Открытие Банк

СРЕДА:

Открытие Банк

Основные особенности преступных групп:

Особенности преступных групп, специализирующихся в области хищения денежных средств:

1.В преступной группе обязательно присутствует несколько участников, имеющих высшее образование и навыки в области информационных технологий.

2.Для хищения используются компьютеры, мобильные телефоны, современные средства коммуникации.

3.Организация строится по распределенному принципу, не позволяющему вычислить всех участников преступного сообщества даже в случае поимки некоторых его членов, которые просто не знают остальных членов группировки. Задания передаются через анонимные сетевые сервисы или по СМС, деньги переводятся на карты преступников через цепочку посредников, не позволяющую вычислить исходных отправителей.

4.Как правило, преступление совершается в несколько этапов, реализация которых осуществляется участниками группы в различных странах, что еще более затрудняет аналитическую работу, поимку и наказание преступников (в частности, при использовании скиммингового устройства в России дубликаты карт изготавливаются в Малайзии, а денежные средства могут быть получены в Таиланде).

5.Существует значительное число каналов незаконной торговли похищенной финансовой информацией и обмена сведениями о действиях служб безопасности банков и правоохранительных органов. В силу всемирного распространения сети Интернет и невозможности отслеживать все коммуникации, преступники могут обмениваться информацией, практически не опасаясь контроля.

Открытие Банк

SMS ФИШИНГ:

СХЕМА МОШЕННИЧЕСТВА

Мошенники используют широковещательные рассылки SMS сообщений (часто от имени Банка России), содержащих следующую информацию:

- Ваша карта блокирована, Информация по телефону (903) 11111111
- По Вашей карте запланирован платёж на сумму 9895 рублей. Для отмены позвоните по телефону (903) 11111111
- Вам поступил платёж на сумму 5768 фунтов стерлингов подтвердите получение, иначе платеж будет возвращён отправителю Телефон для справок (903) 11111111

Цель сообщения инициировать звонок держателя карты мошенникам.
Во время звонка методами социальной инженерии клиента убеждают подойти к банкомату и выполнить ряд процедур под команду мошенников.
В результате клиент сам переводит средства на карту мошенникам или (что значительно чаще) на счет мобильного телефона мошенников.
Мошенники оперативно переводят средства со счета мобильного телефона в различные электронные кошельки, на карты и обналичивают их.
МОШЕННИКИ ОФОРМЛЯЮТ КАРТЫ И НОМЕРА ТЕЛЕФОНОВ НА ПОДСТАВНЫХ ЛИЦ

МЕТОДЫ БОРЬБЫ:

- Постоянная работа по информированию клиентов о возможных угрозах, рекомендации никогда не звонить по телефонам из SMS, но исключительно по телефонам, указанным на карте или сайте Банка.
- Лимитирование операций перевода средства на счета мобильных телефонов по сумме и количеству.
- Формирование рисковых правил, оценивающих профиль клиента и, при несоответствии платежа профилю клиента – приостановка платежа и контакт с клиентом
- Взаимодействие с операторами мобильной связи и правоохранительными органами для отмены подобных платежей и блокировки телефонов мошенников.

АВТОМАТИЧЕСКИЕ ЗАПРАВКИ:

СХЕМА МОШЕННИЧЕСТВА

Мошенники используют правило платёжных систем, согласно которому перед оплатой по карте бензина на автоматической АЗС производится онлайн авторизация на сумму единицы местной валюты (1 доллар, 1 евро, 1 фунт стерлингов и.т.д). Полная сумма платежа за полученный бензин направляется в банк эмитент посредством финансовой транзакции, которая передаётся в банк - эмитент через несколько дней после совершения операции.

СУТЬ СХЕМЫ:

- **МОШЕННИКИ ОФОРМЛЯЮТ КАРТУ НА ПОДСТАВНОЕ ЛИЦО (КАК ПРАВИЛО ПУЛ КАРТ)**
- Карточный счет пополняется (как правило, через интернет или платежный терминал на сумму 500 -1000 рублей
- На автоматической заправке сообщник мошенника, одетый в форму компании, предлагает заправить автомобиль со скидкой за наличный расчёт, получает наличные деньги от водителя, заправляет автомобиль и рассчитывается картой.
- С карты списывает сумма в одну единицу национальной валюты.
- Операция повторяется до исчерпания суммы пополнения карточного счета.
- Через 2-3 дня основная сумма списания приходит в банк - эмитент, по карте образуется технический овердрафт, карта перестаёт работать.
- Мошенники берут следующую карту из пула и продолжают операции

МЕТОДЫ БОРЬБЫ:

- Отказ в авторизации при повторной оплате бензина на заправочных станциях в течение короткого промежутка времени. Анализ остатка на счёте при появлении авторизации на единицу местной валюты на автоматической заправочной станции.
- Формирование рисковых правил, анализирующих движения по счёту и информирующих службу фрод мониторинга в Банке о необычной активности клиентов на автоматических заправках конкретной страны или региона.

Кража средств через Интернет - Банк:

СХЕМА МОШЕННИЧЕСТВА

- Внедрение на компьютер жертвы вредоносной троянской программы
- Получение информации о персональных данных .
- Внедрение на мобильный телефон жертвы программы мониторинга и перехвата сообщений
- Мониторинг финансовых потоков жертвы, выбор момента совершения преступления
- Хищение средств и перевод их на банковские счета, карты, счета мобильных телефонов или электронные кошельки, контролируемые мошенниками
- Снятие наличных денежных средств либо покупка товаров и услуг, в том числе в сети интернет, для последующей перепродажи.

МОШЕННИКИ ОФОРМЛЯЮТ КАРТЫ, ОТКРЫВАЮТ БАНКОВСКИЕ СЧЕТА, СЧЕТА ТЕЛЕФОНОВ И ЭЛЕКТРОННЫЕ КОШЕЛЬКИ НА ПОДСТАВНЫХ ЛИЦ.

МЕТОДЫ БОРЬБЫ:

- Защита компьютера и мобильного устройства с помощью антивирусных программ
- Установка лимитов и ограничений на платежи через Интернет-Банк
- Мониторинг со стороны Банка платежной активности клиентов, приостановка «подозрительных» платежей до звонка клиенту и подтверждения платежа.
- Контроль со стороны банка IP адреса точки входа клиента в Интернет -Банк.

Открытие Банк

СКИММИНГ:

СХЕМА МОШЕННИЧЕСТВА

- Установка на банкомат или входную группу зоны расположения банкоматов электронного устройства для копирования данных магнитной полосы карты, получения сведений о ПИН коде и сохранения их в памяти устройства для дальнейшего использования мошенниками либо передача мошенникам по радиоканалу в режиме online.
- Изготовление поддельной карты с магнитной полосой, аналогичной полосе оригинальной карты.
- Использование поддельной карты и ПИН кода для проведения операций снятия наличных денежных средств или покупок легкореализуемых товаров в магазинах (электроника, телефоны, заправка, дорогая парфюмерия, фишки казино и др.) (Место скимминга и изготовления карт могут располагаться в разных странах)

МЕТОДЫ БОРЬБЫ:

- Использование чиповых карт (копирование и подделка чипа, практически невозможны)
- Лимитирование операций получения наличных в процессинговом центре банка эмитента
- Установка на банкоматы устройств, препятствующих установке скиммеров (пассивных или активных)
- Внедрение на банкоматах системы анализа внешней среды, отключающих банкомат при подозрении на установку посторонних устройств на банкомат.
- Регулярный осмотр банкоматов (либо видеонаблюдение) на предмет отсутствия посторонних устройств.
- Взаимодействие Банка с правоохранительными органами с целью задержания и преследования мошенников.
- Информирование клиентов о проблеме, формирование «безопасного» поведения клиента
- Анализ профиля клиента, временное блокирование карты и контакт с клиентом при подозрении на мошенничество
- Обязательное оперативное SMS информирование клиента об операциях с его электронными денежными средствами

Открытие Банк

Основные особенности хищения электронных денег:

Схематично процесс хищения средств в вышеприведенных примерах можно разбить на три основных этапа:

1. Поиск уязвимости в банковском ПО или процедурах , компрометация компьютера клиента Банка и, собственно, хищение электронных денежных средств.
2. **Перевод средств на счета или электронные кошельки, контролируемые мошенниками**
3. **Получение наличных денежных средств или оплата товаров и услуг похищенными деньгами.**

Во всех примерах мошенники используют перевод средств на счета, карты, электронные кошельки участников Национальной платежной системы. Если преступники лишатся возможности бесконтрольно открывать и использовать банковские счета и электронные кошельки – это существенно затруднит совершение преступлений.

Этап 1 преступления проходит в пределах одного Банка либо в неконтролируемом пространстве (домашний компьютер, торговые точки, интернет)

Этапы 2 и 3 осуществляются с использованием счетов и сервисов одного или нескольких банков, других операторов электронных денежных средств. Создав адекватную систему мониторинга и предотвращения мошенничества, можно существенно затруднить для преступников процесс использования похищенных средств, осуществить оперативную блокировку похищенных сумм и возврат законному владельцу.

Открытие Банк

НЕОБХОДИМО :

СОЗДАТЬ ЕДИНУЮ ФЕДЕРАЛЬНУЮ СЛУЖБУ ФРОД-МОНИТОРИНГА !

Как один из наиболее предпочтительных вариантов - под эгидой мегарегулятора в лице Банка России.

Основная цель службы - создание в стране операционной среды по переводам электронных денежных средств, максимально затрудняющей мошеннические операции.

На период до завершения формирования данной среды основным направлением деятельности должна стать подготовка законодательных предпосылок для создания и взаимодействия аналогичных локальных систем, объединяющих операторов, в том числе и в рамках банковских ассоциаций и объединений.

Открытие Банк

Принципы организации федеральной службы :

- Предоставление Банкам и другим операторам, имеющим отношение к переводам денежных средств, возможности обмена информацией о предполагаемой причастности клиента к совершению сомнительных (suspected) операций с денежными средствами и сведениями о подобных схемах (безусловно, в нормативной базе должно присутствовать четкое определение "сомнительности" и исчерпывающий перечень сведений о клиенте, которые могут быть переданы).
- Осуществление оперативной проверки получателя платежа по спискам лиц, причастных к подозрительным операциям (возможны различные варианты: от полной проверки всех платежей до проверки «по запросу» платежей, вызвавших подозрение у банков).
- Организация оперативной и аналитической работы с использованием информации о получателях электронных денежных средств, в целях выявления мошеннических схем, а также оперативного противодействия переводу средств в адрес сомнительных получателей - физических и юридических лиц
- Обеспечение временной блокировки или внесудебного возврата переведенных денежных средств отправителям платежей при предоставлении инициатором платежа информации о несанкционированном характере перевода.
- Формирование единых требований к участникам переводов денежных в части обязательных мер по противодействию мошенничеству как условий получения и использования лицензии на такую деятельность.
- Разработка принципов и механизмов финансовой ответственности участников национальной платежной системы в случае, если из – за бездействия оператора электронных денежных средств нанесен ущерб клиенту или другому участнику национальной платежной системы.

МЕРОПРИЯТИЯ ПО ПРЕДОТВРАЩЕНИЮ И ПРЕСЕЧЕНИЮ МОШЕННИЧЕСТВА

НЕОБХОДИМЫЕ ДАЛЬНЕЙШИЕ ШАГИ ДЛЯ УСИЛЕНИЯ БОРЬБЫ С МОШЕННИЧЕСТВОМ В ОБЛАСТИ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ
Совершенствование законодательной базы электронного денежного оборота, в том числе усиление ответственности за преступления в области высоких технологий
Формирование единых правил для всех операторов электронных денежных средств , включая ответственность за бездействие при мошенничестве с использованием оборудования или программного обеспечения оператора.
Укрепление взаимодействия между службами мониторинга и предотвращения мошенничества участников рынка через различные ассоциации, партнёрства и другие объединения участников рынка
Укрепление технологической базы служб фрод-мониторинга участников рынка
Развитие взаимодействия между банками и правоохранительными органами в деле пресечения и предотвращения преступлений в области высоких технологий
Повышение грамотности населения в части безопасного поведения при использовании электронных денежных средств.
СОЗДАНИЕ В РОССИИ ФЕДЕРАЛЬНОЙ СИСТЕМЫ МОНИТОРИНГА И ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСТВА В ОБЛАСТИ ЭЛЕКТРОННОГО ДЕНЕЖНОГО ОБОРОТА