Digital Security

Как украсть миллиард: Вывод денег через уязвимости АБС

Илья Медведовский

к. т. н.

Генеральный директор Digital Security

Различные схемы краж денежных средств

Первое правило бойцовского клуба?

Заведомо вынося за скобки ДБО

О выводе денег из банков через уязвимости говорится с 2009 г.

Внутри банка или межбанковским переводом

Внутри банка

- Вывод наличных через собственный банкомат
- Вывод наличных через банкоматы платежной системы

Вывод наличных через банкоматы

- Ограничение: объем денег в собственных банкоматах

- Ограничение: объем денег в банкоматах платежной системы

Вывод наличных через банкоматы

Реализация #1

Создание “бесконечной” карты

Псевдо-
зачисление
на карту суммы

Снятие дневных
лимитов в АБС

Снятие наличных
или оплата
товаров

(схема пока не использовалась злоумышленниками)

Вывод наличных через банкоматы

Реализация #2

Создание бесконечной карты путем “возврата” средств

Зачисление денег на карту (относительно небольшой суммы на уровне лимита)

Снятие наличных

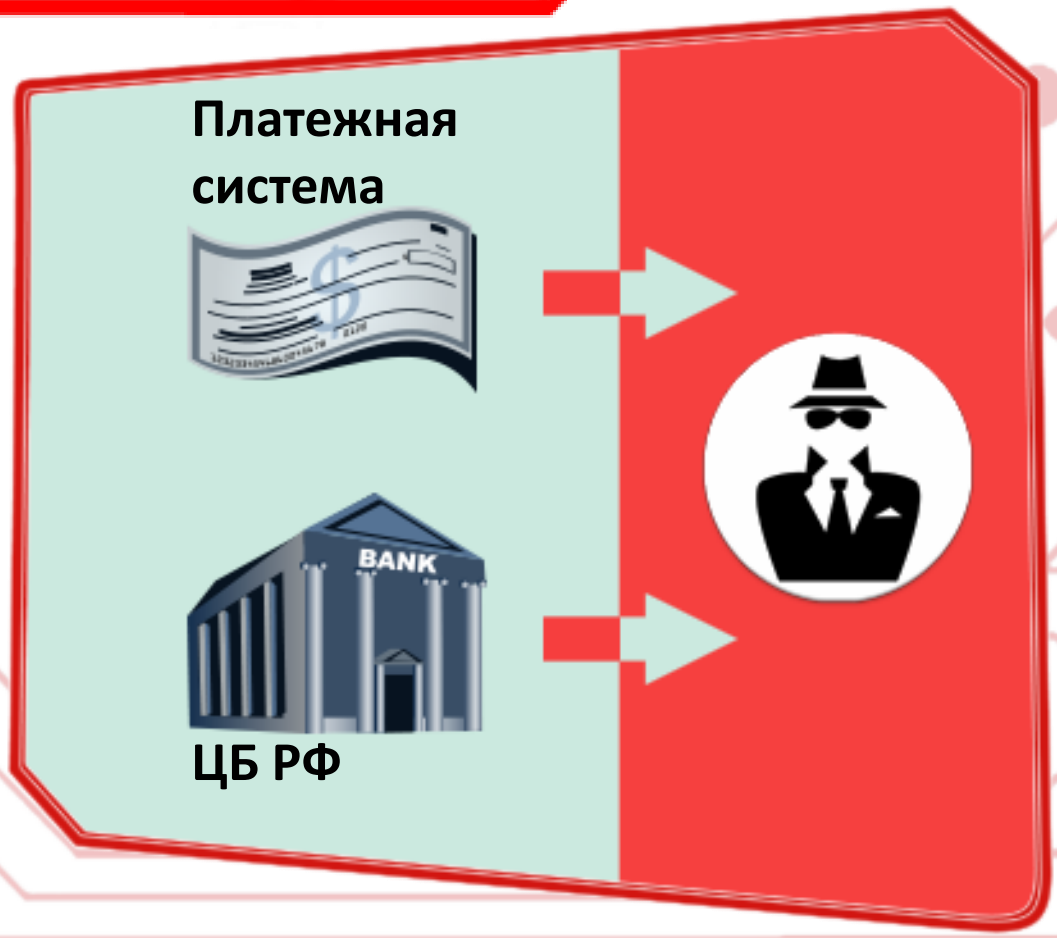
Снятие наличных до опустошения банкомата

Операция возврата снятых денежных средств

(схема применяется злоумышленниками)

Вывод безналичным межбанковским переводом

- Через платежную систему
- Через ЦБ РФ



Вывод безналичным межбанковским переводом

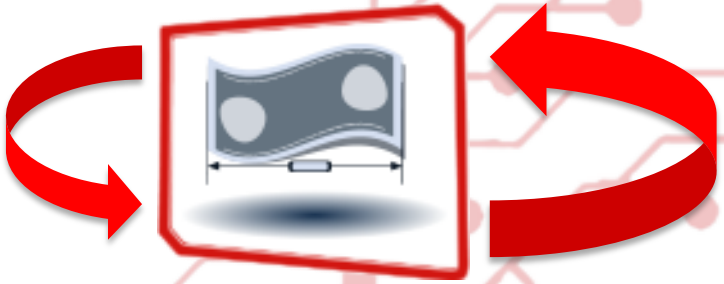
- Ограничение (платежная система): лимит банка в данной платежной системе
- Ограничение (ЦБ РФ): размер денег на корр. счете банка

Вывод безналичным переводом

Реализация

Через платежную систему.

Регулярные переводы на уровне лимита разового платежа и опустошение денежного лимита банка в этой платежной системе



(схема применяется злоумышленниками)

Вывод безналичным переводом

Реализация

В другой банк. Атака на АРМ КБР

Генерация новой или подмена получателей платежа в одной из существующих рейсовых платежек банка в ЦБ РФ

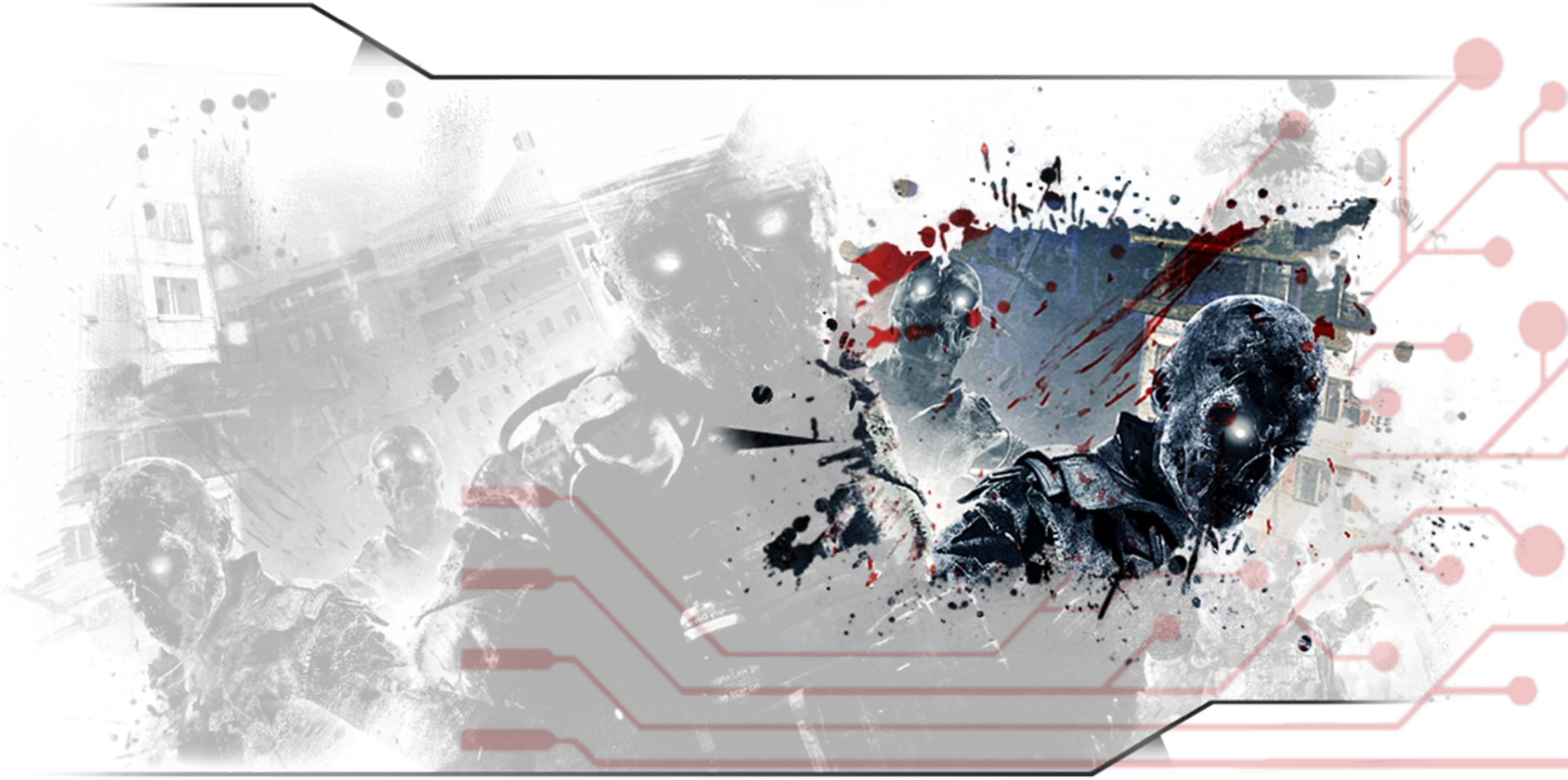
Отправка "рейса" в АРМ КБР

Опустошение корр счета банка

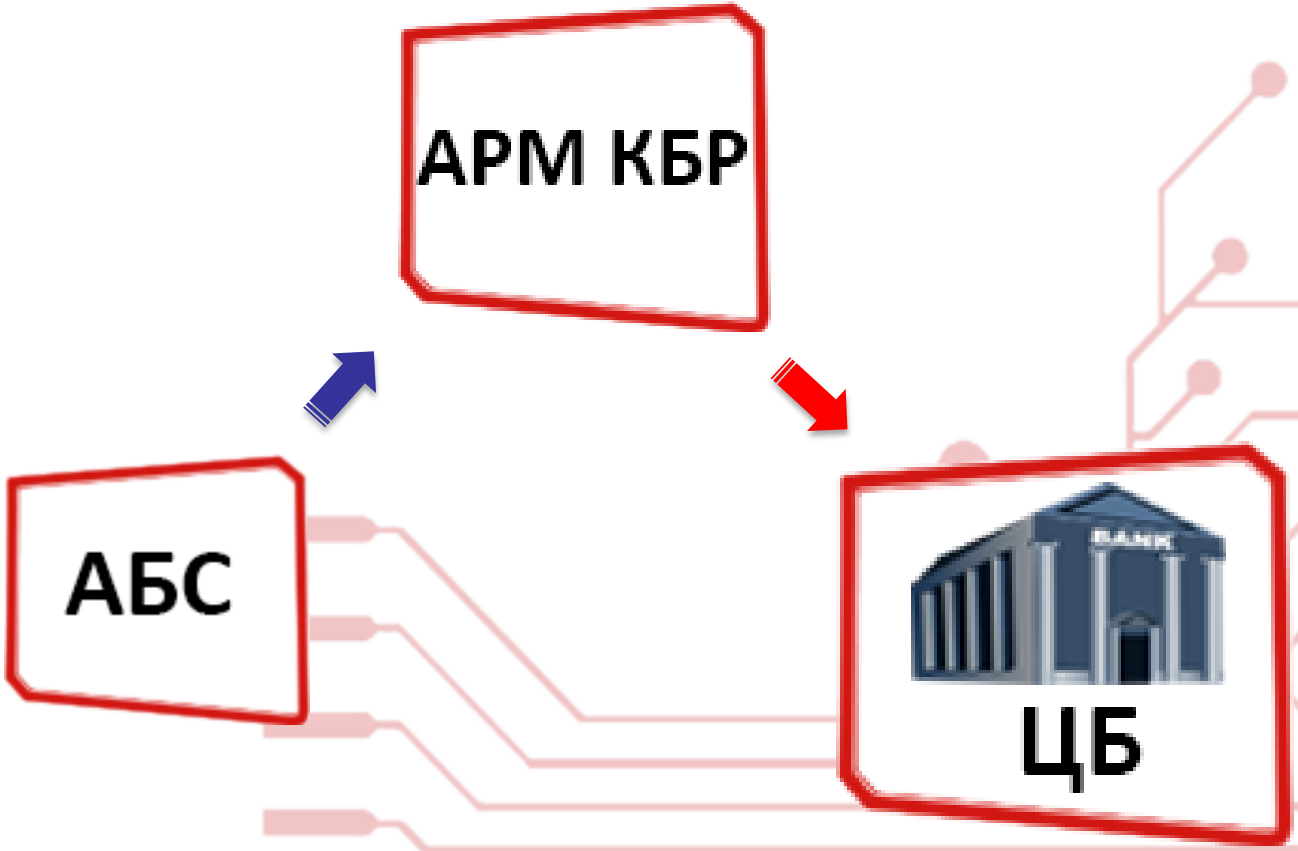
(схема применяется злоумышленниками)

Как будут воровать завтра?

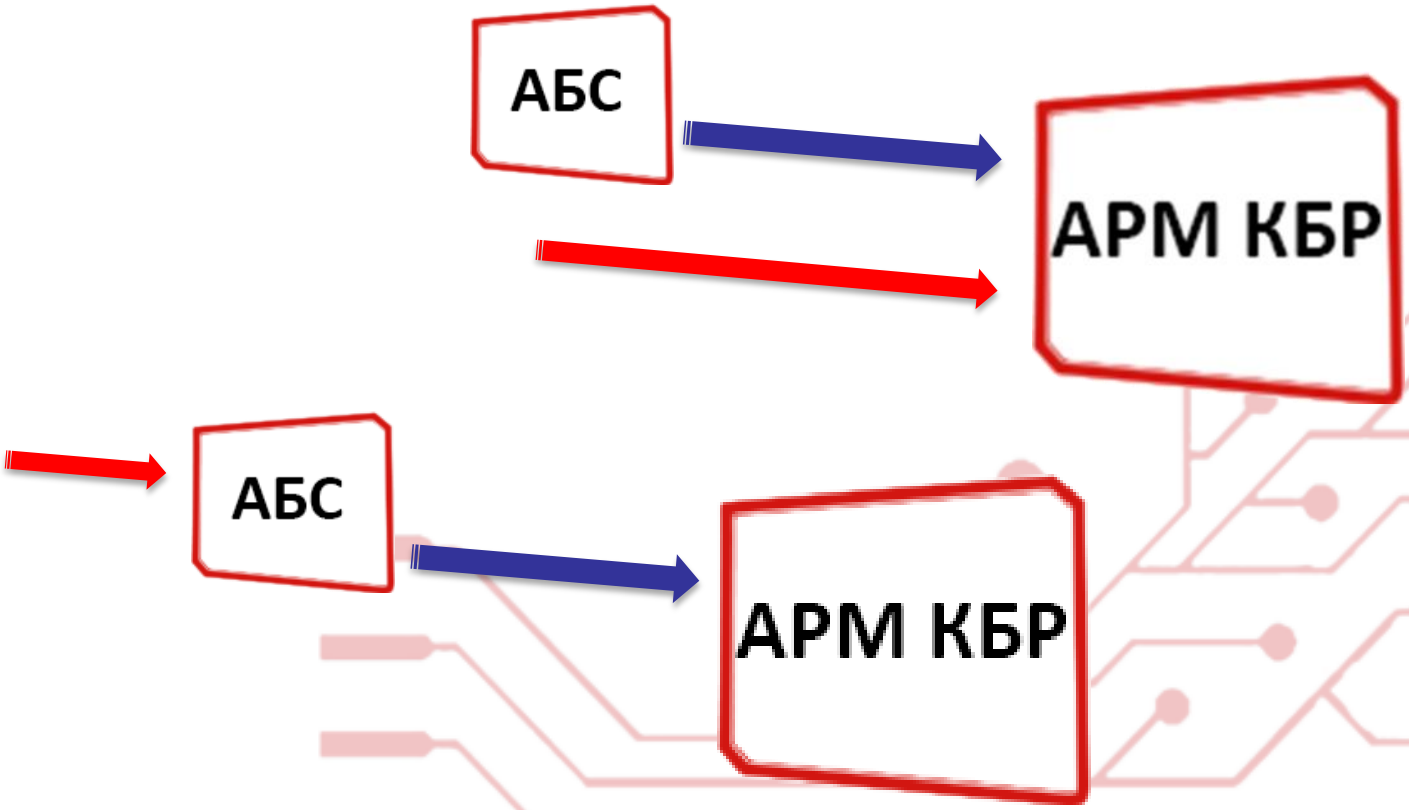
Атаки на платежные системы



Атаки на ЦБ РФ



Атаки на АБС



Спасибо за внимание!

Вопросы?

Digital Security в Москве: (495) 223-07-86
Digital Security в Санкт-Петербурге: (812) 703-15-47

www.dsec.ru
info@dsec.ru