По данным ведущей международной компании по предотвращению и расследованию киберпреступлений (Group-IB) за 1,5 года группировкой Money Taker было проведено 20 успешных атак на банки и другие юридические организации на территории США, России и Великобритании.

В атаке на автоматизированное рабочее место клиента в одном из российских банков «участвовала» разработанная группой одноименная система Money Taker v 5.0. Это модульная программа, каждый компонент которой выполняет определенные действия:

«ищет» платежные поручения и модифицирует их, заменяя имеющиеся реквизиты на реквизиты злоумышленников;
затем «заметает следы».
В момент внесения в платежное поручение изменений оно еще не подписано: на подпись отправляется измененная «платежка» с реквизитами мошенников. Помимо уничтожения следов, модуль сокрытия меняет реквизиты злоумышленников в подтверждении дебета после списания обратно на подлинные.*

Чтобы избежать подобных атак мошенников при проведении платёжных поручений, система «ЗапСиб iNet» оснащена инструментами обеспечения информационной безопасности. Для противодействия удаленным атакам мошенников был разработан сервис «Пакет безопасности», который включает в себя устройство SafeTouch.

Устройство SafeTouch показывает реальные реквизиты подписываемого платежного поручения, которые необходимо сверить с внесенными в программу. Отправка платежного поручения заблокирована до момента подтверждения платежа нажатием кнопки на устройстве SafeTouch. Таким образом, удаленному злоумышленнику не удастся подменить реквизиты платежа.

«Правильное использование устройства SafeTouch при проведении платежных поручений поможет избежать атаки мошенников к счетам Клиента. Важно тщательно сверять корректность введенных реквизитов на экране устройства SafeTouch перед подписанием платежного поручения», - отметила директор Дирекции корпоративного бизнеса Оксана Седых.