

#3

Должна быть продуманная и четкая стратегия защиты

О компании «Инфозащита»

Инфозащита

KASPERSKY lab

1 СПЕЦИАЛИЗАЦИЯ - **защита информации**

30+ **вендоров**

ЛИЦЕНЗИИ **ФСТЭК ФСБ**

СИСТЕМНЫЙ ПРОЕКТНЫЙ **ПОДХОД**

ISO 9001 **СЕРТИФИКАЦИЯ**

2000+ клиентов в 2014 году

>50% **ЕЖЕГОДНЫЙ РОСТ ВЫРУЧКИ**

УНИКАЛЬНЫЕ КОМПЕТЕНЦИИ

ШИРОКИЙ СПЕКТР **ИБ-услуг**

2008 **год основания**

100+ ДЕЙСТВУЮЩИХ СЕРТИФИКАТОВ В ОБЛАСТИ ИБ