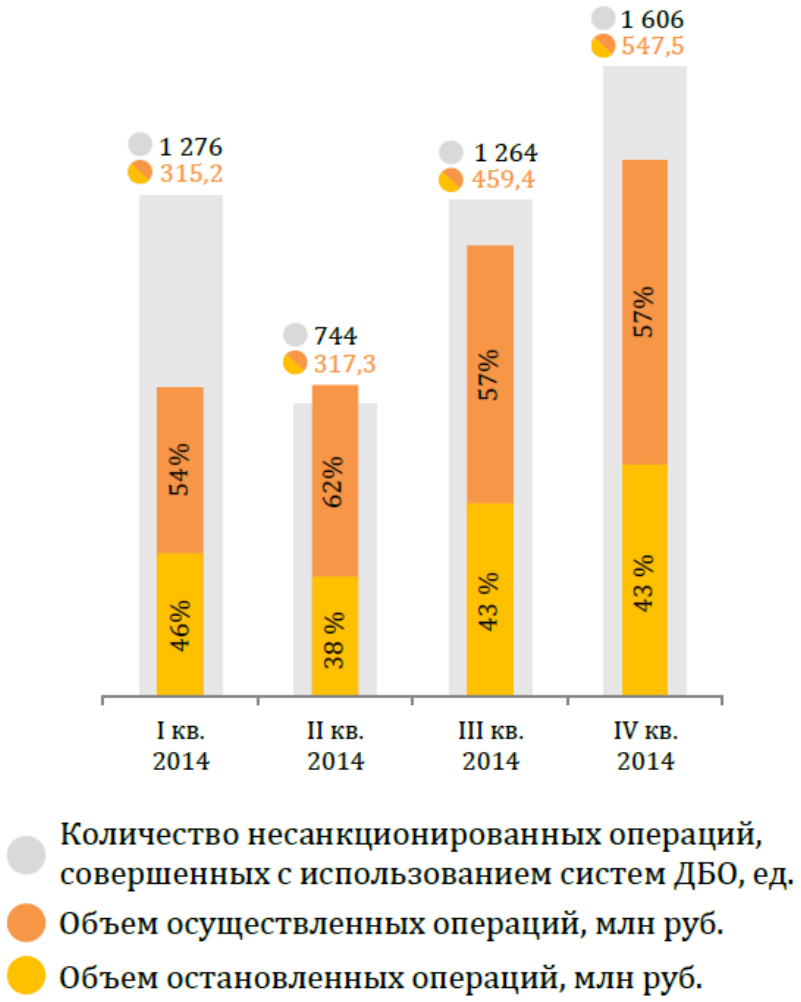
Как атакуют финансовые организации?

Алябьев Андрей,
Банк “ХОВАНСКИЙ”
(в настоящее время – независимый эксперт)

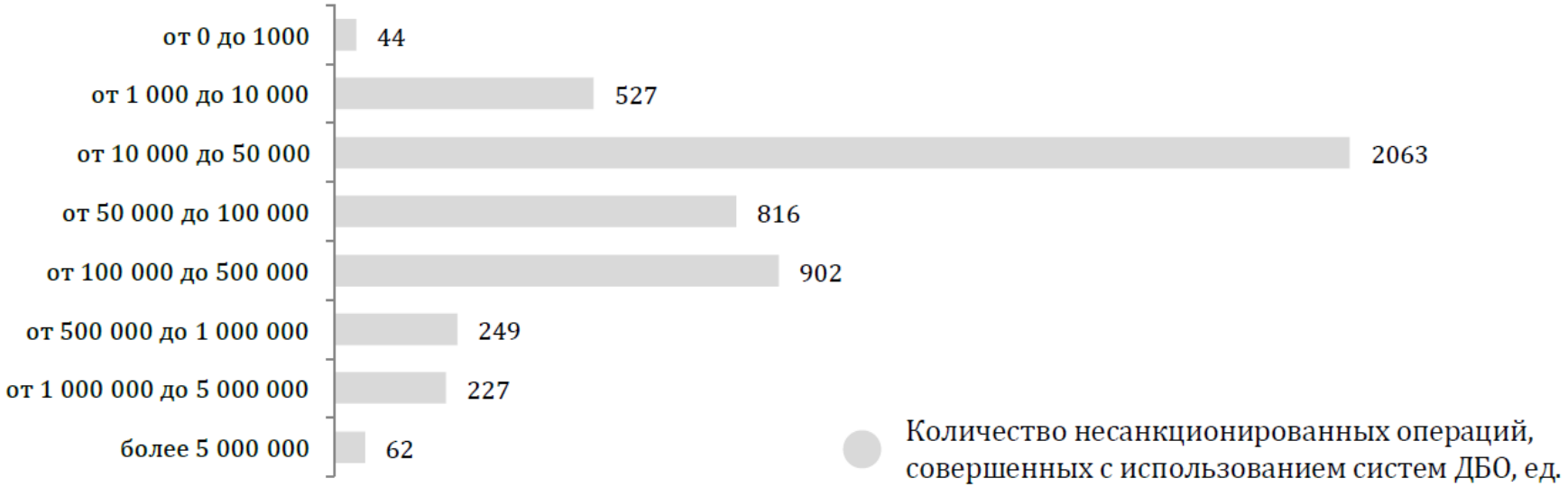
Что происходит ?

За 2014 год в ЦБ было сообщено о 4,89 тыс. случаев попыток хищений через ДБО на общую сумму 1,64 млрд руб. Из них 825 операций на сумму около 900 млн руб. были остановлены Более 80% (на сумму более 700 млн руб.) прошли успешно

Динамика количества и объема несанкционированных операций, совершенных с использованием систем ДБО



Распределение количества несанкционированных операций, совершенных с использованием систем ДБО, по объему несанкционированных операций



Более 80 % от всех несанкционированных операций - списание со счетов физ. лиц. Но наибольший ущерб приносят хищения денежных средств со счетов юр. лиц (не менее 73%).

Сегмент рынка в России и СНГ	Число преступных групп	Общее число успешных атак в день	Средняя сумма одного хищения (в рублях)	Сумма хищений в день (в рублях)	Q2 2014- Q1 2015 (в рублях)	Q2 2014- Q1 2015 (средний курс 57 рублей за $1)
Хищения в интернет-банкинге у юридических лиц	8	16	480 000	7 680 000	1 912 320 000	$33 549 474
Хищения в интернет-банкинге у физических лиц	2	2	76 500	153 000	38 097 000	$668 368
Хищения у физических лиц с Android-троянами	14	70	3 500	245 000	61 005 000	$1 070 263
Целевые атаки на банки	3	-	90 000 000	-	638 000 000	$11 192 982
Обналичивание похищаемых средств	-	-	-	3 635 100	1 192 239 900	$20 916 489
Оборот «кард»-шопов	7	-	-	-	155 314 854	$2 724 822
Итого				**11 713 100**	**3 996 976 754**	**$70 122 399**

Разделение хищений в интернет-банкинге 2 649 422 000 рублей:

Тенденции

- Общий объем хищений несколько сократился, но количество атак выросло
- Целевые атаки на банки все еще популярны
- Новые типы атак для банкоматов
- Увеличение количества инцидентов с криптолокерами
- Атакующие клиентов-физиков переключились с ПК на android
- Обход двухфакторной аутенификации: подмена сим-карт

Атаки на банковскую инфраструктуру

Цели злоумышленников

- Перевод денежных средств
  - АБС
  - ДБО
  - АРМ КБР
  - SWIFT
  - Банкоматы
- Иные деструктивные воздействия
  - Кража информации
  - Шифрование файлов / вымогательство
  - DDOS
  - Прочие

Как атакующий попадает в сеть

- Зараженные сайты
- Съемные носители
- Эксплуатация уязвимостей
- Письма с вредоносными вложениями

- Могут быть сообщники в банке
- Взломавшие могут предоставлять другим злоумышленникам доступ к зараженным узлам

Социальная инженерия

- Письма от регуляторов
- Договорные отношения
- Письма от коллег
- ФССП, банки, коллекторы
- Письма от известных компаний
- Халява
- Фотографии, знаменитости

Примеры из практики

От: ОАО «Газпром нефть» <info@gaz-prom-neft.ru>

К: *****@khovansky.ru

Время создания: Sun, 20 Sep 2015 10:05:05 +0300

Тема: Возврат ошибочно перечисленных денежных средств

Прикрепленные файлы: Письмо на возврат денег и реквизиты Документ Microsoft Office Word 97 - 2003 (.doc).rar

Здравствуйте!

ОАО «Газпром нефть» просит Вас вернуть ошибочно перечисленные на ваш счет денежные средства вернуть нам на следующие реквизиты во вложении.

С уважением, начальник финансового управления Сидоркина Анна

Телефоны +7(812)363-3152

8-800-700-3152 бесплатный звонок по России

Факс +7(812)363-3151

Эл. почта info@gaz-prom-neft.ru

ОАО «Газпром нефть»

virustotal

SHA256:	c6fc639ac583a7bbb1cbfe4d6f05951234908b837119fab1ca90e299e0a001e7
Имя файла:	Письмо на возврат денег и реквизиты Документ Microsoft Office Wor...
Показатель выявления:	16 / 54
Дата анализа:	2015-09-21 09:03:09 UTC (5 часов, 34 минут назад) Показать последний анализ

From: appelsinka88@mail.ru [mailto:appelsinka88@mail.ru]
Sent: Thursday, September 11, 2014 12:06 PM
To: ******@khovansky.ru
Subject:
Importance: High
Sensitivity: Confidential

Здравствуйте
Во вложении - Ваша типовая форма контракта с правками наших юристов. Если наши исправления в части сроков не критичны, хотелось бы организовать встречу и подписание. Жду Вашего ответа.

Вложения: 1
1. Договор_типовый_01092014.zip

virustotal

SHA256:	f4df70fede157839bfd5f4cf8f1080ca710d9756bb6db2d4b958acea6252334e
Имя файла:	Договор_типовый_01092014.zip
Показатель выявления:	6 / 54
Дата анализа:	2014-09-12 06:36:11 UTC (1 год назад) Показать последний анализ

спустя год...

virustotal

SHA256:	f4df70fede157839bfd5f4cf8f1080ca710d9756bb6db2d4b958acea6252334e
Имя файла:	Договор_типовый_01092014.zip
Показатель выявления:	21 / 55
Дата анализа:	2015-09-22 14:13:35 UTC (1 минута назад)

From: Служба Поддержки [mailto:support@cbr.ru.com]
Sent: Thursday, October 22, 2015 10:22 AM
To: alyabiev@khovansky.ru
Subject: Информационная рассылка

Для повышения уровня общественной безопасности служащих Центральный Банк Российской Федерации настоящим письмом сообщает о небольших изменениях способа оценки уровня знаний служащих банков, которая планируется к внедрению в ближайшем времени.
Письмо обязательно советуется к прочтению всем работникам финансово-кредитных учреждений РФ.

Вложения: 1
1. Документ.zip

virustotal

SHA256:	33cef424a9a0fe25b089a0b71481b81e3a3dc000b03ef7385f885213e6e75353
Имя файла:	Документ.zip
Показатель выявления:	4 / 56
Дата анализа:	2015-10-22 07:44:04 UTC (1 неделя, 4 дней назад) Показать последний анализ

+ подобные вещи обсуждаются здесь

http://bankir.ru/dom/threads/123182-Фишинговые-письма

Антивирусы не справляются

Кто в группе риска

- Секретарь / помощник руководителя
- Бухгалтерия
- Менеджеры по работе с клиентами
- ОПЕРУ
- и ИТ тоже...

Что делать

- Учить(ся), учить и еще раз учить
- Неотвратимость наказания для сотрудников
- Рубить доступ в интернет, резать категории доступных сайтов
- Требования к паролям
- Менеджмент инцидентов

Что делать: технические меры

- Сканирование всего трафика в реальном времени
- Сегментирование сети
- Резервное копирование
- Обновлять ПО, закрывать уязвимости
- Контроль съемных носителей
- Контроль доступа к личной (внешней) почте
- Контроль облачных хранилищ
- Комбинация разных средств защиты

Спасибо за внимание

Мои контакты:

Алябьев Андрей

http://facebook.com/andrey.alyabiev

http://ru.linkedin.com/in/andreyalyabiev

Готов ответить на вопросы