УДК:004.08

СКИММЕР

Савушкина А.И., Госуниверситет-УНПК, 11-ИБ

Скиммер – устройство для перехвата информации с магнитной ленты пластиковых карт – таково его официальное определение.

Скиммеры появились примерно в 2002 году в Европе (первое упоминание о них поступило из Англии). Наверняка они существовали и раньше, ибо не имеют какой-то слишком уж сложной конструкции, а банкоматы на улицах европейских городов установлены уже достаточно давно. Но, в любом случае, ранее они не имели массового распространения и нигде не фигурировали. По-настоящему заговорили о скиммерах после того, как в Москве в 2004 году была задержана группа людей "занимающихся незаконным перехватом информации с пластиковых карт". Между прочим, это был первый публичный случай задержания мошенников, и здесь мы опередили Европу. Именно после этого появилось такое понятие как скимминг. Одна из очевидных причин оживления скимминга в России – увеличение объема денежных средств, которые проходят через банковские карты. В настоящий момент он увеличился в несколько раз, поэтому мошенничество в данном секторе остается делом сверхприбыльным.

Современный скиммер состоит из двух частей. Первая – это накладной симулятор приёмника карты в банкомате, предназначенный для считывания информации с магнитной полоски карточки. Устройство содержит считыватель, маленькую микросхему преобразователя информации, контроллер и накопитель. Такие устройства легко выявить в случае, если человек постоянно пользуется одним и тем же банкоматом. Кстати, именно для этого на табло банкомата после ввода карты часто появляется предложение сравнить вид банкомата с картинкой на экране. Поэтому более современные и дорогие устройства усовершенствовали так, что их практически не видно. Считыватель очень маленький – ширина его головки

равна ширине магнитной ленты карты, толщина – 2-2,5 мм. То есть, даже сравнивая, клиент не заметит никакой разницы – скиммер, по сути, находится внутри разъёма. Они накапливают информацию о картах внутри, или с помощью передатчика по беспроводным каналам (чаще всего это Bluetooth или SMS-сообщение) сразу передают её на мобильник или устройство, спрятанное в нескольких метрах от банкомата. Кардер ничем не рискует, потому что не находится рядом с банкоматом. Он крутится поблизости, или время от времени появляется на "точке", чтобы заменить наполненный информацией скиммер.

Вторая часть скиммера – накладная клавиатура, предназначенная для "съёма" информации о PIN-коде карты. Это те же микросхемы, что и на разъёмах для ввода карты, только спрятанные в клавиатуре. Плюс разобранный мобильный телефон, настроенный на постоянную отправку SMS. Поскольку клавиатура банкомата металлическая, то и накладную приходится изготавливать из такого же материала, но она, как правило, на 0,5-1 см выделяется на общей плоскости банкомата, и потому легко обнаруживается. Иногда, чтобы у клиента не возникало подозрений, клавиатуру накладывают на всю рабочую область терминала. Никаких выпуклостей и никаких подозрений. SMS отсылается после нажатия клавиши Enter на клавиатуре. Но есть люди, которые нажимают Enter не на клавиатуре.В этом случае PIN-код не отсылается. Впрочем, можно настроить скиммер на отсылку сообщения после нажатия четвертой цифры PIN-кода. Также есть скиммеры, отсылающие SMS при нажатии любой клавиши.

После получения указанной выше информации мошенники, как правило, записывают её на так называемый "белый пластик" – то есть пластиковую карточку с магнитной полоской, не имеющую каких-либо логотипов и оформления, и с её помощью получают наличные в другом банкомате. Но может изготавливаться и полноценная пластиковая карта, пригодная для оплаты покупок в обычных магазинах. Иногда это безопаснее,

так как в случае с банкоматом преступнику приходится сильно менять внешность, которую обязательно зафиксирует камера банкомата.

Банки совершенствуют оборудование, и заботятся о нашей безопасности. Появились банкоматы со специальной защитой от скиммеров – они сначала втягивают карту в приемное устройство, затем частично выталкивают её наружу, и уже затем окончательно поглощают в своем нутре. Такая процедура сбивает последовательность считывания информации скиммером и делает её непригодной для дальнейшего использования. Старайтесь выбрать такой банкомат, хотя и он не панацея – некоторые скиммеры настроены на считывание информации при извлечении карты из банкомата. Желательно выбрать банкомат рядом с банком, осмотреться в поисках наружных камер – чем их больше, тем лучше. Обязательно внимательно осмотреть банкомат, при обнаружении чего-либо подозрительного отказаться от его использования. Лучше всего пользоваться банкоматами с 9:00 до 11:00 – это время, когда их проверяют полицейские и контролируют и обслуживают сотрудники банков. И этот отрезок времени признан кардерами самым опасным и нерекомендуемым к установке скиммеров. Если поблизости с банкоматом крутятся какие-либо люди с телефонами – стоит отказаться от использования банкоматов. Почаще проверяйте баланс, и если начали исчезать какие-либо суммы, даже очень маленькие – звоните в банк. Во многих странах некоторые уличные телефоны-автоматы принимают пластиковые карты. Вставляешь, звонишь, а деньги списываются со счета. И этот способ признан кардерами одним из самых надежных и безопасных для проверки "валидности" карт. Ущерб от кардинга в России лишь за 2011 год Group-IB оценивает почти в $400 млн, при общем объеме рынка киберпреступности в России в $1,8 млрд за 2011 год и $2,5 млрд за 2010 год. В США, кстати, по данным Секретной службы (USSS), за 2008 год потери от мошенничества с банкоматами составили около $1 млрд (примерно $350 тысяч в сутки).

Цена скиммера зависит от производителя и исполнения. Готовый (заводской) скиммер обойдется минимум в $250, но прибрести его можно только имея связи с мастерами. «Чем ближе продавец к производителю и заводским технологиям, тем ниже выставляемая цена. Посредники уже продают от $1 тыс. Для изготовления накладной части нужен либо рабочий с завода, либо специалист по лазерной резке металла. Сложно подозревать, что такие делают производители самих банкоматов – наверняка там серьезные проверки и учет, однако, судя по исполнению скиммеров, – это отнюдь не кустарного характера работа», - рассуждает электронщик. Изготовление металлического корпуса скиммера - самая сложная работа, электронную «начинку» под силу собрать даже самому обычному электронщику. «Все компоненты абсолютно легальны – их можно купить на радиорынке. В итоге самый простой скиммер обойдется в $20. Главное - подобрать соответствующий разъему банкомата считыватель и контроллер, соответствующий ширине магнитной ленты на карте. Именно контроллер понимает код, ведь на ленте он защищен несложным алгоритмом», - поясняет специалист. Скиммеры становятся все совершеннее с технологической точки зрения, и, чем они совершеннее, тем труднее их обнаружить.

Список литературы:

1.Group-IB [Электронный ресурс]: (с изм. и доп.)- Режим доступа: http://www.group-ib.ru/?view=article&id=387 (дата обращения 15.11.12)

2.Компьютерра ONLINE [Электронный ресурс]: (с изм. и доп.)- Режим доступа: http://www.computerra.ru/431076/ (дата обращения 16.11.12)

3.Центр исследования компьютерной преступности [Электронный ресурс]: (с изм. и доп.)- Режим доступа: http://www.crime-research.ru/news/11.03.2008/4337/ (дата обращения 16.11.12)