цим хотілось би, щоб Україна, як одна із країн, в якій активно використовуються інтернет-технології та кількість користувачів постійно зростає, мала активні засоби захисту та протидії кіберзлочинності та активно готувала кваліфікованих спеціалістів, які б завжди були готові захистити інтереси держави.

Література:

1. Кіберзлочинність та відмивання коштів // Департамент фінансових розслідувань Державна служба фінансового моніторингу України // [Електронний ресурс]. - Режим доступу: http://www.sdfm.gov.ua/content/file/site_docs/2013/20131230/tipolog2013.pdf
2. Markets for Cybercrime Tools and Stolen Data [Електронний ресурс]. – Режим доступу: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/ RAND_RR610.pdf
3. Киберпреступность [Електронний ресурс]. – Режим доступу: http://n-auditor.com.ua/ru/component/na_archive/773?view=material

Кіберзлочини у фінансово-банквський сфері: скімінг та способи його викорінення

Дарвін О.В.
Студент 3 курсу факультету №4 ОДУВС
Олексієнко Д.
Слухач магістратури 2 курсу ПОД
Науковий керівник: О.В. Косаревська
кандидат педагогічних наук, доцент
доцент кафедри кібербезпеки та
інформаційного забезпечення ОДУВС

На сьогоднішній день кіберзлочинність поширена скрізь, одним із чимало важливих видів кіберзлочинності є скімінг. Актуальність платіжних карток на часі важко переоцінити. Українці все частіше розраховуються ними за покупки на лише в інтернет-магазинах, але й у звичайних торгових мережах.

Карткою дійсно легше розраховуватися у супермаркеті,не треба кожного дня думати, скільки брати з собою грошей та перейматися, щоб у вас часом не витягали гаманець у метро чи іншому людному місці. Проте й у цієї медалі є і інший бік – шахраї вже доволі давно досягли того рівня, коли з легкістю можуть спустошити ваш банківський рахунок. Для цього вам лише треба «засвітити» картку у будь-якому банкоматі, магазині або навіть кафе. Це один з самих привабливих способів шахрайства з банківськими картами існує вже досить-таки давно і є реальною небезпекою для всіх власників пластикових карток. Метою скімінга є виготовлення дубліката платіжної картки та зняття з неї всієї готівки в банкоматі, але при цьому справжня картка знаходиться у нас. Ми навіть можемо і не підозрювати, що нас обкрадають. Це дійсно дуже погана погана і неприємна ситуація, з якою може зіткнутися кожен з нас. Ми навіть можемо і не підозрювати, що нас обкрадають. Це дійсно дуже погана і неприємна ситуація, з якою може зіткнутися кожен з нас.

Саме слово «скімінг» з'явилося на початку 90-х років минулого сторіччя, від аналогічної назви спеціального електронного пристрою, який злодії прикріплюють до картоприймача в банкоматі, і з того часу розпочав набирати обертів, як з кількості вчинених злочинів, так і в плані удосконалення прийомів та технічних засобів, що використовуються злочинцями [2].

На актуальність боротьби з даним видом злочинів в Україні вказує створення Управління боротьби з кіберзлочинністю МВС України та Департаменту кіберполіції Національної поліції України, функцією яких є розкриття злочинів пов'язаних з банківською сферою та платіжними системами.

Огляд сучасної наукової думки стосовно протидії скімінгу, а саме робіт Кійкова В.М. та Онищенко Ю.М. доводить, що найбільш ефективними технологіями банківської боротьби за скімінгом є : фізичний моніторинг, пасивний анти-скімінг і активний санти-скімінг [1].

Фізичний моніторинг банкоматів включає в себе періодичний огляд банкомату співробітниками банку, інкасаторами, або фахівцями сервісної служби на аутсорсингу. В ході перевірки за графіком заповнюється спеціальний журнал перевірок, щоб в разі знаходження чужорідного пристрою виявити проміжок часу, протягом якого був ризик компрометації карт. На практиці це ненадійний і дорогий спосіб боротьби зі скімінгом.

Пасивний анти-скімінг проявляється в тому, що банк встановлює на щілину карто приймача спеціальні анти-скімінгові накладки, що підключені до спеціального датчика, який спрацьовує в разі

спроби шахрая зняти анти-скімер з банкомату. Датчик може складатися із звичайних проводів, які рвуться при знятті анти-скімера з банкомату, або пари магніт + геркон (при якому контакти геркона реагують на видалення анти-скімінгової накладки з вбудованим магнітом), при цьому в процесі видалення анти-скімера наявність герконової пари шахрай може не помітити, що підвищує шанси його піймання. Недолік пасивного анти-скімінгу в тому, що багато власників карт, начитавшись і надивившись страшилок про банкоматні шахрайства, побачивши сторонній пристрій бояться (і до речі цілком виправдано) користуватися таким банкоматом. Частково вирішити цю проблему вдається шляхом розміщення спеціальної наклейки, де зображений правильний вид карто приймача. Технології зробили крок далеко вперед і виготовлені шахраями скімери важко відрізнити від анти-скімерів, навіть для співробітників банку. Пасивний анти-скімінг це бюджетний, компромісний, але не кращий варіант боротьби зі скімінгом [5].

Активний анти-скімінг це найдорожчий, але ефективний спосіб боротьби зі скімінгом. Пристрій встановлюється в середині банкомату і непомітно зовні. Активний анти-скімер контролює простір перед банкоматом і дозволяє моментально виявити несанкціоновану установку на нього сторонніх пристроїв. Анти-скімер може також створювати радіоперешкоди в області щілини карто приймача, що перешкоджають роботі сторонніх електронних пристроїв. Датчики анти-скімера дозволяють аналізувати електромагнітне поле в зоні розміщення картридера, ПІН-клавіатури і монітора в разі різкої зміни напруженості поля (включення випромінювальних пристроїв при радіопередачі, установка стороннього обладнання), пристрій подає команду на керуючий блок банкомату, який виводить банкомат з режиму обслуговування клієнтів і може виконувати додаткові дії (відправка команд, СМС, оповіщення служби охорони і моніторингу і т.д.) [4].

Найдієвішим із напрямків боротьби зі скімінгом є перехід на мікропроцесорні пластикові картки (EMV–технологія) і за можливістю відмовитися від карток з магнітної стрічкою. В таких умовах для боротьби з проблемою підробки картки із забезпеченням збереження PIN-коду,полягає у використанні виробниками і власниками терміналів удосконалених і більш захищених способів оновлення ссесійних ключів в алгоритмі 3DES та шифрування даних для PIN-коду (стандарт ANSIX9.8) Найбільш всього захищеним на даний час вважається алгоритм шифрування 3DES [3].

На підставі зазначеного можна зробити висновки, що скімінг займає самостійне місце в структурі кіберзлочинів в банківський системі. Одним із дієвих засобів боротьби зі скімінгом є перехід на мікропроцесорні пластикові картки (EMV–технологія) і за можливістю відмовитися від карток з магнітної стрічкою. В таких умовах для боротьби з проблемою підробки картки із забезпеченням збереження PIN-коду, полягає у використанні виробниками і власниками терміналів удосконалених і більш захищених способів оновлення сесійних ключів в алгоритмі 3DES та шифрування даних для PIN-коду (стандарт ANSIX9.8).

Найбільш всього захищеним на даний час вважається алгоритм шифрування 3DES.

Література:

1. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю / О.В. Орлов,Ю.М. Онищенко // Теорія та практика державного управліня.-2013.- Вип. 3. – С 3-9. – Режим доступу: http://gov.ua/j-pdf/Tpdu_2013_3_3.pdf

2. Про затвердження Типологій легалізації (відмивання) доходів,одержаних злочинним шляхом, у 2013 році : наказ Держ. служби фінанс. моніторингу від 25 груд. 2013 р. № 157 [Електронний ресурс]. –Режим доступу: http://cct.com.ua/2014/25.12.2013_157.htm.

3. Schmidt L. Warning signs [Електроннийресурс] / LucindaSchmidt. – Режим доступу: http://moneymanager.smh.com.au/articles/2003/10/15/1065917445606.html

4. Wisconsin Bankers Association Warns Consumers, Asks forHelp In Identifying ATM Card Skimming Scam [Електроннийресурс]. – Режимдоступу: http://www.wisbank.com/Media/Press%20Releases/PR_ATM_Card_Skimming_Scam.htm.

5. Costa C. MasterCard International Hosts First Global RiskManagement Symposium [Електроннийресурс] / Christina Costa. –Режимдоступу: http://www.mastercardintl.com/cgi-bin/newsroom.cgi?id=706.