Практика обеспечения безопасности систем ДБО в кредитных организациях.

Павел Крылов

Зам. начальника
Отдела по контролю за банковскими рисками
ОАО «Сведбанк»

Как-то в ноябре 2009

Swedbank

- На следующий день после инцидента копия жесткого диска клиента и адрес C&C.
- Из-за **ошибки** злоумышленника банк смог получить резервные копии базы данных с сервера bot-сети.
- В результате **только за ноябрь 2009** в базе злоумышленника оказались:
  - данные с 239 клиентов из 67 банков;
  - данные клиентов не банковских организаций (в том числе телекоммуникационных)
  - данные для различных производителей интернет-банков.

Итоги по данному случаю

Swedbank

- Только 12 банков запросили у нас информацию.
- Сайт злоумышленника действовал еще минимум месяц.
- Данный злоумышленник не профан.
- Только один банк поделился информацией об IP-адресах, с которых были произведены несанкционированные платежи.
- На 15.02.10 в Управлении К была информация о владельце сим-карты, с которой осуществлялся доступ через Yota. Дальнейшая судьба не известна.
- Остальные задействованные операторы не смогли предоставить информацию по использованию Интернет своими пользователями.

Общие тенденции

- Попытки каждый месяц, сезонность
- Уровень внимания клиента к проблеме низкий
- **Злоумышленники чувствует себя вполне безопасно**

Стратегия

Как можно больше предотвращать, «отфильтровывать»,

чтобы снизить количество инцидентов и

минимизировать количество судебных дел.

В первую очередь…

Навести порядок в ДБО со стороны банка:

- Юридические вопросы
  - Наличие действующих лицензий ФСБ
  - Аттестация системы ДБО
  - Вопросы смены ключей у клиента и Банка
- Провести процедуру разбора конфликтных ситуаций
  - Наличие эталонного ПО для проверки ЭЦП
  - Лицензии на ПО проверки целостности
  - Внутренние процедуры по созданию ключей
- Пентестинг

Шерлок Х.: Зачем? (кроме очевидного)

Swedbank

- Производитель не имеет опыта расследования инцидентов ДБО
- Банки не могут дорабатывать систему ДБО самостоятельно
- У мошенников есть знания и деньги!!!

Банк должен расследовать инциденты, чтобы заполнить «вакуум» опыта у разработчика.

Шерлок Х.: Инструментарий

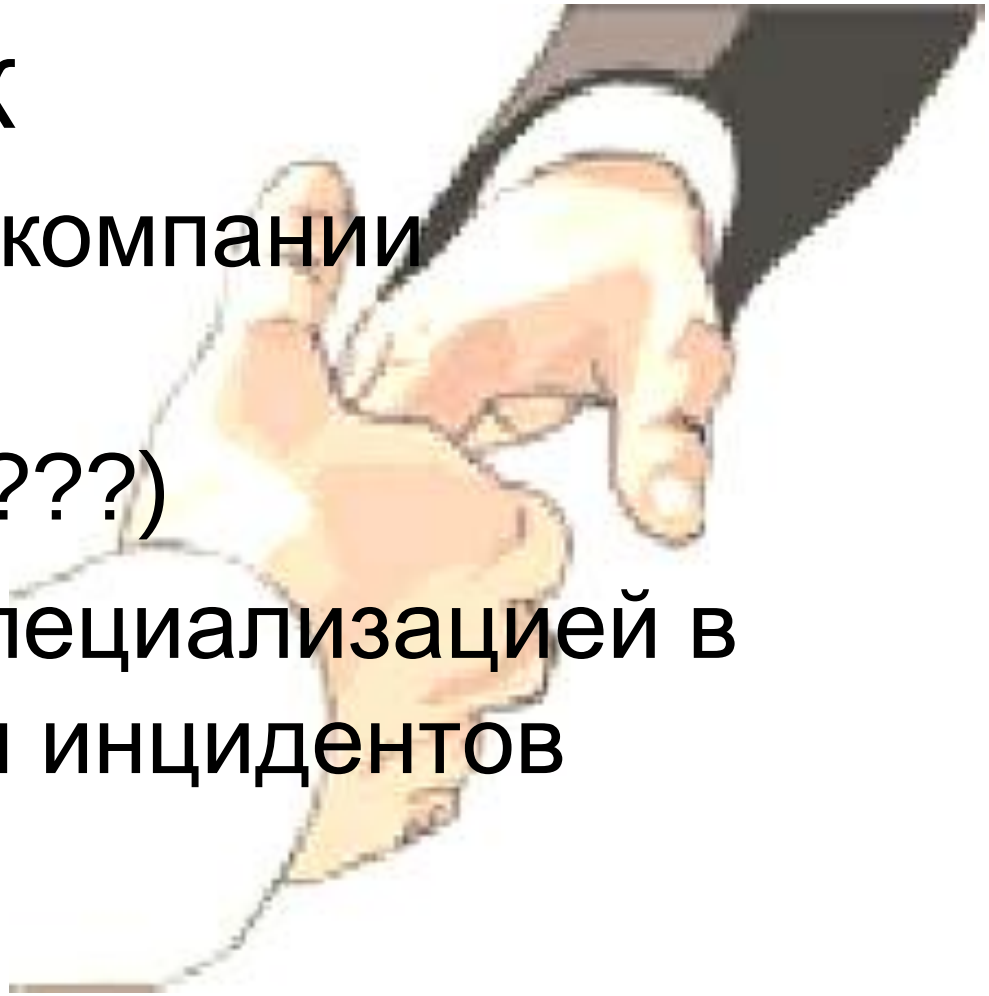
Swedbank

- EnCase Forensic v6
  - Терминальный доступ к «криминалистическим» ПК в Филиалах
- FastBloc 3
- RIP Linux
- Выделенная машина с VMWare Workstation и открытым доступом в Интернет

Шерлок Х.: Взаимодействие

Swedbank

- Управлением К
- Антивирусные компании (virustotal.com)
- Другие банки (???)
- Компании со специализацией в расследовании инцидентов



«Фильтр»: Обучение Клиента

«Краеугольный камень» в обеспечении информационной безопасности ДБО!

- вносить риски в договора
- периодические рассылки
- предлагать технические меры

«Фильтр»: система мониторинга

Swedbank

- **С момента задумки до реализации основного функционала прошел месяц.**
- Риск = IP-адрес * User-Agent * Cookies * Account number
- Будущие доработки:
  - повышение уровня риска при доступе клиента из общедоступных сетей (Yota, Корбина и т.п.)
  - учет ранее сделанных заходов с неизвестных адресов при оценке риска платежа (поведенческий анализ)
  - смена страны (заметное изменение адреса), из которых заходит «клиент», при сохранении cookie
  - СМС-информирование клиента о подозрительном платеже
  - более тесная интеграция с АБС

«Фильтр»: система мониторинга

Swedbank

From: naemon@[redacted]
To:
Cc:
Subject: fraud monitoring

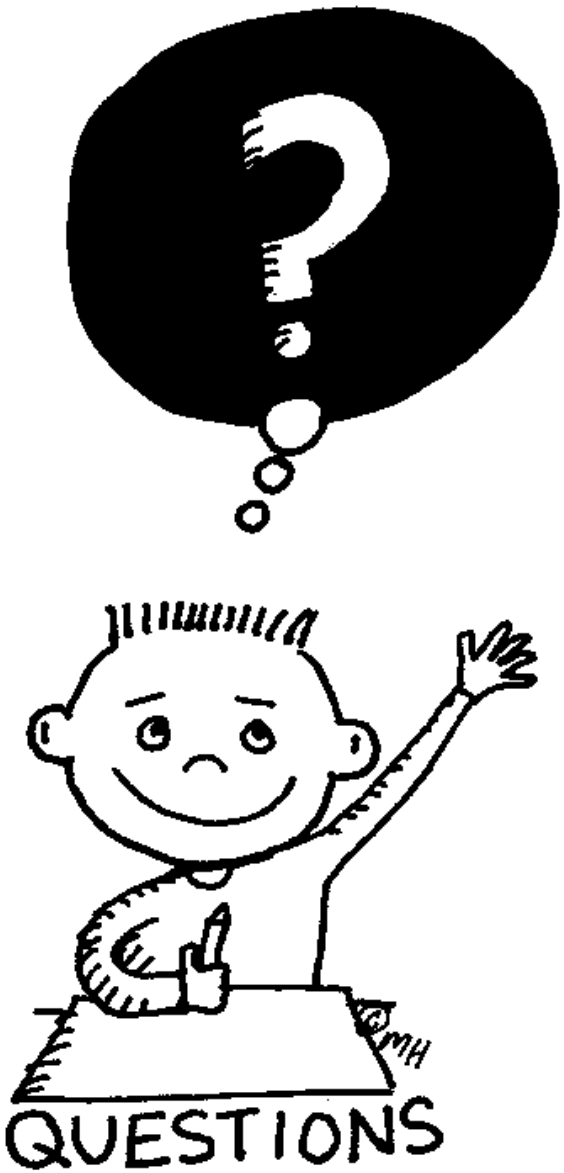
Уровень опасности	4064
Сумма	300000.00
Клиент	[redacted]
Время регистрации	2011-01-18 15:01:54
Причина	Перевод на счет физ.лица другого банка **(I)** с неизвестным ранее счетом получателя **(II)** с IP-адреса, который отличается на 32 бит **(III)** с использованием другого браузера (различаются cookie) **(IV)** с другого компьютера (различаются значения user-agent)

Детали списания средств

AMOUNT	300000.00
CURRCODE	810
CUSTID	[redacted]
DOCUMENTDATE	18.01.2011
DOCUMENTNUMBER	175
FILTERIDENT	NEW
FTMP	0
GROUND	[redacted]Командировочные расходыБез налога (НДС)
IDR	[redacted]|734155|540090814
KBOPID	1

«Фильтр»: проблемы взаимодействия

- Связываетесь ли Вы с банком-получателем, чтобы сообщить о счете «дропа»?
- Спрашиваете ли Вы у клиента, какие еще системы ДБО стоят на взломанном компьютере?


QUESTIONS