УДК 004.056.5

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА ПРОСТОРАХ МОБИЛЬНОГО ИНТЕРНЕТА

***Илья Павлович Михнев**, канд. техн. наук, доцент кафедры Информационных систем и математического моделирования,*
E-mail: mkmco@list.ru,
Волгоградский филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте РФ»,
http://vlgr.ranepa.ru

Статья анализирует основные угрозы информационной безопасности на просторах мобильного Интернета. Рассмотрены атаки на социальные сети и Man-in-the-Browser атаки. Показан самый надежный способ защиты от утечек информации через мобильные устройства и съемные носители.

Ключевые слова: информационная безопасность, мобильный Интернет, защита информации, информационные ресурсы

Введение


И.П. Михнев

В настоящее время во всем мире резко повысилось внимание к проблеме информационной безопасности на просторах мобильного Интернета. Это обусловлено процессами стремительного расширения потоков информации, пронизывающих все сферы жизни общества. Информация давно перестала быть просто необходимым для производства вспомогательным ресурсом или побочным проявлением всякого рода деятельности. Она приобрела ощутимый стоимостной вес, который четко определяется реальной прибылью, получаемой при ее использовании, или размерами ущерба, с разной степенью вероятности наносимого владельцу информации. Однако создание индустрии переработки информации порождает целый ряд сложных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса информации, циркулирующей и обрабатываемой в информационно-вычислительных системах и сетях [1].

Сегодня мобильный Интернет приобретает все большую популярность и по своей распространенности скоро догонит традиционный проводной аналог. Растут скорости передачи данных, развиваются связные технологии, и любой современный гаджет использует возможности мобильного соединения в полном объеме. Мобильный Интернет – отличный помощник делового человека в поездках и командировках. Смартфон всегда путешествует вместе со своим владельцем и оперативное решение таких задач, как работа с электронной почтой, создание и редактирование документов, а также веб-серфинг с помощью мобильного устройства, уже давно не являются чем-то особенным.

Однако возможность беспроводного доступа ко Всемирной паутине практически из любой точки земного шара таит в себе ряд специфичных опасностей. Вредоносные программы, которые благополучно фильтруются антивирусами на компьютерах, на просторах мобильного Интернета в полной мере проявляют себя, угрожая безопасности вашего устройства. Не стоит забывать и про то, что баланс лицевого счета абонента представляет большой интерес для недобросовестных контент-провайдеров и различного рода мошенников.

Основные угрозы на просторах мобильного Интернета

Эксперты сходятся во мнении, что основные угрозы в сфере мобильного мошенничества в 2015–2016 гг. будут связаны с мобильным банкингом. Мобильные платформы не отличаются столь же высокой степенью защиты, как интернет-сайты или банко-

маты, и поэтому более уязвимы для мошенников [2]. Злоумышленники будут всеми способами пытаться проникнуть в браузер и мобильные приложения пользователя и завладеть его персональными данными с целью получить контроль над счетом. В недалеком будущем следует ожидать повышенного интереса мошенников к p2p-платежам, которые, по мнению специалистов, скоро должны стать популярными в нашей стране.

В погоне за персональными данными владельцев смартфонов преступники часто прибегают к методам социального инжиниринга – управления действиями пользователя без помощи технических средств, манипулируя исключительно человеческими слабостями. Так, известна мошенническая схема, которую условно можно назвать «звонок от сотрудника техподдержки». Звонящий представляется сотрудником техподдержки сотового оператора и сообщает о необходимости перепрограммирования телефона на новые параметры в связи с проведением технических работ. Владельца аппарата просят ввести комбинацию букв и цифр, после чего с его счета снимаются средства.

Попасться на удочку мошенников можно при посещении определенных ресурсов. Так, во время веб-серфинга часто можно встретить предложения «обновления» программного обеспечения. Такие оповещения можно получить, например, при переадресации с других, безопасных сайтов. После взаимодействия с таким информационным баннером происходит загрузка вредоносной программы, которая автоматически рассылает SMS-сообщения на платные короткие номера. С проблемой автоматической рассылки SMS-сообщений также сталкиваются пользователи, которые устанавливают программное обеспечение с многочисленных сайтов, предлагающих взломанные версии платных программ.

Существует и такая схема: на устройство приходит извещение о том, что для данного номера пришло MMS-сообщение. При переходе по ссылке, указанной в информационном письме, происходит загрузка вредоносной программы с последующей рассылкой SMS-сообщений на платные номера. В последнее время для автоматической загрузки вредоносного ПО достаточно просто открыть такое сообщение, особенно если у вас подключена опция автоматического перехода по полученным ссылкам.

Особую бдительность следует проявлять, пользуясь платными сервисами, которые предоставляют различные интернет-ресурсы. Порой на них бывает указана неверная информация, занижена стоимость предлагаемого контента. Рассчитывая скачать содержимое за написанную крупным шрифтом сумму, можно не обратить внимание на едва различимое примечание внизу, что цена указана на одни сутки. При этом вы оплачиваете подписку сразу на несколько месяцев. Также на сайте может быть не обозначено количество SMS-сообщений, которое необходимо отправить для совершения покупки. Особое внимание следует уделить вирусам, которые попадают в смартфоны через MMS, Интернет и установленные приложения. После заражения устройство начинает самостоятельно отправлять SMS-сообщения на платные короткие номера мошенников. Рассылка SMS или MMS без ведома пользователя может производиться Java-приложениями, в результате чего под угрозой оказываются и номера из списка контактов жертвы, на которые также отправляются сообщения для дальнейшей передачи вируса. Индикаторами того, что вы стали жертвой вредоносной программы может стать непривычно быстро разряжающийся аккумулятор и пропажа средств с лицевого счета. Получить вредоносное Java-приложение на своем аппарате можно также при скачивании и установке зараженных вирусом игр.

Но лишиться средств можно не только по вине мошенников, но и из-за своей собственной халатности, например, в результате неправильной настройки мультимедийного устройства. Любой гаджет, будь то смартфон или ноутбук, с каждым годом увеличивает собственное потребление интернет-трафика. Для мобильного устройства это могут быть различные процессы синхронизации, загрузка карт и другой соответствующей информации (например, сведений о пробках, дорожных происшествиях) при использовании навигатора. В настройках такого устройства по умолчанию включены многие

опции, связанные с функциями обмена данными. При работе с ноутбуком интернет-соединение используется для автоматической загрузки различного рода обновлений: как самой ОС, так и установленного программного обеспечения.

Работа аппарата с настройками по умолчанию, без ограничения по расходу интернет – трафика, в домашнем регионе пользователя может быть приемлема как для него, так и для состояния его абонентского счета. Это объясняется низкими ценами на трафик и наличием льготных пакетов различного плана. В роуминге, когда цена за 1 Мб мобильного Интернета резко возрастает, ситуация приобретает иной характер. И любое регулярное обновление, постоянная подгрузка информации, а также другие привычные для абонента действия могут пагубно сказаться на балансе его счета.

Несмотря на предупреждения о дороговизне использования мобильного интернета в поездках, а также большом количестве историй с нашими соотечественниками, которые, закачав несколько серий любимого сериала, оказались должны несколько миллионов рублей операторам связи, такие случаи все еще имеют место. К счастью, в 2015 г. ситуация с ценами на мобильный Интернет в роуминге сильно отличается от той, которая была на рынке услуг сотовой связи несколько лет назад. Сегодня операторы большой тройки предлагают специальные пакеты трафика и тарифы для поездок и путешествий, которые предназначены для оптимизации затрат на мобильную связь и Интернет вне домашней зоны. Тем не менее, покупка местной сим-карты в некоторых случаях оправдана до сих пор [3].

При установке любых приложений на свой смартфон рекомендуется очень внимательно читать пользовательские соглашения, а также смотреть список опций, и процессов, которые программа запрашивает при инсталляции. Не будет лишним и чтение комментариев к загружаемым приложениям, так как порой информация, содержащаяся в отзывах других потребителей, может помочь избежать неблагоприятных последствий установки. Тем же, кто получает приложения только из официального магазина Google Play Market, рекомендуется отключить в опциях своего смартфона возможность установки приложений из ненадежных источников.

Если говорить о Google Play, то, в отличие от Apple Store, данный официальный репозиторий приложений для операционной системы Android до недавнего времени содержал в себе большое количество вирусных и других программ, способных нанести ущерб устройствам. Позже модерация была усилена, а загружаемый софт отныне проверяется антивирусом. Благодаря этим мерам удалось удалить большое количество вредоносного ПО и программ-подделок. Бороться с такими программами, помимо отключения вышесказанных опций в настройках смартфона, помогают также средства антивирусной защиты.

Еще одна проблема, с которой могут столкнуться владельцы смартфонов, ноутбуков и планшетов, – неумышленная покупка того или иного приложения. Вероятность такой ситуации довольно высока, учитывая богатый выбор программ, представленных в Google Play Market и Apple Store. В этом случае предусмотрена процедура возврата потраченных денежных средств. Временной интервал, за который можно отказаться от покупки, составляет 24 часа для App Store и 15 минут для Google Play.

Атаки на социальные сети

Социальные сети – идеальная площадка для распространения троянов и прочих вредоносных программ. Аккаунт в Twitter, Facebook and LinkedIn с миллионом подписчиков представляется лакомым куском для мошенников, поскольку, завладев им, можно разослать вирус большому числу пользователей. Последние, доверяя источнику, скорее всего, кликнут на злополучную ссылку или откроют файл.

Социальные сети облегчают проведение так называемых drive-by атак, при которых компьютер пользователя заражается при простом посещении сайта, содержащего вредоносный код [4]. Если ссылку на этот ресурс распространить в социальной сети,

последствия будут катастрофическими. Так, в 2010 г. сотни тысяч пользователей стали жертвами Trojan Carberp после посещения одного нидерландского новостного сайта [5].

Аналогичную угрозу таит в себе активное использование поисковиков. «Представьте себе, что огромное число людей ищет в Google информацию об одном и том же событии, а злоумышленники находят лучшие фотографии, иллюстрирующие его, и заражают их вирусом. При просмотре картинок компьютеры пользователей инфицируются». Лучшей защитой в подобных ситуациях является информирование пользователей. Победить преступность только при помощи технологий невозможно – эта мысль является ключевой в индустрии безопасности последних лет. Но и пренебрегать своевременным обновлением антивирусных программ и патчей не стоит: службы безопасности организаций должны зорко следить за тем, чтобы и сотрудники предприятия, и клиенты не забывали обновлять свои системы и соблюдать основные правила безопасного пользования.

Атаки Man-in-the-Browser

Man-in-the-Browser – атака, при которой вредоносное ПО внедряется в клиентский интернет-браузер и при старте перевода денежных средств за считанные секунды изменяет параметры транзакции так, как угодно мошеннику. Обнаружить этот процесс крайне сложно [6]. «Злоумышленники могут разработать вирус для атаки на одну конкретную организацию. Такие атаки совершаются не каждый день, но когда это происходит, они имеют успех». Существует два способа предотвращения подобных нападений – контроль процесса аутентификации на сервере и мониторинг транзакционных аномалий [7]. Если «клиент» утверждает, что он в США и пытается получить доступ к американскому счету, однако устройство, с которого совершаются попытки войти в аккаунт, находится в другой стране, это свидетельствует о высоком риске мошенничества.

Использование личных устройств в служебных целях

В последнее время все большее число сотрудников компаний прибегают в процессе работы к личной технике, имеющей доступ к корпоративным базам данных, и это открывает широкие возможности для мошенничества [8]. В связи с этим организациям следует ограничивать доступ к ценной информации с личных устройств. Для этого потребуется иметь в своем распоряжении системы обнаружения мошенничества, чтобы определять, когда доступ к серверам совершается удаленно и отслеживать действия, которые теоретически могут способствовать преступной деятельности.

«Борьба со злоумышленниками должна быть результатом сотрудничества разных подразделений предприятия. Плохая защита – лучший стимул для хорошего нападения. К сожалению, многие организации еще не пришли к пониманию этой истины» [9].

В эпоху высоких технологий информация стала дороже золота, а потому конфиденциальные данные воруют все чаще и больше. И это серьезная проблема, ведь потерявшая свои коммерческие секреты компания может попросту закрыться. Особенно если это средний или малый бизнес, существующий в высококонкурентной среде [10].

Заключение

Автор считает, что самый надежный способ защиты от утечек через мобильные устройства и съемные носители – это шифрование. Найти инструменты, реализующие шифрование, нетрудно. Гораздо сложнее выбрать среди них наиболее эффективный. Главный принцип защиты информации заключается в том, что затраты на нее не должны превышать ущерба, который может нанести потеря или кража этой информации.

Поэтому для защиты данных оптимально использовать систему, которая, как минимум, не потребует сложного внедрения и штата специалистов для поддержки, а в идеале будет обладать более широкой функциональностью, чем просто шифрование данных на мобильных устройствах и флеш-накопителях.

Современная система шифрования должна защищать данные не только на съемных носителях (включая, но не ограничиваясь флешками), но и в облачных хранили-

щах, файлы и папки на локальных и сетевых ресурсах.

Удобнее, если шифрование будет осуществляться в прозрачном режиме, то есть незаметно для пользователей. При этом администратор системы должен иметь возможность указать типы данных и сценарии, для которых информация будет шифроваться принудительно либо по инициативе пользователя.

Чем более гибкое и многоуровневое разделение прав доступа к зашифрованной информации предоставляет система, тем она эффективнее и удобнее в использовании. Администратор должен иметь возможность настраивать самые различные правила, начиная с отдельного сотрудника или отдела и заканчивая всей компанией. Ну и, конечно, необходимо иметь возможность расшифровывать файлы на сторонних компьютерах с помощью пароля. Если система защиты корпоративных данных удовлетворяет перечисленным выше требованиям, то перед вами действительно надежный инструмент, который сможет защитить ваш бизнес от утечек информации.

Литература

1. Основы информационной безопасности хозяйственной деятельности: учебное пособие / *И.П. Михнев*; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. 144 с.

2. *Сальникова Н.А., Астафурова О.А.* Автоматизация поискового конструирования сложных СВЧ-устройств // Известия Волгоградского государственного технического университета. 2013. Т. 17. № 14 (117). С. 122–126.

3. *Астафурова О.А., Сальникова Н.А., Кулагина И.И.* Интеграция научных разработок в обучении бакалавров экономического профиля // Известия Волгоградского государственного технического университета. 2014. Т. 11. № 14 (141). С. 12–14.

4. *Михнев И.П.* Мультимедийные технологии в образовательном процессе // Современные наукоёмкие технологии. № 2/2004. С. 109–112.

5. *Михнев И.П.* Обучение и контроль знаний студентов с помощью UniTest // Фундаментальные исследования. № 1/2008. С. 94–95.

6. *Мединцева И.П.* Организационные аспекты использования информационных технологий в высшей школе // Известия Волгоградского государственного технического университета. 2007. Т. 4. № 7(33). С. 171–173.

7. *Лопухов Н.В., Сальникова Н.А.* Логистический паспорт региона // Известия Волгоградского государственного технического университета. 2014. Т. 11. № 14. С. 82–84.

8. Правовое регулирование и кадровая обеспеченность органов местного самоуправления: исторический аспект и современные основы: учебное пособие / Н.В. Сорокина, С.В. Михнева. Волгоград: Изд-во: ООО «Волгоградское научное издательство», 2013. 211 с.

9. *Михнев И.П.* Информационная безопасность в современном экономическом образовании // Международный журнал прикладных и фундаментальных исследований. № 4/2013. С. 111–113.

10. *Сальникова Н.А., Михнев И.П.* Проведение аттестации знаний студентов с помощью компьютерного тестирования // Известия Волгоградского государственного технического университета. 2007. Т. 4. № 7(33). С. 182–185.

Information security in the vast mobile Internet

***Ilya Pavlovich Mikhnev**, Ph.D., Associate Professor of Information Systems and Mathematical Modelling, Volgograd branch of the Russian Presidential Academy of National Economy and Public Administration, Russia, http://vlgr.ranepa.ru*

The article analyzes the main threats to information security in the vast mobile Internet. Considered an attack on the social network and Man-in-the-Browser attacks. It shows the most reliable way to protect against leaks via mobile devices and removable media.

Keywords: information security, mobile Internet, data protection, information resources