# Не отследить, а предупредить:
## инсайд от банка до банкомата

**Денис ГАСИЛИН,**
*руководитель отдела маркетинга, компания SafenSoft*

Существует мнение, что угроза инсайдерской активности воспринимается с точки зрения защиты конфиденциальной информации от утечки, намеренной или ненамеренной. Такой подход устаревает с увеличением количества таргетированных атак на организации. В наши дни борьба с инсайдом должна восприниматься в первую очередь как комплекс мер, принимаемых в целях предотвращения любой вредоносной активности изнутри организации.

Люди склонны совершать ошибки. К примеру, намеренная «утеря» зараженной флешки на территории организации уже давно стала одним из способов заражения информационных систем компании. Обнаруживший такую флешку сотрудник зачастую подключает ее к рабочему компьютеру. Проблема заключается в том, что операционные системы компьютеров этих сотрудников позволяют использовать любые носители информации, не требуя никаких проверок и разрешений. Существуют технические средства, позволяющие избежать подобных ситуаций, но более половины организаций, согласно исследованию компании Ponemon, предпочитают никак не ограничивать сотрудников в использовании флеш-накопителей, потому что не хотят следующего за такой мерой понижения продуктивности. Организационные меры необходимо поддерживать технически или концентрироваться на технической реализации принципа «все, что не разрешено, то запрещено». Данный подход также называется принципом «белых списков» и позволяет сводить на нет любые не санкционированные ответственным лицом изменения в системе, предотвращая атаки на компанию изнутри. Примером защитного ПО для рабочих компьютеров, созданного по такой технологии, является решение SafenSoft Enterprise Suite.

Самыми коммерчески ценными для киберпреступников, т. е. самыми простыми способами получить немедленную прибыль, сейчас являются кража наличных денег из устройств и информации с банковских карт. И то и другое достигается за счет взаимодействия с устройствами самообслуживания: банкоматами, POS-терминалами, реже – терминалами для оплаты различных услуг. Существует два основных вида вредоносного кода для устройств самообслуживания: «диспенсеры», способные выдавать команды на выдачу наличных в обход стандартных процедур, и «скиммеры», которые, как и традиционные скиммеры, крадут данные с карточек, но делают это на программном уровне, что серьезно затрудняет обнаружение.

Главная проблема для злоумышленника при заражении устройства самообслуживания вредоносным кодом заключается в получении доступа. Такое устройство гораздо сложнее заразить, чем обычный компьютер, потому что доступ к нему обычно имеют только сотрудники, а внешних каналов связи, открытых для посторонних, практически не существует. Каждый случай успешного заражения – большой успех для злоумышленников, ведь через каждое устройство проходит множество пластиковых карт, а если есть возможность прямого диспенса, то из одного зараженного банкомата можно украсть миллионы рублей. При этом современный вредоносный код достаточно продвинут, чтобы избегать обнаружения антивирусами, а также самоуничтожаться после исполнения своей миссии, что значительно затрудняет расследование инцидентов. За прошедшие два года было зафиксировано множество случаев заражения устройств самообслуживания, а доступность специализированного вредоносного кода на «черном» рынке вышла на новый уровень. Такие трояны, как Backoff, заразивший POS-терминалы более чем тысячи компаний в США, и Ploutus, созданный в Латинской Америке и способный опустошать банкоматы по всему миру, продаются через Интернет. Продавцы не только проведут демонстрацию «продукта», но и расскажут, как им пользоваться и какое дополнительное оборудование может понадобиться. Единственный выход из ситуации – специальное защитное ПО для банкоматов, исключающее возможность заражения системы вредоносным кодом, не важно, обслуживающим персоналом или посторонним взломщиком. Рост продаж нашего продукта для банкоматов SafenSoft TPSecure позволяет надеяться, что бизнес воспринимает эту угрозу всерьез. ■