Разработчик антивирусного программного обеспечения компания «Доктор Веб» сообщает о появлении новой троянской программы, поражающей банкоматы одного из крупнейших производителей. Вирус Trojan.Skimer.18 способен перехватывать данные банковских карт, включая информацию о счете и PIN-коде. Полученные данные троян отправляет злоумышленникам. Вредоносная программа Trojan.Skimer.18 является первым подобным вирусом, направленным на банкоматы, распространенные в России.

Вирус представляет собой динамичную библиотеку, которая запускается из цифрового приложения, после чего выбирает файл для хранения информации о прошедшей транзакции. После запуска в ОС инфицированного банкомата, вредоносная программа ожидает авторизации пользователя. Далее Trojan.Skimer.18 считывает и сохраняет в файл Track2 данные карты – ее номер, PIN-код, срок действия, сервисный код. Вирус способен обойти шифровку PIN-кода, используемую разработчиками программного обеспечения банкоматов для обеспечения безопасности транзакций.

Управление Trojan.Skimer.18 осуществляется с помощью специальных мастер-карт. При попадании в инфицированный банкомат такой карты, на дисплее устройства появляется диалоговое окно, посредством которого злоумышленники управляют троянцем. По команде мошенников вирус может вывести на экран статистику по похищенной информации, удалить файлы из журнала, изменить режим работы банкомата или перезагрузить его.

Данные, похищенные Trojan.Skimer.18, записываются на чип мастер-карты, при этом информация проходит процедуру сжатия. Специалисты «Доктор Веб» отмечают схожесть вируса Trojan.Skimer.18 с аналогичными вредоносными программами, из чего сделан вывод о том, что авторство троянцев принадлежит одному разработчику.

Источник: igeek.ru