

ПОД ПРИЦЕЛОМ ХАКЕРА

В последние годы интернет-банкинг становится распространенной услугой не только среди компаний, но и среди частных клиентов. Удобство пользования этой системой неоспоримо, однако, к сожалению, это понимают и мошенники. Кражи хакерами средств с банковских счетов в настоящее время участились, отмечают участники рынка.

ВЕРОНИКА МАСЛОВА

В прошлом году, например, хакеры получили доступ к банковскому счету французского президента Николя Саркози. Как писали СМИ, недоброжелатели каким-то образом стали обладателями логина и пароля для управления счетом президента через интернет и несколько раз снимали с него небольшие суммы. Недостачу заметил сам Саркози, после чего сообщил об этом полиции. Между тем сообщения о похищении средств с банковских счетов — не редкость. По статистике, которую приводит Украинский банковский портал (banker.ua), при обороте операций в \$2 млрд кражи путем взлома пользовательских компьютеров через глобальную сеть составляют порядка 0,1%. А это — ни много ни мало — \$20 млн. Недавно в Нью-Йорке была раскрыта одна из самых крупных хакерских атак в истории. Получив доступ к внутренней информации, электронной почте и данным о кредитных картах, преступники за два последних года смогли проникнуть в системы более 2,5 тыс. компаний из США и еще 195 стран.

Растущая активность интернет-мошенников вызывает беспокойство и российских регуляторов. В июне прошлого года Центробанк разослал банкам письмо, в котором сообщал о появлении в российском сегменте интернета веб-сайтов, имитирующих интернет-представительства ряда российских кредитных организаций. Доменные имена и стиль оформления таких сайтов, как правило, сходны с именами подлинных веб-сайтов банков, а содержание прямо указывает на их якобы принадлежность соответствующим кредитным организациям, говорилось в сообщении ЦБ. При этом посетителям таких сайтов сообщаются заведомо ложные банковские реквизиты и контактная информация. «Использование подобных реквизитов, а также вступление в какие-либо деловые отношения с лицами, фактически представляющими ложные банки, связано с риском и может привести к нежелательным последствиям для клиентов кредитных организаций», — говорилось в письме. В связи с этим ЦБ рекомендовал банкам подготовить и распространить среди клиентов памятку, содержащую исчерпывающую контактную информацию, рекомендации по безопасному использованию банковских интернет-технологий, а также предложения клиентам информировать кредитную организацию о самостоятельно выявленных ложных веб-сайтах банка или о полученных сведениях подобного рода по электронной почте или иным способом.

МОШЕННИКИ АКТИВИЗИРУЮТСЯ

Как говорят сами участники рынка, в последнее время они фиксируют значительное увеличение количества атак на компьютеры клиентов систем интернет-банкинга с целью хищения денежных средств клиентов. По словам директора по информационным технологиям банка



ПРИ ОБОРОТЕ ОПЕРАЦИЙ В \$2 МЛРД КРАЖИ ПУТЕМ ВЗЛОМА ПОЛЬЗОВАТЕЛЬСКИХ КОМПЬЮТЕРОВ ЧЕРЕЗ ГЛОБАЛЬНУЮ СЕТЬ СОСТАВЛЯЮТ ПОРЯДКА 0,1%

«Санкт-Петербург» Ярослава Шелина, вирусные технологии усложняются на фоне относительной стабилизации количества нового вредоносного программного обеспечения, так что глобальные эпидемии, а также появление новых схем интернет-мошенничества участились. «Программы, оснащенные руткит-функционалом (функционал программы, которая сама по себе не является вирусом, но подготавливает систему для проникновения троянской программы. — „b“) не только получили широкое распространение, но и значительно продвинулись в своей эволюции. В связи с этим можно утверждать, что угроза хакерских атак в последнее время существенно возросла», — говорит господин Шелин.

Конечно, наибольший интерес для мошенников представляют счета юридических лиц, так как обычно находящиеся на них суммы значительно превышают суммы на счетах частных банковских клиентов. К тому же ответственность за сохранность денег в компаниях «размыта» по широкому кругу лиц — что-то сисадмин не доделал, что-то бухгалтер не знал, директор не заметил. Что касается физлиц, то пока подавляющее их большинство предпочитает в день зарплаты перекладывать деньги из банкомата в кошелек. «С такими проще работать по старинке — в темном подъезде», — отмечают банкиры. Таким образом, основные силы направляются банками на защиту счетов корпоративных клиентов.

Чаще всего на плохо защищенный компьютер клиента внедряется вредоносная (троянская) программа, предназначенная

для похищения ключей и паролей доступа клиента к системам интернет-банкинга, рассказывают в пресс-службе банка ВТБ24. Затем хакер соединяется с системой интернет-банкинга от имени клиента и пытается провести операции по переводу денежных средств со счета клиента на счета, открытые на подставных лиц. «Не последнее место в арсенале мошенников занимают и средства социальной инженерии», — добавляет господин Шелин. Злоумышленник связывается с клиентом от имени банка, убеждает его дать ему какие-либо свои учетные данные (например, имя и пароль) или просит запустить присланную от имени банка программу для того, чтобы устранить какой-то опасный вирус. На самом же деле это и оказывается вирус, который крадет данные с компьютера.

АНТИХАКЕРСКИЕ ТЕХНОЛОГИИ

Чтобы защитить клиентов, банки совершенствуют свои системы безопасности. Так, в ВТБ24 внедрили дополнительную защиту для юридических лиц на основе одно-разовых паролей, передаваемых клиентам в SMS-сообщениях. Для физических лиц банк сделал обязательным использование переменных кодов, вводимых со скрэтч-карт. «В дальнейшем планируем внедрение системы аутентификации клиентов, работающей с токенами различных видов, EMV-картами, USB-токенами с криптографическими функциями и другими средствами аутентификации, а также внедрение системы фрод-мониторинга»,

— сообщили в пресс-службе банка. Банк «Санкт-Петербург» постоянно работает над совершенствованием системы защиты информации в системе «Банк-Клиент» и «Интернет-Банк». По словам господина Шелина, система включает в себя идентификатор — уникальную числовую последовательность, позволяющую однозначно идентифицировать пользователя; пароль и SMS-код для входа в систему, отправляемый на номер мобильного телефона, указанный пользователем в заявлении на подключение. Доступ к системе осуществляется в сети интернет через защищенное соединение по протоколу SSL (Secure Socket Layer). В системе «Интернет-Клиент» для юридических лиц дополнительно используется стойкое шифрование и электронно-цифровая подпись (ЭЦП) всех данных, которыми клиенты обмениваются с банком. Шифрование защищает данные от перехвата злоумышленником, ЭЦП однозначно удостоверяет авторство данных. Подобные же средства защиты включает и подсистема «Банк-Клиент».

В банке «ВТБ Северо-Запад», кроме криптографической защиты, применяются специализированные устройства защиты периметра корпоративной вычислительной сети с модулями обнаружения вторжения, рассказали в его пресс-службе. Клиентам предоставляется возможность использования USB-ключа, защищенного от взлома, а также возможность доступа из сети интернет по фиксированным IP-адресам, что предотвращает мошенничество в случае кражи ключей.