Безопасность банковских операций

Артем Баранов – ведущий вирусный аналитик компании ESET.

Введение

Безопасность при проведении банковских операций играет на сегодняшний день очень большую роль. Появление различных сервисов онлайн-банкинга, оплата покупок через интернет, повсеместное использование POS-терминалов сделали проблему безопасности банковских операций актуальной как никогда. Если еще лет десять назад у пользователя в России не было большого выбора механизмов оплаты интересующей его услуги или покупки, то сейчас ситуация существенно изменилась.

Сегодня проведение банковских операций может выполняться следующими широко распространенными способами:

- *проведение платежа через сервис онлайн-банкинга;*
- *платеж с использованием мобильного приложения (мобильное устройство);*
- *онлайн-платеж через браузер;*
- *платеж с использованием приложения банка для ПК/Mac;*
- *платеж с использованием POS-терминала;*
- *проведение операции через банкомат;*
- *посещение банковского учреждения.*

Очевидно, что из вышеперечисленных способов проведения банковской операции оплата через POS-терминал наиболее популярна среди пользователей, как, впрочем, и онлайн-платеж или использование банкомата. Сегодня банки предоставляют пользователям бесплатные приложения по работе со своим счетом и выполнение необходимых операций на ПК/Mac, а также сервисы онлайн-банкинга для работы через браузер.

Каждый из этих способов за исключением, пожалуй, посещения банка и проведения банковской операции через сотрудника банка является потенциальной целью злоумышленников. Так или иначе, их интересуют данные, находящиеся на кредитной карте, в т.ч. ее номер, CVV-код, имя держателя, а также PIN-код. Получив доступ к этой информации, злоумышленники могут затем продать ее на специальных подпольных форумах кардеров либо самостоятельно воспользоваться этой информацией для получения средств со счетов скомпрометированных пользователей. Рассмотрим безопасность вышеперечисленных способов оплаты.

Удобно и быстро

Первые четыре способа используются пользователями из-за их удобства и доступности на компьютере или мобильном устройстве. При использовании веб-браузера для оплаты покупки или проведения банковской операции пользователю нужно ввести данные своей кредитной карты в специальные формы веб-страницы, из которой они будут доставлены на сервер банка. Такая операция сама по себе является потенциально небезопасной, поэтому банки и сервисы онлайн-оплаты предпринимают необходимые действия по защите такой операции следующими способами:

- использование https для страницы ввода данных кредитной карты (передаваемые между компьютером пользователя и сервисом оплаты данные шифруются на уровне http-протокола, что исключает их попадание к третьим лицам);
- использование двухфакторной аутентификации (обычно этот метод основан на использовании одноразовых паролей, выдаваемых банком. Также это может быть код подтверждения на основе SMS-сообщения, т.н. mTAN (Mobile Transaction Authentication Number). Операция проводится только после подтверждения пользователем, т.е. когда он вводит действительный mTAN-код или одноразовый пароль).

Злоумышленники могут использовать специальный вредоносный код, т.н. банковские вредоносные инструменты или банковские троянские программы для хищения данных кредитной карты при использовании браузера для оплаты. Суть такого вредоносного ПО сводится к тому, что, будучи установленным на компьютере пользователя, он использует специальные механизмы внедрения своего кода в процесс браузера и получения оттуда интересующих его конфиденциальных данных.

Обычной практикой таких вредоносных программ является отображение для пользователя поддельных веб-форм для ввода номера карты, имени держателя и даты окончания ее действия. По сути, только очень внимательный пользователь сможет отличить поддельную веб-форму от настоящей. После ввода данных в такую форму они записываются в специальный файл и позже отправляются на сервер злоумышленников.

Использование https при таком виде атаки не является проблемой для вредоносной программы, поскольку она может управлять процессом получения данных внутри процесса. В то же время многие из них при показе поддельной веб-страницы с формами отключают использование https, т.е. в строке браузера пользователя не будет указано использование https. Для самого пользователя такой признак является ключевым показателем того, что следует отказаться от проведения операции и обратиться к антивирусному ПО.

Двойной узел

Другой механизм, используемый банками, т.н. двухфакторная аутентификация, является действительно серьезной защитой от злоумышленников. В то же время ESET как антивирусная компания уже наблюдала использование злоумышленниками таких вредоносных программ, которые умеют обходить данный метод защиты. Суть его сводится к установке специального мобильного компонента вредоносного кода на мобильное устройство пользователя. После установки такого компонента вредоносная программа перехватывает поступающие от банка SMS-сообщения и перенаправляет их злоумышленникам. Для защиты от подобных программ следует быть более бдительными, поскольку злоумышленники используют специальные фишинговые уловки для убеждения пользователя в установке этого мобильного компонента. Одной из таких вредоносных программ является обнаруженный нами в прошлом году вредоносный инструмент Hesperbot, который использует именно такой подход.

Приложение всех усилий

Что касается использования специальных приложений для работы с системой онлайн-банкинга, а также использования сервиса онлайн-банкинга через браузер, то в данном случае злоумышленников могут интересовать логин и пароль, используемые пользователем для входа в аккаунт. Например, обнаруженная вирусной лабораторией ESET вредоносная программа Win32/Spy.Ranbyus использует специальные механизмы атаки на Java-приложение известной системы онлайн-банкинга (рис. 1).

```
int __usercall inject_javaw<eax>(int a1<ebx>)
{
  int v1; // eax@3
  char v3; // [sp+0h] [bp-10h]@1

  init(&v3);
  create_process_mutex(&v3);
  if ( get_config_value_96() )
    get_import(&v3);
  delete_iBank_files();
  check_BIFIT_keys(a1);
  mem_alloc();
  init_java_hooks(&v3);
  init_javaw_grabber();
  init_java_javaw_browser_grabber();
  v1 = get_imports_table();
  (*(v1 + kerne132_Sleep))(0xFFFFFFFFu);
  exit_process(&v3);
  return 0;
}
```

Рис. 1. Часть кода вредоносной программы, которая осуществляет атаку на приложение онлайн-банкинга.

POSледний рубеж

Оплата с использованием POS-терминалов также может быть небезопасной в том случае, если злоумышленники смогли скомпрометировать компьютеры внутренней сети компании, ответственной за обслуживание таких терминалов. Последние инциденты в конце ушедшего года показали, что десятки миллионов пользователей могут быть скомпрометированы таким способом, если компания не заботится о безопасности своих клиентов. В качестве примера можно привести получивший широкий резонанс инцидент с американской ритейлерной компанией Target, которая была скомпрометирована злоумышленниками, в результате чего все используемые POS-терминалы, которые использовались в магазинах этой сети, оказались небезопасными.

Вредоносные программы, которые ориентированы на компьютеры POS-терминалов, внедряют свой код в процесс операционной системы, в контексте которого осуществляется проведение этого платежа. Такой процесс содержит данные магнитной полосы или чипа карты, когда она, в свою очередь, проводится через терминал. После того как код вредоносной программы оказался внедренным в такой процесс, он получает доступ к данным магнитной полосы и др. данным, например, PIN-коду, который клиент вводит на терминале. Затем данные записываются в файл и отправляются на сервер злоумышленникам.

Компрометация компании, которая обслуживает клиентов через POS-терминалы, очень опасна, поскольку злоумышленники получают централизованный доступ ко всем терминалам этой компании. В случае с Target, компания поставила на уровень риска данные более ста миллионов своих клиентов. Можно констатировать, что в таком случае от держателя кредитной карты мало что зависит, поскольку вся ответственность ложится на компанию, которая обслуживает терминалы.

При проведении банковской операции через банкомат, например при снятии наличных средств или переводе средств, злоумышленники могут воспользоваться специальными приспособлениями – наподобие скиммеров и накладных клавиатур. Эти приспособления используются для получения данных с магнитной полосы карты, а также для получения PIN-кода.

В последнее время злоумышленниками стали использоваться миниатюрные тепловизионные камеры, позволяющие определять PIN-код по тепловым отпечаткам на клавиатуре без использования каких-либо дополнительных устройств.

Рис. 2. Пример накладной клавиатуры для банкомата, которая используется злоумышленниками для получения доступа к PIN.

Таким образом, держателю карты следует проявлять бдительность при использовании банкомата, прикрывать рукой клавиатуру при наборе PIN-кода, а также не использовать банкомат в местах, которые кажутся подозрительными.

Как мы видим, “золото” по безопасности получает довольно архаичный способ совершения платежей, поэтому пользователям стоит искать свою “золотую середину” – компромисс между безопасностью и удобством (рис. 2).

Остается отметить, что внимательность и бдительность держателя карты – лучшая защита при использовании любого способа проведения платежной операции. Если есть подозрение в компрометации данных карты, лучше всего обратиться в ближайшее отделение банка с просьбой ее заблокировать для выяснения подробностей.

Заключение

По нашим оценкам, на текущий момент риски проведения онлайновых банковских операций уменьшаются в следующем порядке:

- *проведение платежа через сервис онлайн-банкинга;*
- *платеж с использованием мобильного приложения (мобильное устройство);*
- *онлайн-платеж через браузер;*
- *платеж с использованием приложения банка для ПК/Mac;*
- *платеж с использованием POS-терминала;*
- *проведение операции через банкомат;*
- *посещение банковского учреждения.*

*В данном случае в качестве основного критерия использовалась “ответственность за безопасность при проведении платежной операции”. Поскольку все перечисленные способы проведения платежей по своей сути являются изначально защищенными, и каждый из них может быть по-своему скомпрометирован, то показателем выступает вероятность компрометации среды реализации этого способа (риски). Например, все четыре первых способа в бОльшей степени подпадают под зону риска, поскольку ответственность за контроль компьютера/браузера/мобильного устройства, на котором проводится платежная операция, ложится на плечи пользователя, который может и не отнестись достаточно ответственно к обеспечению своей безопасности. В то же время ответственность за использование банкоматов и POS-терминалов берет на себя обслуживающая компания с соответствующей лицензией, которая **обязуется** обеспечить соответствующий уровень защиты, и которая, по сути, должна возместить убытки своим клиентам в случае его неисполнения (в рамках действующего законодательства и судебной практики, прим. ред.).*

Артем Баранов,
компания ESET

Видеоаналитика для Сбербанка России

Январь 2014 г. – Компания «Техносерв» объявила о завершении проекта по расширению возможностей “Кредитной фабрики” Сбербанка России.

В рамках совершенствования системы предупреждения мошенничества при кредитовании физических лиц банк заказал внедрение системы выявления случаев подлога и подделки документов с использованием технологий машинного зрения. Основой данного решения стала разработка на базе собственного продукта компании “Техносерв” – “Каскад-Поиск”. Это система распознавания лиц, реализующая функции идентификации личности по фотографии или фотороботу, предназначенная для использования в оперативной, справочной и экспертной работе. Специально для Сбербанка разработчики “Техносерва” адаптировали продукт, предназначенный для работы силовых структур, под требования и бизнес-процессы банка, а команда входящей в Группу “Техносерв” компании “Рексофт” создала эргономичный интерфейс новой системы.

Решение «Каскад-Поиск» было интегрировано с централизованной автоматизированной системой рассмотрения кредитных заявок Сбербанка и, работая в режиме онлайн, использует архив фотографий заемщиков, ранее обращавшихся в банк за кредитом, для выявления мошеннических схем с использованием поддельных документов высокого качества.

В момент подачи заявки на кредит программа на основе снимка лица потенциального заемщика строит математическую модель, содержащую информацию о геометрии лица клиента (т.н. метрический шаблон), а затем сравнивает эту модель с шаблонами, занесенными в ту или иную выборку, например, выборку «стоп-лист банка» или выборку клиентов, вышедших на раннюю просрочку. Благодаря ряду инновационных решений сравнение по всем базам проходит в течение нескольких секунд (хотя каждая заявка прогоняется почти по десятку баз, некоторые из которых имеют размер, близкий к миллиону объектов).

В настоящее время система распознавания лиц уже введена в промышленную эксплуатацию и позволяет выявлять лиц, манипулирующих своими данными при подаче заявки на кредит или использующих поддельные документы. В частности, благодаря системе могут выявляться случаи использования мошенниками документов добросовестных клиентов, даже если мошенник пытается получить кредит в банке по чужим документам первый раз, когда одно и то же лицо подает документы под двумя разными фамилиями или одинаковые паспортные данные вносятся на два разных лица.