Логическая безопасность ДБО: прошлое, настоящее, будущее

Денис Гасилин
Руководитель отдела маркетинга компания SafenSoft

Дистанционное банковское обслуживание выгодно всем участникам кредитно-финансового рынка. Клиенты финансовых учреждений год за годом обретают все больше возможностей управлять своими счетами, а организации снижают издержки на содержание офисов и получают возможность предлагать клиентам дополнительные услуги. Но от такого взрывного роста выигрывают не только банки и пользователи услуг, но и третья сторона — кибермошенники. Традиционные средства обеспечения безопасности не поспевают за рынком, благодаря чему ущерб от мошенничества в системах ДБО нашей страны уже составляет около 100 млн долл. в год, и к 2015 г. объем потерь может достичь 171 млн долл.

ДБО можно условно разделить на три вида.

Устройства самообслуживания (банкоматы, POS-терминалы и киоски) уже давно и прочно вошли в нашу жизнь. Увеличение числа сервисов, предлагаемых клиентам через банкомат, ведет к увеличению «площади атаки» для потенциальных злоумышленников. Атаки на банкоматы и сети банкоматов принимают самые различные формы, от грубых нападений с целью выведения системы из строя, как в мартовской атаке на южнокорейский банк, до скрытого внедрения вредоносного кода в сами устройства. Согласно отчету экспертов ATMIA за 2012 г., логические угрозы для банкоматов уже вышли на третье место среди основных угроз, и только использование новых технологий в области защиты информации способно остановить или хотя бы замедлить эту тревожную тенденцию — традиционные подходы, требующие широкополосного доступа в Интернет и существенных ресурсов, не работают в условиях ограниченной программной среды банкомата.

Мобильный банкинг, выступающий в основном в виде приложений для таких мобильных устройств, как планшеты и смартфоны, — самое новое направление в триаде средств ДБО. Согласно исследованию Digital Security, проведенному для банковских приложений для iOS и Android 37 самых популярных банков страны, все приложения мобильного банкинга в России содержат хотя бы одну уязвимость. Особенную опасность представляет концепция, подразумевающая интеграцию банковских услуг с «лишними» сервисами наподобие социальных сетей. Стоит отметить, что специфика распространения приложений для Android такова, что вредоносные программы зачастую распространяются через официальный интернет-магазин Android Market. Так, по данным на декабрь 2011 г. около 30% всех вирусов для Android распространялось именно по этому каналу. Появление в последнее время на рынке мобильных устройств, работающих под ОС Windows 8, ведет к тому, что гаджеты обретают все больше уязвимостей, а ресурсы их аппаратной части используются под завязку.

Третий вид ДБО — привычный и существующий уже достаточно долгое время *Интернет-банкинг*. В последнее время данный вид ДБО в большинстве своем используется юридическими лицами с рабочих станций внутри организации, уступая частных лиц и их расчеты мобильному банкингу. Так как операции проводятся на обычных компьютерах, весь спектр традиционных угроз актуален для компаний, пользующейся данной услугой. Самым известной в нашей стране вредоносной программой в этой области является троянец Carberp, постоянно модернизируемый своими создателями — последняя модификация была обнаружена в марте 2013 г.

Первая волна распространения каждой новой вредоносной программы или модификации старой, расходящаяся по атакованным организациям до момента обновления вирусных баз, каждый раз заставляет констатировать, что обычные системы защиты, основанные на принципе действия «черных списков», не обладают достаточными возможностями для отражения атак на данный вид ДБО. Киберпреступники постоянно совершенствуют свой инструментарий, и единственным выходом из ситуации может быть только защита, основанная на проактивных технологиях и принципе «белых списков», предотвращающая несанкционированные изменения в системе вне зависимости от наличия или отсутствия исполняемого кода в вирусных базах.