УДК 343.985

А.Г. Александров, С.Г. Клюев, Е.С. Поликарпов, М.А. Ледовская

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ УПРАВЛЕНИИ ДЕНЕЖНЫМИ СРЕДСТВАМИ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ

Краснодарский университет Министерства внутренних дел Российской Федерации, Краснодар, Россия

Исследованы вопросы использования мобильных приложений, мобильных устройств связи в качестве средства совершения хищения денежных средств с электронных банковских счетов, балансовых средств мобильных счетов. В статье рассмотрены способы совершения краж денежных средств с расчетного счета через «Мобильный банк». Исследован способ совершения хищения денежных средств с электронного счета с помощью вредоносного программного обеспечения. Троянская программа, используемая злоумышленниками, распространялась через SMS-рассылки, в которых была ссылка на загрузку вредоносной программы под видом лицензионного программного обеспечения, во время установки которой запрашивались права администратора, также ссылки на установку троянской программы приходили через мессенджеры и личные сообщения в социальных сетях, а также размещались на стенах пользователей социальных сетей. Рассмотрен способ совершения хищения денежных средств с электронного счета с использованием SMS-банкинга – процедуры перевода денег при помощи отправки специально сформированного SMS сообщения на номер банка. Исследован один из новых видов мошенничества с использованием возможностей средств мобильной связи, а именно USSD кодов. Пользователю сотовой сети сообщалось о проверке мобильной линии и предлагается набрать USSD код, в случае выполнения данной просьбы «сотового оператора» мошенники получают доступ к SIM карте, что позволяло им производить фактически любые действия: осуществлять звонки за счет абонента, получать доступ к мобильному банку.

Ключевые слова: мобильные приложения, хищения, мобильный банк, SMS-банкинг.

Введение.

С появлением смартфонов, поддерживающих множество функций, участились случаи незаконного получения доступа к их содержимому. Это обуславливается наличием в памяти телефона достаточных сведений для реализации преступного плана, связанного с воровством денег. В основном жертвами злоумышленников являются владельцы телефонов с установленной операционной системой Android. Однако, среди потерпевших встречаются и пользователи простых телефонных аппаратов сотовой связи [1].

Ситуации, когда деньги украдены с карты через мобильный банк, встречаются довольно редко. Это объясняется тем, что системы безопасности во многих банках делают данную схему крайне трудновыполнимой, но все же иногда имеющей место. Если вдаваться в

техническую составляющую данной схемы, то заключается она в том, что на ваш телефон при переводе средств не приходит ни SMS сообщения, ни требования ввести разовый ключ. Это объясняется тем, что некоторые сотовые операторы крайне халатно относятся к безопасности своих клиентов, и мошенники могут (при серьезном подходе к делу) установить так называемый блокиратор (или перехватчик), с помощью которого SMS с кодом будет приходить не на номер, привязанный к карте, а на телефон злоумышленников.

При этом в выписке по счету, уже позже, можно будет обнаружить реквизиты, на которые были переведены средства. Получается, что вы нечего не теряли, код никому не сообщали, но деньги с вашего счета чудесным способом исчезли. Обращение в банк за разъяснением ситуации, как правило, ничего не дает, так как транзакция в выписке указана, а высланный банком код был использован. Поэтому требовать что-то от банка в подобных случаях бесполезно.

Основная часть.

Приложение мобильный банк создано для управления банковским счетом самостоятельно. А вот Интернет-банк немного другое понятие. Причем, стоит заметить, что управлять Интернет-банком можно, только с компьютера. Конечно, современные телефоны позволяют работать с подобными сайтами, но при этом нарушается безопасность. Работать с такими интернет-страницами нет смысла даже на планшете. По поводу этих правил есть множество нюансов, которые будут описаны ниже.

Сам по себе, мобильный банк представляет версию интернет-банка, которая настроена на непосредственную работу с малыми экранами, имеет оптимизированный функционал и интерфейс. При его помощи можно осуществлять множество операций, среди которых:

- пополнение электронных кошельков;
- осуществление оплаты за услуги коммерции;
- участие в банковских акциях;
- пополнение счета телефона;
- получение детальной информации о своем счете;
- блокирование счета;
- перевод своих средств на другие карты.

То есть, количество возможностей, практически, как у обычного сайта, но нельзя открывать и закрывать счета или оплачивать конкретные покупки, так как на подобные действия установлены ограничения.

В принципе, мобильный банк направлен на осуществление быстрого расчета, но иногда могут возникнуть небольшие проблемы. Например,

мобильный банк неким образом пытается выманить у вас деньги в форме некоторых простых операций, суммы которых могут быть разными, также как и причины оплаты.

Раньше мобильный банкинг натыкался на некоторые проблемы в виде зависания платежей или переводов, но со временем проблемы решились. Почему же нарушается безопасность на малых экранах, ведь функции работают безотказно и нет причин для переживаний? Не все так просто, как кажется, ведь малый функционал не может обеспечить полноценной безопасности.

Если взглянуть глубже, то каждому понятно, что мобильный банк – приложение, которое без труда обеспечивает выход в Интернет, но отличается принципиально от любой программы. Планшет или мобильный телефон работают таким образом, что могут автоматически, без дополнительных подсказок, которые способны возникать на ноутбуке, но не на телефоне, пересылать некоторую информацию на посторонние серверы. Последние, в свою очередь, могут использовать данные, если перехватят их в свою пользу.

Вот так и выходит, что теряются средства. В таких случаях, даже установленный антивирус, адаптированный под мобильный интерфейс, не сможет помочь. Такой «вредитель» внедряется с помощью программы, которую невозможно определить, так как в мире не создано системы, которая смогла бы контролировать и стандартизировать мобильные приложения. Понятно, что распространить, растиражировать приложение может кто угодно.

Решение проблемы пока нельзя осуществить в меру того, что она только возникла. Следовательно, современные банки, такие как «Сбербанк» призывают клиентов использовать приложения, которые расположены исключительно на сайте банка. Вот поэтому рекомендуется применять компьютеры для этой системы, которые более-менее могут среагировать на внедрение или, по крайней мере, сообщить пользователю о подозрительном интернет-ресурсе.

Мошенники придумывают новые способы совершения преступлений. К одному из новых видов мошенничества относится использование возможностей средств сотовой связи, а именно USSD кодов. Сотовый абонент получает телефонный звонок на свой мобильный телефон от инженера-оператора мобильной кампании, клиентом которой он является. Оператор (он/она) представляется и говорит стандартную фразу: «В целях повышения качества обслуживания разговор записывается…» и далее пользователю сотовой сети сообщается о проверке мобильной линии и предлагается набрать USSD код - #90 или

#09 или другую комбинацию цифр и символов. В случае выполнения данной просьбы «сотового оператора» мошенники получают доступ к SIM карте, что позволит им производить фактически любые действия: осуществлять звонки за счет абонента, получить доступ к мобильному банку. В случае поступления подобного звонка необходимо сразу нажать клавишу отбоя вызова и не выполнять никаких просьб злоумышленников.

Так же мошенники могут прибегнуть к другой тактике. На телефон абонента приходит SMS сообщение следующего содержания: «Посмотри свои фотографии»; или «Посмотри фото нужно разобраться». Сообщение содержит имя абонента, а иногда и даже улицу проживания. При открытии данного сообщения с лицевого счета абонента списываются все балансовые средства. Подобные SMS сообщения необходимо сразу удалять и не переходить по предлагаемой интернет ссылке.

В последнее время увеличилось число краж денежных средств, находящихся на расчетных счетах физических и юридических лиц в различных кредитных учреждениях, с использованием сети «Интернет». Сейчас банки предоставляют физическим и юридическим лицам услуги по перечислению денежных средств на различные расчетные счета через автоматизированную систему в сети «Интернет» – так называемый «мобильный банк» (банк-онлайн). Система позволяет получать подробную информацию о банковских продуктах (вклады, карты, кредиты), совершать платежи, оплачивая, в частности, коммунальные услуги, связь, интернет, телевидение. С помощью системы можно пополнять счета электронных кошельков, совершать платежи по произвольным реквизитам, осуществлять переводы между вкладами и банковскими картами, переводить средства клиентам банка.

Некоторые граждане при открытии расчетных счетов и получения банковской карты осуществляют регистрацию в системе «мобильный банк» в отделении банка, при этом идентификатор и пароль к личному кабинету для осуществления банковских операций сообщаются на чеке. После получения данных сведений и первичного использования паролей клиентом чек нередко выбрасывается в мусорную корзину. При этом граждане даже не задумываются о том, что может в дальнейшем произойти с данными сведениями, кто и для каких целей может их использовать. Через некоторое время клиент банка может узнать, что с его расчетного счета не санкционированно были списаны и переведены различные суммы денежных средств.

Из сложившейся практики по фактам хищений через «мобильный банк», следует, что обычно денежные средства переводятся за оплату покупки на расчетные счета магазинов, расположенных за пределами

Российской Федерации, либо на расчетные счета подставных лиц.

Получается, что такие преступления совершаются по невнимательности и беспечности граждан, которые «выбрасывают» сведения: идентификатор и пароли от личного кабинета в «мобильном банке». И, как ни странно, реализации сложившейся ситуации в какой-то мере поспособствовал сам банк, выпустивший карту. При подключении карты к услуге «Мобильный банк», предоставляется возможность переводить средства с карты, привязанной к номеру телефона, на другую карту посредством SMS-сервиса. Во многих банках есть такая услуга. Отправка SMS сообщения на короткий номер, например 900, с текстом «Инфо» (в любой раскладке и в любом регистре) дает возможность узнать информацию обо всех картах, привязанных к данному номеру. Поэтому мошеннику не обязательно заранее знать о существовании карты. SMS сообщение с текстом «Перевод» на тот же номер с указанием другого телефона, к которому так же привязана карта и суммы, даёт возможность преступнику перевести указанную сумму на свою карту. На выполнение данных действий злоумышленнику потребуется не более минуты, соответственно он получает возможность обналичить денежные средства в ближайшем банкомате.

Хищение денежных средств с электронного счета может быть совершено с использованием вредоносного программного обеспечения. В данном случае злоумышленники использовали собственно разработанный банковский троян, предназначенный для хищения денежных средств через программы мобильного банкинга, установленные на смартфонах под управлением платформы Android. Распространение вредоносной программы преступники осуществляли фактически во всех регионах страны.

Вирусные атаки проводились злоумышленниками на мобильные устройства клиентов российских банков, работающих на платформе Android. Троянская программа, которую они использовали, после установки на мобильное устройство запрашивала баланс привязанной к номеру банковской карты, скрывала поступающие SMS-уведомления и осуществляла переводы денежных средств с банковского счета на счета, подконтрольные злоумышленникам.

Вредоносное программное обеспечение было разработано именно для того, чтобы совершать хищения денежных средств с банковских счетов. Программа обладает функциями, позволяющими совершать хищения более эффективно. Одним из способов совершения хищения является использование SMS-банкинга – процедуры перевода денег при помощи отправки специально сформированного SMS сообщения на номер

банка.

Также злоумышленники получали данные о банковских картах, используя фишинговые (фальшивые) страницы в сети Интернет. При открытии диалогового окна Google Play, вредоносная программа показывала свое окно с предложением ввести данные банковской карты. После введения пользователем данных своей карты, они немедленно передавались на сервер злоумышленника.

В дальнейшем преступники использовали фишинговые страницы для получения не только данных банковской карты, но и для завладения логином и паролем от интернет-банкинга. Когда пользователь запускал банковское приложение, троянская программа подменяла оригинальное окно на фишинговое, где пользователь сам вводил необходимые данные, которые передавались на сервер подконтрольный преступникам.

Обладая логином, паролем, а также доступом ко всем SMS сообщениям, в том числе от банков с SMS-кодами, злоумышленник мог успешно совершать банковские переводы.

Распространяя вредоносную программу через SMS-рассылки, в которых была ссылка на загрузку вредоносной программы под видом Adobe Flash Player, во время установки которой запрашивались права администратора, также ссылки на установку троянской программы приходили через мессенджеры и личные сообщения в социальных сетях, а также размещались на стенах пользователей соцсетей. [2]

Исходя из анализа рассмотренных примеров, указанные преступления условно можно разделить на несколько видов:

- совершенные путем использования sim-карты, приобретенной правонарушителем у оператора сотовой связи, которая имеет абонентский номер предыдущего владельца с активной услугой «Мобильный банк»;
- совершенные путем использования sim-карты, выбывшей из владения собственника (потеря, хищение sim-карты);
- совершенные путем использования вредоносного программного обеспечения (компьютерного вируса) либо вредоносных компьютерных программ, загруженных на мобильный телефон;
- совершенные путем подключения на абонентский номер правонарушителя через банкомат услуги «Мобильный банк» с использованием банковской карты потерпевшего. [3]

Выявленные преступления указанной категории, как правило, квалифицируются по ст. 158 УК РФ, а в некоторых случаях по совокупности ст.ст. 158 и 272 УК РФ. Однако не всегда судебно-следственная практика единообразна, а в ряде случаев вообще противоречива. В основном это относится к случаям оценки

правоприменителями действий правонарушителей, совершивших хищения денежных средств путем использования sim-карты, приобретенной ими у оператора сотовой связи, имеющей абонентский номер предыдущего владельца с активной услугой «Мобильный банк», либо выбывшей из владения собственника (потеря, хищение sim-карты). Такая неоднозначная судебно-следственная практика в области сложилась в виду отсутствия каких-либо официальных разъяснений о совокупности применения ст.ст. 158 и 272 УК РФ при указанных выше обстоятельствах. [3]

Таким образом, столкнувшись с указанными трудностями, правоприменители неоднозначно квалифицируют подобные действия по совокупности преступлений, предусмотренных статьями 158 и 272 УК РФ. При квалификации хищении денежных средств с электронного счета с использованием вредоносного программного обеспечения, позволяющих получить контроль над операционной системой мобильного телефона, необходимо проведение соответствующей компьютерной экспертизы. При наличии положительного заключения, действия злоумышленников должны квалифицироваться по совокупности преступлений, предусмотренных ст.ст. 158, 272 и 273 УК РФ, а при отрицательном - по ст. 158 УК РФ. [3]

Заключение.

В настоящее время единственным способом частной превенции данной ситуации является установка антивирусного программного обеспечения, либо использование обновленной версии приложения мобильного банка для платформы Android со встроенным антивирусом.

Также в целях профилактики краж денежных средств с расчетного счета через «Мобильный банк» необходимо следовать нескольким простым правилам:

1. Если у Вас подключен «Мобильный банк», «SMS банкинг» или другой подобный сервис (в каждом банке он свой), то никогда не оставляйте телефон, к которому привязана карта, без присмотра.

2. Если Вы до сих пор не знаете, подключены ли Вы к подобной услуге, а такое часто бывает, то обязательно узнайте. И сделайте это ка можно скорее любым доступным способом. Посмотрите на сайте Вашего банка, как это лучше сделать, проверьте, а потом уже сами решите, надо ли Вам это. Многие банки подключают данный сервис, не спрашивая об этом клиента. Или спрашивают, но завуалированно, например «Вы хотите, чтобы Вам приходила смс, когда будет перечислена пенсия?».

3. Если Вы потеряли телефон, к которому привязана банковская карта - немедленно снимите все деньги, обратитесь в банк для блокировки

карты и оператору связи для блокировки сим-карты.

4. Не следует никому рассказывать о своих финансах на картах, счетах, электронных кошельках. Не сообщайте никому никакие данные, пароли, коды, номера, не говорите об подключённых услугах и сервисах. И держите телефон всегда под присмотром.

5. Установить по карте лимит на совершение безналичных расходных операций в календарный месяц. Использовать для Мобильного банка простой телефон.

В итоге, можно сделать вывод, что мобильный банк не является безопасным, ведь ограничивать его со всех сторон нет возможности, хотя работает он безупречно. Когда будет решена проблема непонятно, но недостатки очевидны: особой привязки к функции SIM нет и мобильный банк – не самостоятельная программа. Так же правоприменительной практикой выработана необходимость принятия Постановления Пленума Верховного Суда Российской Федерации, содержащего разъяснения отдельных вопросов, возникающих у судов при применении законодательства, предусматривающего ответственность за совершение преступлений в сфере компьютерной информации.

ЛИТЕРАТУРА

1. Как мошенники снимают деньги с банковской карты через мобильный банк: [Электронный ресурс] URL: http://znatokdeneg.ru/uslugi-bankov/plastikovye-karty/moshenniki-snyali-dengi-s-karty-cherez-mobilnyj-bank-kak-vernut.html (Дата обращения: 24.07.2018).
2. Как происходит хищение денег через мобильный банкинг: [Электронный ресурс] URL: https://www.gazeta.ru/tech/2015/04/13/6637105/great-android-russian-robbery.shtml (Дата обращения: 25.07.2018).
3. Баранов С.А., О некоторых вопросах квалификации действий лиц, совершивших кражу денежных средств с использованием системы дистанционного банковского обслуживания «мобильный банк» // Баранов С.А., Волченко А.В., Лазарев Д.С., Когтева А.Н., Новикова Е.А., Проблемы правоохранительной деятельности 2016. № 1. С. 14-17

A.G. Aleksandrov, S.G. Klyuev, E.S. Polikarpov, M.A. Ledovskaya

ANALYSIS OF THREATS TO INFORMATION SECURITY WHEN THE MANAGEMENT OF FUNDS USING MOBILE DEVICES

Krasnodar University of the Ministry of the Interior of the Russian Federation, Krasnodar,Russia

The issues of using mobile applications, mobile communication devices as a means of committing theft of funds from electronic bank accounts, balance funds of mobile accounts are investigated. In the article methods of committing money thefts from a settlement account through the "Mobile Bank" are considered. The way of committing the theft of funds from an electronic account using malicious software was investigated. The Trojan program used by attackers was distributed via SMS-mailings, in which there was a link to downloading a malicious program under the guise of licensed software, during the installation of which administrator's rights were requested, also links to the installation of the Trojan program came via instant messengers and personal messages on social networks, and Also, they were placed on the walls of users of social networks. The method of committing theft of funds from an electronic account using SMS banking is considered. It is a procedure for transferring money by sending a specially generated SMS to the bank number. One of the new types of fraud using the capabilities of mobile communications, namely USSD codes, has been investigated. The user of the cellular network was informed of the mobile phone check and is asked to dial the USSD code, if this request is made by the "cellular operator", scammers get access to the SIM card, which allows them to make virtually any actions: make calls at the expense of the subscriber, access to the mobile bank.

Keywords: mobile applications, theft, mobile banking, SMS banking.

REFERENCES

1. Kak moshenniki snimayut den'gi s bankovskoy karty cherez mobil'nyy bank: [Elektronnyy resurs] URL: http://znatokdeneg.ru/uslugi-bankov/plastikovye-karty/moshenniki-snyali-dengi-s-karty-cherez-mobilnyj-bank-kak-vernut.html (Data obrashcheniya: 24.07.2018).
2. Kak proiskhodit khishchenie deneg cherez mobil'nyy banking: [Elektronnyy resurs] URL: https://www.gazeta.ru/tech/2015/04/13/ 6637105/great-android-russian-robbery.shtml (Data obrashcheniya: 25.07.2018).
3. Baranov S.A., O nekotorykh voprosakh kvalifikatsii deystviy lits, sovershivshikh krazhu denezhnykh sredstv s ispol'zovaniem sistemy distantsionnogo bankovskogo obsluzhivaniya «mobil'nyy bank» // Baranov S.A., Volchenko A.V., Lazarev D.S., Kogteva A.N., Novikova E.A., Problemy pravookhranitel'noy deyatel'nosti 2016. No. 1. pp. 14-17