МНЕНИЕ ЭКСПЕРТА

Михаил Калиниченко, исполнительный директор «СНС Холдинг»

Атаки на банкоматы и терминалы не прекратятся, пока владельцы банкоматов не начнут уделять достаточно внимания информационной безопасности устройств самообслуживания. Даже уже известные и идентифицированные угрозы могут быть остановлены только специализированным защитным программным обеспечением, основанным на принципе проактивной защиты и обладающим мощными средствами самозащиты, а про новейший вредоносный код и говорить нечего. Традиционный подход к защите программной среды не работает в контексте устройств самообслуживания.

Кроме того, необходимо уделять пристальное внимание физической безопасности банкомата — сложность доступа к компьютеру устройства вкупе с отключением загрузки с внешних носителей и установкой пароля на внесение изменений в BIOS может остановить преступников низшего уровня. Но этого, конечно же, недостаточно для защиты от серьезной преступной организации, особенно вкупе с возможной инсайдерской активностью. Кроме того, в некоторых случаях злоумышленникам даже не нужно физически взаимодействовать с устройствами после первичного заражения — киберпреступнику достаточно получить звонок или сообщение от своего «денежного мула» и послать банкомату команду на выдачу наличных. Несколько раз за последние 10 лет банкоматы даже заражались дистанционно. Специализированное защитное ПО, такое как Safe`n`Sec TPSecure, необходимо также и для того, чтобы отличить обычные перебои в работе устройства от зловредной активности. Необычное поведение банкоматов, такое как прерывание связи или прекращение обслуживания «родных» карт при работе сторонних, может свидетельствовать о заражении, за которым последует извлечение наличных или запись данных пластиковых карт клиентов, но в журнале устройства зловредная активность, разумеется, не отобразится. А вот защита, позволяющая предотвратить такое заражение или установленная уже после заражения, сможет также оперативно сообщить обо всех действиях злоумышленников или, например, выявить неудачливого инсайдера.