Світличний В.А.,
к.т.н., Харківський національний
університет внутрішніх справ

СУЧАСНІ КІБЕРЗЛОЧИНИ З ВТРУЧАННЯМ У РОБОТУ БАНКОМАТІВ

Побічним явищем від масової комп'ютеризації та створення мережі Інтернет є поява кіберзлочинності. З кожним роком зростає суспільна небезпека, що наноситься ними шкоду світовій економіці, фінансових рахунках простих громадян. Одним з найпоширеніших видів кіберзлочинів в системах інтернет-банкінгу, є «скімінг», тобто підробка банківських карт. Так за даними американських експертів компанії Visa Inc., що надає послуги проведення платіжних операцій, лідерами серед незаконних операцій з банківськими картами являються саме скіммінг та використання його результатів за допомогою online-шахрайства.

Ще одна очевидна причина пожвавлення скіммінга в Україні - збільшення обсягу грошових коштів, які проходять через банківські карти. На даний момент він збільшився в кілька разів, тому шахрайство в даному секторі залишається справою надприбутковою. При великому ринку шахрайства в онлайн-банкінгу і системах дистанційного банківського обслуговування для юридичних осіб, новий ринок привернув українських та іноземних хакерів, тому що населення країни набагато гірше навчено правилам безпеки при використанні пластикових карт, як в банкоматі, так і в Інтернеті.

Свою роль відіграють і інші особливості української кіберзлочинності: надприбутки, ілюзія безкарності і слабке законодавство.

Скіммінг (від англ. skim – знімати вершки) - створення копії магнітної смуги для виготовлення клону карти користувача за допомогою спеціалізованих пристроїв, які називаються "скімери" і "шиммери" і найчастіше встановлюються на банкомати. За принципом дії ці пристрої не відрізняються один від одного і потребують використання прихованих відеокамер або накладок на клавіатуру банкомату для отримання PIN – коду [1].

Однак в шиммінгу замість традиційних громіздких скіммерів на щілину приймача пластикових карт банкоматів використовується дуже тонка, гнучка плата, впроваджується через цю щілину в середину банкомата. "Шим" підсаджується за допомогою спеціальної карти – носія: її просовують у щілину банкомату, де тонкий "шим" приєднується до контактів, що прочитує дані з карт, після чого картка-носій видаляється. Далі все працює, як і при традиційному скіммінгу – тобто вставляються в банкомат пластикових карт, де зчитуються всі важливі дані "дампи", які потім використовуються зловмисниками для виробництва карток – дублікатів та зняття з їх допомогою грошей. Єдине, але дуже важливе на відміну від скіммінгу полягає у відсутності будь-яких зовнішніх ознак шиммінгу того, що в банкоматі сидить "жучок". Виходячи зі специфікацій, що регулюють розміри щілини кард-рідера,

товщина "шима" не повинна перевищувати 0,1 мм [1], інакше він буде заважати пластиковим картам. Це приблизно вдвічі тонше людської волосини.

Для власників банківських платіжних карток розроблено величезну кількість різноманітних інструкцій і правил безпеки. Основні з них наступні:

При проведенні операцій з карткою користуйтеся тільки тими банкоматами, які розташовані в безпечних місцях і обладнані системою відеоспостереження і охороною: у державних установах, банках, великих торгівельних центрах і т. д [2].

Звертайте увагу на картоприймач і клавіатуру банкомату. Якщо вони обладнані якими-небудь додатковими пристроями, то від використання даного банкомата краще утриматися і повідомити про свої підозри за вказаним на моніторі банкомату телефону.

У випадку некоректної роботи банкомату – якщо він довгий час перебуває в режимі очікування або мимоволі перезавантажується – відмовтеся від його використання. Велика ймовірність того, що він перепрограмований зловмисниками.

Ніколи не піддавайтесь допомозі порадам сторонніх осіб при проведенні операцій з банківської картки в банкоматах. Зв'яжіться з Вашим банком – він зобов'язаний надати консультаційні послуги по роботі з картою.

У торгових точках, ресторанах і кафе всі дії з Вашою картою повинні відбуватися у Вашій присутності. В іншому випадку шахраї можуть отримати реквізити Вашої картки за допомогою спеціальних пристроїв і використовувати їх в подальшому для виготовлення підробки.

Використані джерела:

1. Світличний В.А. Виявлення пристроїв для незаконного втручання в роботу банкоматів / В.А. Світличний, А.П. Синиця // Збірник тез доповідей XXIII науково-практичної конференції курсантів та студентів «Актуальні проблеми сучасної науки і правоохоронної діяльності», м. Харків, 17 травня 2016 р. /Харківський національний університет внутрішніх справ. – 2016. – с.211
2. Дьяков М. Сюрприз для банкомата: вирусы и способы защиты от них: [Електронний ресурс]. – Режим доступу: http://www.prostobankir.com.ua/it/stati/syurpriz_dlya_bankomata_virusy_i_sposoby_zaschity_ot_nih