Babr24.com

Автор: Алексей Муравьев РАССЛЕДОВАНИЯ, ИРКУТСК 12291 09.04.2012, 09:46 1156

Сбербанк: апофеоз ненадежности?

Со Сбербанком в новой, капиталистической России всегда было что-то не так.

Унаследовав худшие черты советских сберкасс, Сбербанк умудрился по-крупному «кинуть» всех своих клиентов, в начале 90-х годов фактически отказавшись от гарантий обеспечения вкладов граждан. Это привело к тому, что вклады населения фактически превратились в ничто. Несмотря на то, что Сбербанк в настоящее время является весьма преуспевающей и прибыльной организацией, он не торопится выплачивать компенсации по тем вкладам. Вероятная логика руководства банка вполне очевидна: зачем выплачивать компенсации, если владельцы «старых» сбережений скоро уйдут из этого мира естественным путем.

Пользуясь государственной «крышей», Сбербанк консолидировал у себя не только значительные вклады населения, но и фактически монополизировал всвозможные коммунальные платежи. Само собой, сделано это было все в тех же «совковых» традициях: тесные помещения, огромные очереди, некомпетентные и еле передвигающиеся сотрудники, невероятно неудобный режим работы.

Сбербанк одним из последних в России решился на нормальную автоматизацию, снизойдя до мировых стандартов пластиковых карт и электронных переводов. Но и тут все оказалось не слава богу.

Через систему «банк-клиент» вдруг начали исчезать деньги со счетов. Последний крупный скандал произошел в Иркутске в середине марта 2012 года: со счета некоммерческого фонда было переведено полмиллиона рублей на частное лицо. Любопытно, что Сбербанк в таких вопросах занимает жесткую отказную позицию, обвиняя во всем клиента и несоблюдение им правил работы с «банк-клиентом». Вот что рассказывает про технологию «банк-клиент» специалист по банковской безопасности одного из иркутских банков М.:

«В подавляющем большинстве случаев благоприятные условия для мошенников создают сами пользователи, не соблюдающие требования информационной безопасности и надеющиеся на русский "авось".

Не нужно обвинять во всех бедах банк. Вы же, когда покупаете железный сейф, не считаете, что за сохранность средств в нем ответственна фирма, которая Вам этот сейф продала. Так и тут: не нужно раскидывать ключи от сейфа где попало, или вовсе оставлять его незапертым, а потом удивляться, что из него пропали ценности.

Как это работает? Вы формируете документ. Под электронным документом ставится электронно-цифровая подпись (ЭЦП), которая обеспечивает целостность и аутентичность документов в системе, то есть гарантирует, что документ отправили именно Вы, и что после отправки документ не изменялся. Для обеспечения защищенного взаимодействия через Интернет используются функции криптографической защиты: данные, которые Вы отправляете, шифруются. Доступ к секретному ключу ЭЦП защищен паролем, известным только его владельцу. Не имея в распоряжении секретного ключа и не зная пароля доступа к нему, невозможно сформировать подпись под электронным документом.

С клиентом заключается договор, по которому клиент обязуется хранить и не передавать третьим лицам пароль и хранилище с секретным ключом ЭЦП клиента. Электронный документ с ЭЦП является основанием для совершения финансовых операций и доказательной базой при разрешении конфликтной ситуации. Таким образом, банк не несет ответственности за ущерб, причиненный клиенту в результате использования третьими лицами секретного ключа ЭЦП клиента.»

Каким образом в случае с Иркутским фондом был украден «ключ»? Очень просто: через Интернет. Клиенту «подсадили» троянскую программу, которая и украла ключи электронно-цифровой подписи, хранящиеся на «флэшке».

Казалось бы, действительно, виноват сам клиент. Но при ближайшем рассмотрении проблемы возникает несколько вопросов.

Во-первых, представим ситуацию: некто нашёл (или даже стащил) какой-то ключ - обычный, от физического, а не виртуального замка. Что ему с этим ключом делать? Совать его во все подходящие по типу замки? А если за дверью окажется хозяин квартиры? А если замок стоит на двери в закрытом подъезде? А если владелец ключа - из другого города? А если это ключ вообще не от квартиры, а от сменённого уже замка? Вот так и в банковском деле. Ведь очевидно, что система «банк-клиент» стоит далеко не на всех компьютерах в России. Для того, чтобы «подсадить» на конкретный компьютер троянскую программу, нужно **знать**, у какого клиента сколько денег на расчетном счету, каким банком обслуживается клиент и какой у него IP-адрес. Само собой, без «крота» (и не одного) внутри самого Сбербанка тут обойтись нельзя: а это означает, что служба безопасности банка, что называется, «мышей не ловит».

С точки зрения цивилизованной банковской системы, «слив» каких-либо сведений о клиенте - целиком на совести банка, и банк несет за это полную ответственность. Но это в цивилизованной, конечно.

Конечно, вероятен и такой вариант, когда некий злоумышленник распространяет «троянов» по всем доступным компьютерам, ворует все пароли подряд, а потом уже думает, что с ними делать. Но в этом случае мы должны представить себе некоего сетевого «профессора Мориарти», консолидировавшего в своих руках нити сотен преступных группировок. Идея заманчивая, но, скорее всего, невероятная: сейчас не XIX век, и спецслужбы работают ничуть не хуже, чем сетевые преступники. А чем сильнее консолидация преступных нитей в одних руках, тем выше вероятность «провала».

Во-вторых, служба безопасности Сбербанка, само собой, прекрасно знает о существовании «троянских коней» и прочих вирусных/хакерских программ. И, тем не менее, совершенно спокойно пропускает невероятно подозрительную и откровенно «паленую» транзакцию со счета юридического лица на счет физического лица в совершенно другом городе. Ну да, банк не обязан перезванивать главному бухгалтеру и уточнять, действительно ли эта операция была проведена. Не обязан - но может. И вот это - уже вопрос репутации. В приличном банке такая махинация не пройдет никогда, потому что приличный банк заботится в первую очередь о своей репутации. В банке же с махровыми «совковыми» традициями клиент всегда неправ - ему и расплачиваться.

Наш собеседник, специалист по банковской безопасности, подтверждает неправоту банка в этом вопросе:

«Единственное, что мне непонятно в этой истории, - это почему операционисты провели платеж на крупную сумму со счета юр. лица на физ. лицо. Очень часто такие платежи являются либо случаями мошенничества, либо способом отмывания денег; в некоторых банках есть практика звонков клиентам с уточнением реквизитов документа. Знаю случаи, когда благодаря таким звонкам выявлялись факты кражи ключей и таким образом предотвращались потери денег клиентов. »

Заметим, что еще пять лет назад система «банк-клиент» производства Сбербанка имела «привязку» к компьютеру. То есть провести транзакцию можно было только с одного компьютера - и ни с какого другого. При запуске система «банк-клиент» запускала проверку идентификационных кодов материнской платы, подделать который практически нереально.

Почему такая защита была отменена? Это - тайна, неизвестная никому. Вполне вероятно, что именно эта система мешала кому-то использовать чужие счета для обогащения. Возможно и то, что «системщики» просто облегчали себе жизнь, избавившись от «настройки лишних гаджетов». Однако отмена подобной защиты означает, что Сбербанк сознательно и целенаправленно создал огромную «дыру» в собственной безопасности.

В-третьих, через систему «банк-клиент» возможен перевод только на то физическое лицо, которое зарегистрировано в банковской системе. То есть, как ни крути, но Сбербанк (или полиция) может узнать, кому были переведены эти деньги. То есть злоумышленника можно найти. Не можем же мы представить себе ситуацию, когда крупнейший банк в России, почти наполовину государственный, способен перевести полмиллиона рублей неизвестно кому, и даже не спросить данные паспорта?

Ну и четвертое, самое главное. С 2001 года в России существует закон о противодействии легализации (отмыванию) доходов. Согласно этому закону, любая значительная сумма денег, переводимая частному лицу, требует особо пристального внимания банка и обязательной идентификации лица, которому переводятся деньги. Судя по всему, в рассматриваемом нами случае Сбербанк просто забыл о существовании такого закона.

Все эти аргументы, безусловно, известны руководству Сбербанка России. Однако воз и ныне там. Сбербанк

не хочет нести никакой ответственности за средства, выведенные криминальными хакерами со счетов его клиентов.

Автор: Алексей Муравьев © Babr24.com РАССЛЕДОВАНИЯ, ИРКУТСК 12291 09.04.2012, 09:46 1156
URL: https://babr24.com/?ADE=104596 Bytes: 8418 / 8397 Версия для печати

Автор текста: **Алексей Муравьев**.

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта