Кибермошенники нацелились на финансовые данные

Денис Гасилин

Среди информации, потенциально доступной злоумышленникам в киберпространстве, наибольшей популярностью пользуются финансовые данные. Это закономерно — такую информацию проще всего превратить в деньги, продав на черном рынке, либо воспользовавшись ею самостоятельно.

Впрочем, в последние годы кибератаки на банки и финансовые организации не сводятся лишь к похищению данных клиентов, заражению использующих ДБО (дистанционное банковское обслуживание) устройств вредоносным кодом или попыткам проникнуть в защищенный периметр ИТ-инфраструктуры компании с целью модификации или уничтожения определенных записей. DDoS-атаки на банковскую инфраструктуру вплоть до атак непосредственно на сети банкоматов имеют две основные цели: нанесение ущерба и сокрытие мошеннических финансовых операций в общем «шуме» от нападения.

Киберугрозы постоянно усложняются, поэтому необходима повышенная бдительность и выделение достаточных ресурсов на идентификацию и нейтрализацию соответствующих рисков. Ущерб от кибератак может заключаться в снижении доступности или увеличении времени на обработку запроса в онлайн-сервисах для банкинга, хищении персональных данных или коммерческой тайны и, разумеется, мошенничестве.

Сами киберугрозы в этой области можно разделить на несколько основных типов. Во-первых, это взлом банковских сетей с целью модификации данных или внедрения шпионских программ в инфраструктуру. Во-вторых, это всевозможные атаки, направленные на сервисы ДБО, от заражения банкоматов вредоносным кодом до использования уязвимостей в мобильных устройствах для обхода валидации финансовой операции владельцем счета по СМС. В-третьих, — грубые DDoS-атаки, направленные не на кражу данных, а на нанесение непосредственного вреда финансовой организации.

В этом году и в ближайшем будущем угрозы будут распределяться по направлениям, на которые следует обратить особое внимание как самим финансовым организациям, так и регуляторам в этой области.

Мобильный банкинг развивается хаотично, обилие платформ, разобщенность разработчиков приложений ДБО и представителей банков и прочих финансовых организаций, относительная простота утери мобильного устройства — все эти и многие другие факторы привели к тому, что на данный момент этот канал проведения транзакций стал самым уязвимым среди прочих. Однако пример UW Credit Union, компании, полностью отказавшейся от приложений мобильного ДБО в пользу обычного веб-интерфейса, доработанного под мобильные системы, вряд ли получит распространение. Несмотря на все риски, связанные с использованием мобильных устройств, это решение слишком выгодно с точки зрения бизнеса, чтобы его реализацию смогли остановить или хотя бы замедлить соображения безопасности. Даже появление таких троянов, как Bugat и Eurograbber, которые могут обходить двухфакторную аутентификацию, не останавливает бум на рынке банковских приложений, так что число атак растет, и проблема приобретает все большую остроту. Защита мобильных устройств, способная полностью «вылечить» от инфекции, при этом не поглощая весьма ограниченные ресурсы таких мини-компьютеров, будет в цене.

Стоит отметить интересный факт — в последнее время продажи банковских троянов на черном рынке киберпреступников резко сократились. Вместо этого отдельные группы злоумышленников концентрируются на разработке и поддержке отдельных программ вместо хаотичной доработки чужих приложений и модулей, как это было раньше. Кооперация между кибермошенниками вывела создание вредоносных программ на уровень разработки коммерческого ПО в обычных условиях, — что приводит к постоянному появлению новых модификаций вредоносного кода, бросающих вызовы поставщикам защитных решений. Особая нагрузка ложится на решения, работающие по принципу анализа сигнатур и «черных списков».

Совершенствуются и техники DDoS-атак, их количество растет. С сентября 2012 г. по май 2013 г. крупные банки США подверглись трем волнам атак, усиливающихся с каждым разом, а пример южнокорейских банков Shinhan и NongHyup показал, как такое нападение способно полностью парализовать деятельность компании на часы, если не дни, что приводит к большим прямым убыткам и огромным репутационным потерям. При этом вектор атаки сейчас смещается на меньшие по размеру и оборотам банки, которые не могут тратить необходимые для покупки, установки и настройки комплексных систем защиты информации суммы и которые не имеют достаточного количества квалифицированных специалистов, чтобы полноценно развернуть такие системы самостоятельно. Вообще небольшие, слабо защищенные организации сейчас стали крайне привлекательными целями для кибермошенников, ведь в цепочке связей между физическими деньгами и данными на серверах таких организаций достаточно одного слабого звена, чтобы вся система была скомпрометирована. Это продемонстрировало нам дерзкое преступление, совершенное в феврале 2013 г.: успешный взлом процессингового центра в Индии и банка Ras Al-Khaimah в ОАЭ стали началом глобальной преступной операции, затронувшей более 20 стран и обогатившей преступников по меньшей мере на 45 млн. долл. Малые и средние по размеру кредитно-финансовые организации отчаянно нуждаются в решениях, не требующих длительного и затратного внедрения, но при этом способных успешно защищать ИТ-инфраструктуру от нападения извне.

Что же касается вмешательства изнутри, то количество случайных утечек данных в банковской сфере снизилось практически до нуля и традиционные DLP-системы вполне справляются с такими угрозами для персональных и корпоративных данных. Однако злонамеренные утечки данных по-прежнему происходят и тенденции снижения их количества пока не наблюдается. Недавний скандал с воровством с зарплатных карт Сбербанка, которое совершили действующие сотрудники, не является чем-то из ряда вон выходящим — во всем мире идет поиск способов пресечения подобных преступлений в автоматическом режиме. Отдельно стоит отметить проявившиеся новые каналы утечек информации, в первую очередь — из резервных копий и мобильных устройств, также по понятным причинам неудовлетворительно работает мониторинг распространения документации в бумажном варианте.

Больше стало и манипуляций с устройствами самообслуживания и рабочими местами операторов на точках розничной торговли. Трояны, перехватывающие данные с карточки и введенный пин-код на этапе передачи данных от клавиатуры к компьютеру, подключение внешних устройств и заражение POS-терминалов кодом, по сути, являющимся высокотехнологичным аналогом скиммера, — все это приходит на смену грубым методам ограбления банков и банкоматов. Незащищенность некоторых элементов цепи приводит к курьезам вроде случая в Комсомольске-на-Амуре в первой половине этого года, когда продавец в салоне мобильной связи смог обокрасть компанию-работодателя на миллионы рублей, использовав на своем рабочем месте программу, позволяющую получать преимущество в компьютерных играх и с легкостью модифицировавшую цены в торговой системе.

Автор — руководитель отдела маркетинга компании SafenSoft.