АЙЖАНОВ С. А., ПРЕПОДАВАТЕЛЬ КАФЕДРЫ УПРАВЛЕНИЯ ОВД КАРАГАНДИНСКОЙ АКАДЕМИИ МВД РК ИМ. Б. БЕЙСЕНОВА

МОШЕННИЧЕСКИЕ СХЕМЫ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ

Сетевые мошенники изобретают все новые способы обмана интернет-пользователей в Казахстане. В качестве одной из наиболее популярных площадок для реализации своих планов злоумышленники избрали социальные сети «В контакте», «Мой мир», «Одноклассники»[1]. Подобный выбор не случаен, поскольку именно на сайтах социальных сетей присутствует наибольшее число посетителей, плохо разбирающихся в компьютерных технологиях и пренебрегающих простыми правилами информационной безопасности. Именно они и становятся легкой «добычей» сетевых мошенников.

Рассмотрим некоторые мошеннические схемы для пользователей популярных социальных сетей.

Одним из способов интернет-мошенничества являются рекламные картинки и документы. Данная схема весьма проста и широко распространена. Первоначально владелец учетной записи социальной сети «В контакте» получает сообщение от одного из пользователей, зарегистрированных в его списке друзей. Такое послание обычно не вызывает подозрений, поскольку люди привыкли относиться с некоторой степенью доверия к информации, получаемой от своих знакомых. На момент отсылки такого послания учетная запись отправителя уже взломана, а его логин и пароль находятся в руках злоумышленников. Сообщение, как правило, содержит ссылку на графический файл, предлагающий посетить сайт злоумышленников для установки какого-либо приложения. Тонкость заключается в том, что рекламирующее мошеннический (фишинговый[2]) сайт изображение хранится на одном из серверов внутренней системы файлового обмена и потому при переходе по ссылке пользователю не демонстрируется сообщение о том, что он покидает сайт социальной сети. Это еще сильнее притупляет его бдительность — ведь на экране появляется объявление, подписанное якобы администрацией сайта. Стоит пользователю перейти на рекламируемый сайт, оформление которого копирует интерфейс данной социальной сети, и ввести свои учетные данные в форму авторизации, как они тут же попадают в руки злоумышленников, и от его имени по списку друзей начинается отправка сообщений, содержащих фишинговые ссылки.

Разновидностью подобного рода мошенничества является использование функции «Документы». Ничего не подозревающему пользователю отсылается личное сообщение, включающее ссылку на скачивание документа Word, в котором содержится подробная инструкция по установке специальной программы, якобы позволяющей просматривать число посетителей его странички в социальной сети. Под видом этой программы распространяется вредоносное программное обеспечение.

К другой категории потенциальных жертв сетевых мошенников можно отнести поклонников компьютерных игр. Из числа игроков мошенники вычисляют наиболее опытных, «продвинутых», им отсылается личное сообщение с предложением воспользоваться «уязвимостью» данного приложения, позволяющей бесплатно получить игровые предметы, которые в реальной игре можно приобрести только за деньги. Если игрок соглашается, все дальнейшее общение сетевые мошенники переносят в Skype. Выбор данного средства коммуникации не случаен: трафик Skype не поддается фильтрации в

отличие от других протоколов мгновенного обмена сообщениями, таких как ICQ. В ходе дальнейшего общения злоумышленники предлагают жертве скачать и установить приложение, под видом которого распространяется троянская программа, предназначенная для перехвата нажатий клавиш и отправки на удаленный FTP-сервер украденных таким образом паролей. При попытке открыть данный файл происходит мгновенное заражение компьютера.

Еще один способ сетевых мошенников заставить потенциальную жертву выполнить необходимые действия — заинтриговать ее, заинтересовать неожиданным результатом. Как и в других случаях, процесс вовлечения пользователя социальной сети в мошенническую схему начинается с того, что он получает содержащее ссылку сообщение от одного из людей, занесенных в его список друзей. Щелкнув «мышью» по этой ссылке, пользователь перенаправляется на специализированный сервис, предназначенный для сокращения гиперссылок, а уже оттуда — на встроенное приложение, опубликованное на одной из страниц социальной сети. В процессе подобной переадресации пользователь не получает никаких предупреждений. Созданное злоумышленниками приложение демонстрирует значок учетной записи жертвы и пояснение, сообщающее, что в Интернете опубликован видеоролик с его участием. Интересная особенность данной мошеннической схемы заключается в том, что на этой же странице выводятся комментарии пользователей из списка друзей жертвы. Комментарии, естественно, генерируются программой автоматически на основе заданного злоумышленниками шаблона. Там же публикуется ссылка на сам «ролик» — она состоит из имени жертвы и расширения «avi».

По щелчку «мышью» на предложенной злоумышленниками ссылке происходит перенаправление пользователя на принадлежащий мошенникам сайт, при этом на экране появляется диалоговое окно с предложением указать логин и пароль учетной записи. Если жертва выполняет данное требование, эта информация передается злоумышленникам.

В следующей мошеннической схеме также используется то обстоятельство, что пользователи относятся с большей степенью доверия к информации, поступающей от своих знакомых. Злоумышленники отсылают потенциальной жертве сообщение от одного из друзей с просьбой проголосовать за него на каком-либо сайте. Учетная запись отправителя послания к этому моменту уже является взломанной, а проводящий голосование сайт принадлежит злоумышленникам.

По указанной ссылке открывается интернет-ресурс, действительно предлагающий «проголосовать» за выбранного кандидата, щелкнув мышью на его фотографии. Однако для того чтобы отдать свой голос, необходимо войти на сайт. Формы регистрации и авторизации на сайте отсутствуют, но посетитель может выполнить «вход» с использованием специальной системы «интеграции» с социальными сетями Twitter, Facebook, «Мой мир», «Одноклассники», «В контакте».

Естественно, эта «система интеграции» — поддельная: достаточно указать в соответствующей форме свои логин и пароль, и они будут незамедлительно переданы злоумышленникам.

В последнее время появился новый способ мошенничества, основанный на том, что на главном меню сайта появляется новый пункт. По щелчку «мыши» на этом пункте меню открывается диалоговое окно, в котором пользователю предлагается указать свой номер мобильного телефона. На указанный номер спустя несколько секунд приходит СМС-сообщение с предложением отправить СМС, содержащее демонстрируемый на экране компьютера код. Затем жертва мошенников получает еще одно СМС с вопросом «Выслать пароль?», на которое предполагается ответ «Да», потом поступает третье по счету сообщение, содержащее запрос «Вы принимаете условия сайта?» (еще раз «Да»), и, наконец, жертва получает код, который следует ввести в демонстрируемую на экране форму. Выполнив все эти манипуляции, пользователь соглашается с условиями платной подписки, согласно которым с его счета регулярно будет сниматься определенная денежная сумма за информацию, которая должна быть, по мнению пользователя, в указанном новом пункте главного меню.

Украденные злоумышленниками логины и пароли (аккаунты) могут использоваться злоумышленниками для подписки пользователей на различные тематические группы рекламного содержания, для голосований и, естественно, для дальнейшего распространения ссылок на мошеннические сайты. Похищенные учетные записи в социальных сетях нередко используются в качестве объекта купли-продажи на всевозможных форумах. Кроме того, взлом пользовательских страниц в социальных сетях может ставить своей целью похищение средств со счетов жертвы путем отправки СМС либо подключения его к платным подпискам или распространение вредоносных программ.

Во избежание несанкционированного доступа к страницам в социальных сетях, в том числе и к содержимому электронной почты, а также для предотвращения возможных последствий, связанных с действиями мошенников, необходимо предпринимать следующие меры:

не принимать предложение дружбы от незнакомых людей;

не открывать подозрительные ссылки, полученные в сообщениях даже от друзей и знакомых;

никогда не устанавливать на свой компьютер программы, которые присылают в сообщениях;

не устанавливать и не запускать игры и приложения, рекламируемые в спам-рассылках;

никогда и ни при каких обстоятельствах не вводить логин и пароль от своей учетной записи в «Моем мире», «Одноклассниках», «В контакте» на подозрительных сайтах;

не использовать слишком простой пароль и один и тот же логин и пароль для различных сайтов;

не оставлять на странице слишком подробную информацию о себе;

поменять пароли в социальных сетях и электронной почте, а также проверить компьютер на наличие вирусов, если выяснится, что страница пользователя взломана;

использовать современное антивирусное программное обеспечение.

[1] http://ru.wikipedia.org/wiki

[2] http://ru.wikipedia.org/wiki