RTM GROUP

Хищение денежных средств с использованием информационных технологий

RTM TECHNOLOGIES — первая экспертная компания, специализирующаяся на проведении нормативных и нормативно - технических экспертиз в области ИБ и ИТ.

rtmtech.ru

СОДЕРЖАНИЕ

Статистика хищения денежных средств в РФ

Несанкционированный перевод – незаконная операция по переводу денежных средств.

По данным ЦБ РФ, за январь-март 2021 года мошенники украли путем несанкционированных переводов 2,9 млрд руб. Это на 57% больше, чем в первом квартале прошлого года.

Из этой суммы банки смогли вернуть клиентам только 7,3%. Для сравнения: в первом квартале 2020 года мошенники украли 1,8 млрд руб., а банки вернули — 11,3%.

Распространённые способы хищения денежных средств

Методы «социальной инженерии» – использование слабостей человеческого фактора

- Преступник может позвонить пользователю банковской карты под видом сотрудника банка, чтобы узнать пароль, сославшись на необходимость решения какой-либо проблемы в компьютерной системе или с банковским счетом, зачастую дезинформируя о его блокировке.
- Преступники отправляют фальшивые SMS-сообщения от близких людей потерпевших, в которых просят о перечислении определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации.

Размещение на открытых сайтах заведомо ложных предложений об услугах и продаже товаров

- Дистанционные хищения совершаются посредством размещения на открытых сайтах заведомо ложных предложений об услугах и продаже товаров за денежное вознаграждение, которое в дальнейшем перечисляется на банковский счет злоумышленника.

Распространённые способы хищения денежных средств

Хищение денежных средств при наличии мобильных телефонов и банковских карт в руках злоумышленников

- Денежные средства неправомерно списываются со счетов потерпевших, когда в руки преступников попадают их мобильные телефоны с установленными на них банковскими сервисами.
- То же самое касается и банковских карт: похитителями совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа – деньги снимаются в банкоматах.

Фишинг - получение идентификационных данных пользователей

- Фишинг представляет собой пришедшие на почту поддельные уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать или обновить личные данные.
- Это письмо как правило содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести необходимую для преступников информацию – пароль от личного кабинета, пин-код банковской карты и другие данные.

Распространённые способы хищения денежных средств

Распространение троянских программ

- Троянские программы могут обладать набором разрешений, позволяющих управлять SMS-сообщениями, совершать различные платежи, выполнять загрузку других вредоносных программ, например банковских троянов или программ-вымогателей. Также могут позволять получить несанкционированный доступ к удалённому управлению компьютером.
- Данные программы распространяются под видом какого-либо легитимного программного обеспечения, приложения для мобильного телефона или файла.

Распространённые способы хищения денежных средств

Распространение банковских троянов

- Банковские трояны или «банкеры» крадут данные учетных записей электронных банковских систем, систем электронных платежей, пластиковых карт пользователей этих услуг и отправляют данные злоумышленнику.
- Для получения учетных данных для доступа к банковским счетам используется фишинг: предполагаемые жертвы перенаправляются на контролируемую злоумышленниками страницу для ввода учетных данных.

Распространение программ-вымогателей

- Программа-вымогатель блокирует компьютер, а затем требует выкуп за то, чтобы разблокировать его.
- В большинстве случаев заражение программами-вымогателями происходит следующим образом. Вредоносная программа сначала получает доступ к устройству. В зависимости от типа программы-вымогателя шифруется либо вся операционная система, либо отдельные файлы. Затем от пострадавших требуют выкуп.

Основные причины хищения денежных средств

Человеческий фактор и техническая неосведомлённость людей.

Поздняя блокировка банковских счетов в случаях утери банковской карты или мобильного телефона с установленным банковским сервисом.

Невыполнение рекомендаций при работе с системой дистанционного банковского обслуживания (ДБО).

Методы «удалённого» хищения денежных средств постоянно эволюционируют.

Как защититься от хищения денежных средств?

Необходимо обучать основам информационной безопасности сотрудников компании и граждан, в особенности пожилых.

Необходимо сразу же после обнаружения утери банковской карты или мобильного телефона с установленным банковским сервисом обратиться в службу поддержки банка.

Необходимо следовать рекомендациям при работе с системой дистанционного банковского обслуживания (ДБО).

Необходимо изучать новые методы «удалённого» хищения денежных средств и сообщать об их появлении гражданам.

Объекты исследования при проведении экспертизы по факту хищения денежных средств

Мобильные телефоны и компьютеры, на которых может быть установлена вредоносная программа

Установленные на мобильных телефонах почтовые клиенты, мессенджеры, банковские сервисы и антивирусное программное обеспечение

Различные лог-файлы

Различные документы из банков, которые содержат подробные сведения о совершённых денежных переводах

Какие методы анализа могут применяться для исследования?

Органолептический анализ	Анализ на основе восприятий органов чувств (например, визуальный анализ фишинговых страниц, фальшивых SMS-сообщений и так далее).
Инструментальный анализ	Проводится при использовании специализированного программного обеспечения для исследования мобильных телефонов, вредоносных программ и так далее.

Опыт RTM Group в проведении экспертиз по фактам хищения денежных средств

1. Подтверждение невыполнения рекомендаций для работы с системой дистанционного банковского обслуживания (ДБО).
2. Выявление нетипичных признаков осуществления денежных переводов (получатель, время, сумма перевода, устройство и регион).
3. Обнаружение вредоносного программного обеспечения, которое предоставляло удалённый доступ к компьютеру.
4. Обнаружение вредоносного программного обеспечения, которое предназначено для кражи пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт.

СПАСИБО ЗА ВНИМАНИЕ!

Музалевский Федор Александрович

Директор технического департамента RTM Group

Волокитин Сергей Анатольевич

Ведущий эксперт компьютерно-технического направления RTM Group

8 800 201-20-70

info@rtmtech.ru

https://rtmtech.ru

GroupRTM

rtm.group

@GroupRtm

rtm.group.Russia

t.me/kurilka_ib