Обзор и схемы атак за 2017 год

БАНК РОССИИ
ФИНЦЕРТ

Основные схемы атак в 2017 году

В течение года ФинЦЕРТ фиксировал атаки всех известных видов на финансовые организации и их клиентов. Чаще всего следующие:

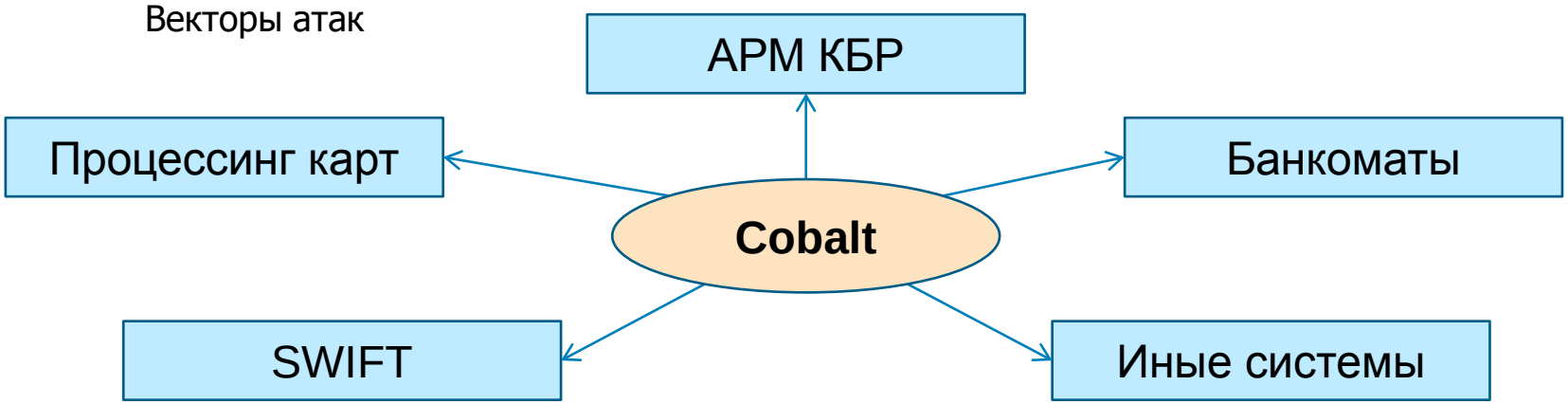
1. Целевые атаки на финансовые организации с использованием программного обеспечения **Cobalt Strike**
2. Атаки на клиентов финансовых организаций вредоносными программами для **подмены** платежных поручений
3. Хищения денежных средств из **банкоматов** с физическим подключением
4. Атаки **шифровальщиков**

1. Cobalt Strike – наибольшая угроза

Cobalt Strike – не вредоносная программа, а инструмент для тестирования. Но этот инструмент оказался идеален для целевых атак.

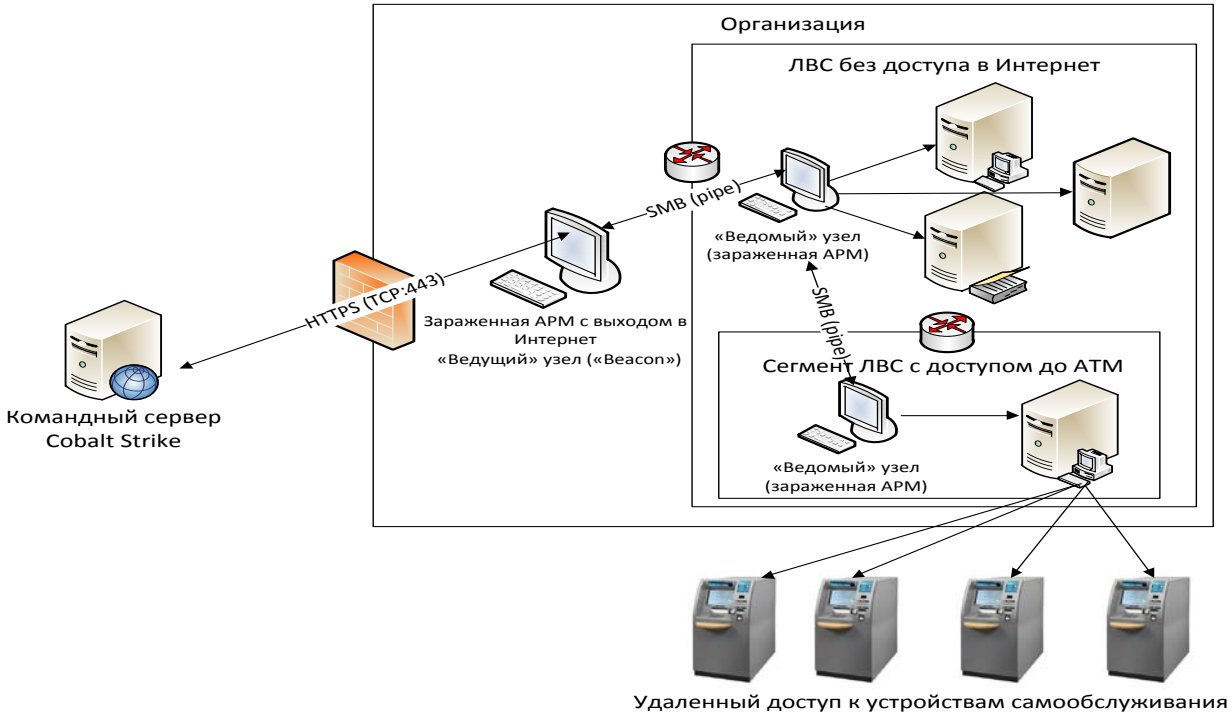
За 2017 год действиями преступной группы, использующей Cobalt Strike, финансовым организациям России причинен ущерб на сумму более

1 миллиарда 100 миллионов рублей



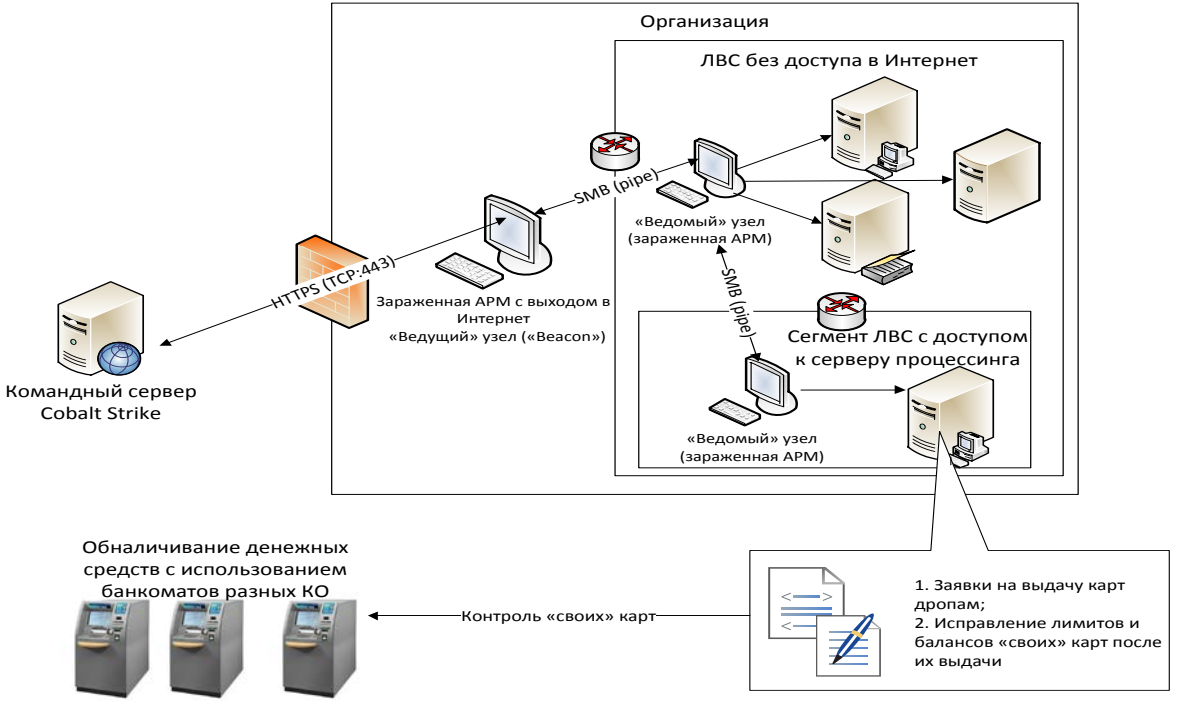
Целевая атака Cobalt Strike – банкоматы

Типовая атака с использованием ПО Cobalt Strike направлена на банкоматы кредитных организаций. После проникновения в информационные системы отыскиваются компьютеры или сервера, имеющие доступ к банкоматам. На банкоматы устанавливаются вредоносные программы. Хищение осуществляется путем направления в заранее согласованные моменты команд на выдачу денежных средств.



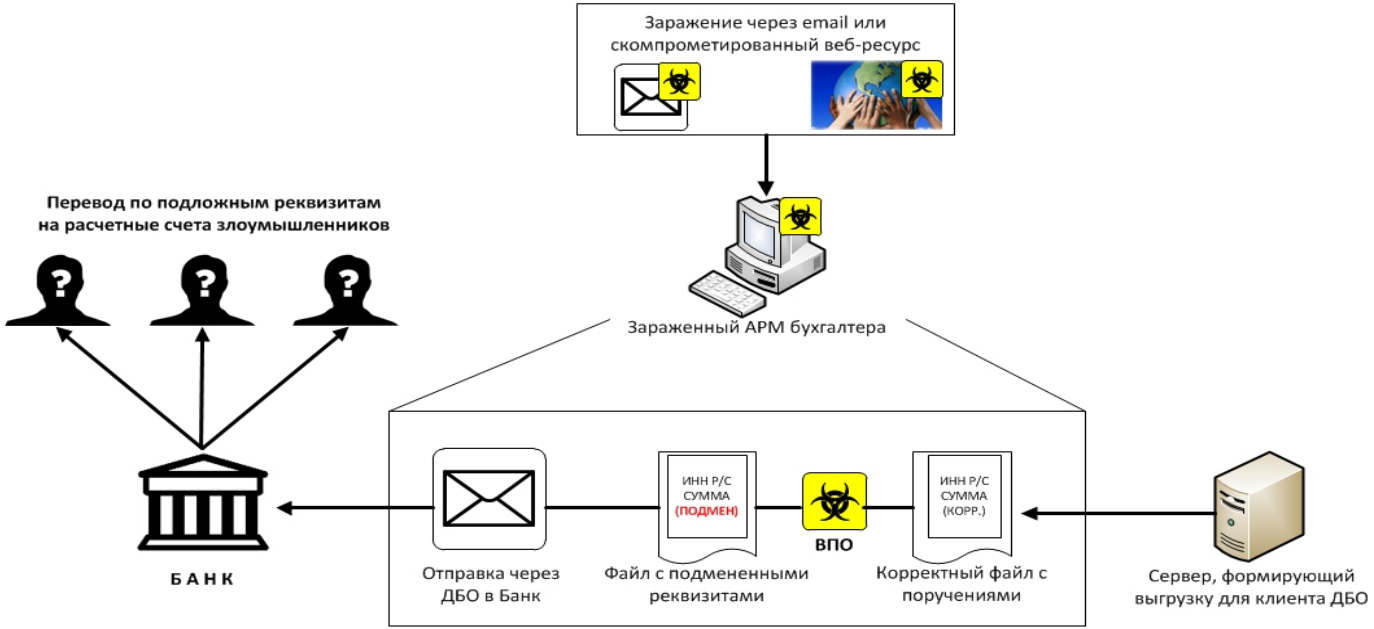
Целевая атака Cobalt Strike – процессинг карт

Другая распространённая схема атаки с использованием ПО Cobalt Strike направлена на процессинг платежных карт кредитных организаций. После проникновения в информационные системы отыскиваются компьютеры, с которых ведется управление процессингом карт, либо непосредственно сервера процессинга. Затем скупаются платежные карты организации. В заранее согласованные моменты балансы и лимиты этих карт резко поднимаются.



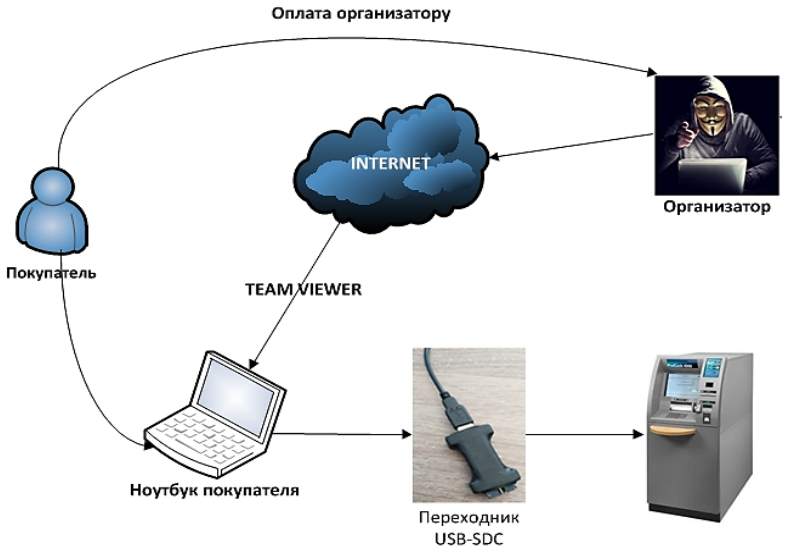
2. Атаки на клиентов банков - подмена поручений

Атака направлена на файлы экспорта-импорта бухгалтерских программ, используемые для передачи платежных поручений в системы ДБО. Вредоносные программы подменяют часть реквизитов получателей платежей, оставляя неизменными суммы. В результате, отчасти из-за невнимательности плательщиков, в банки уходят поручения о платежах на заранее подготовленные злоумышленниками счета. В 2017 году чаще всего использовались вредоносные программы Fibbit и TwoBee. В настоящее время ФинЦЕРТ исследует новый вид таких программ.



3. Атаки на банкоматы с физическим подключением

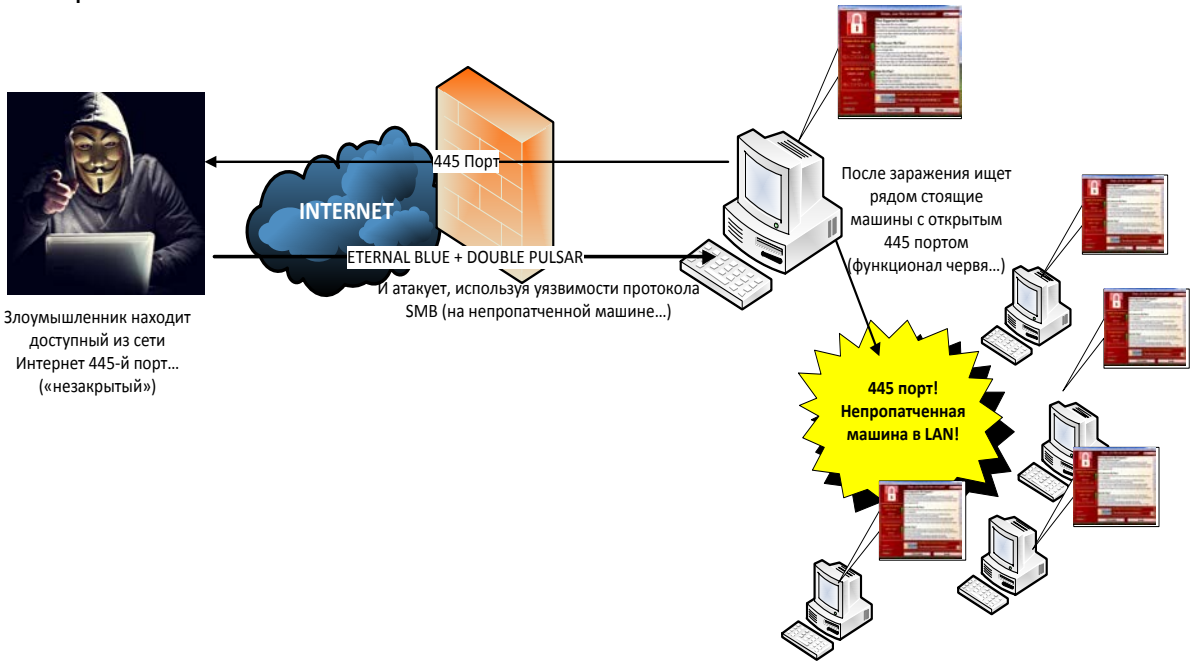
Атаки как «сервис». Организаторы продают в «Даркнете» технические средства и находят исполнителей. Последние отыскивают банкоматы нужных моделей, вскрывают корпуса, подключают к внутренним устройствам портативные компьютеры с использованием предоставленных организатором технических средств. Организатор осуществляет удаленное управление агрегатами банкомата и направляет команды на выдачу денежных средств. С каждого хищения организатор получает либо фиксированную сумму, либо процент от суммы, выданной банкоматом. На банкомате и использованном ноутбуке остается очень мало криминалистики-значимых следов.



4. Атаки шифровальщиков

Наиболее резонансная атака шифровальщика в 2017 году – WannaCry. Для саморапространения использовалась уязвимость CVE-2017-0147 в протоколе Microsoft SMB. Наибольший урон был нанесен компьютерам, на которые не были установлены последние на момент атаки обновления.

Среди российских кредитных организаций пострадавших практически не было - заражено незначительное количество устройств самообслуживания, без финансового ущерба. От похожей атаки – NotPetya – пострадала 1 кредитная организация.



Что изменилось по сравнению с 2015-2016 годами?

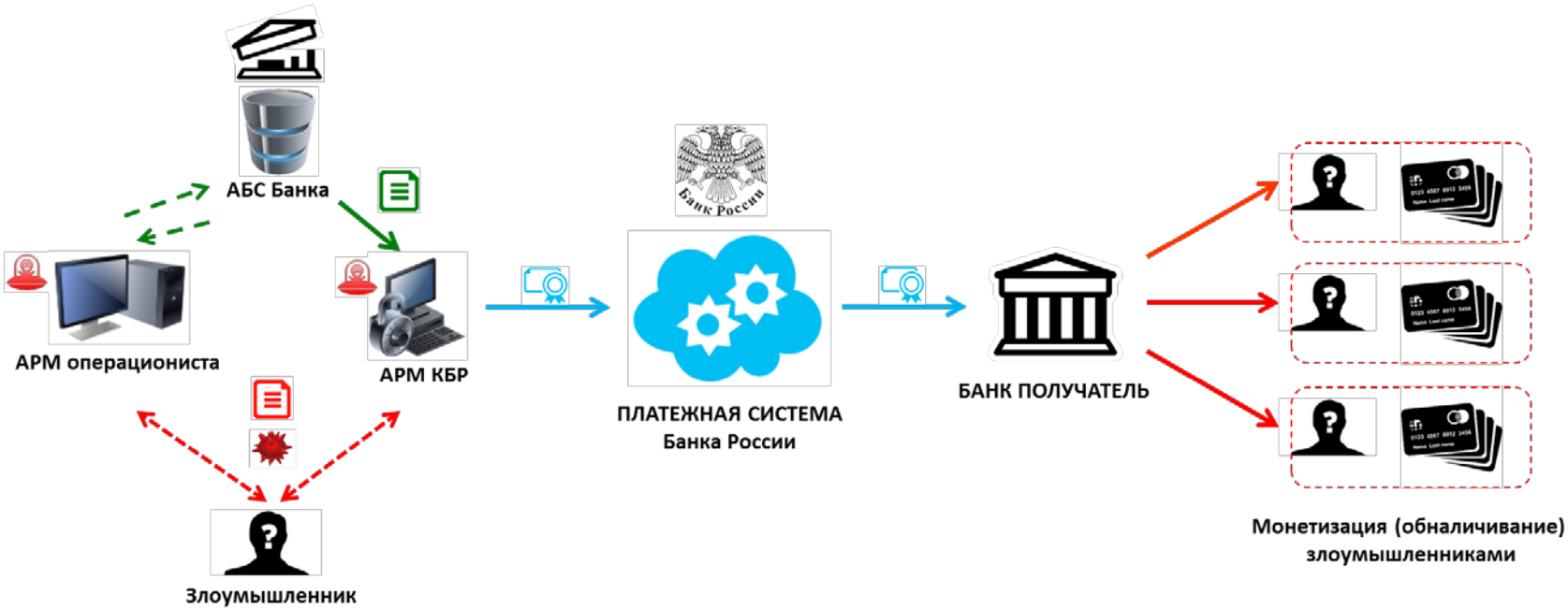
В прошлые годы ФинЦЕРТ также фиксировал атаки всех известных видов на финансовые организации и их клиентов. Однако в 2015-2016 наиболее опасными были:

- Целенаправленные атаки на финансовые организации с подменой входных данных для **АРМ КБР**
- Атаки на финансовые организации **Reversal**

Атаки с подменой входных данных для АРМ КБР

Атаки данного типа были направлены на изменение содержимого XML-документов, используемых для формирования электронных сообщений, направляемого по платежной системе Банка России.

С октября 2015 по декабрь 2016 зафиксировано **25** атак на инфраструктуру кредитных организаций. Совершены попытки хищения денежных средств на общую сумму более **3 млрд 100 млн руб.** Из этой суммы при участии ФинЦЕРТ были предотвращены хищения на сумму порядка **1 млрд 600 млн руб.**



Атаки Reversal

Атака связана с особенностью обработки сообщений об отмене авторизации переводов денежных средств процессинговым центром. В большинстве случаев, процессинговые центры не проверяли подлинность таких запросов, в связи с отсутствием контроля ряда полей указанной операции, .
Пострадала одна кредитная организация, сумма ущерба составила около **450 млн руб**.

Спасибо за внимание!

БАНК РОССИИ
ФИНЦЕРТ