РАССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ И ЭЛЕКТРОННЫХ ПЛАТЁЖНЫХ СРЕДСТВ

Иван Бабенко,
эксперт (Республика Молдова)

This article will provide a general overview on electronic commerce crimes investigation and on related Forensic. Also, you can find here general investigative methods and improvement recommendations at the level of issuing companies, and at the state level.

С развитием информационных технологий и коммерческих отношений привычные нам денежные операции переходят в электронный формат, предоставляя человеку удобный и эффективный инструментарий электронной коммерции.

Электронная коммерция (ЭК) - предпринимательская деятельность по осуществлению коммерческих операций с использованием электронных средств обмена данными. К объектам электронной коммерции относят различные товары, услуги и информацию. В качестве основного платёжного инструмента используются, электронные деньги.

Электронные деньги (ЭД) — это денежные обязательства эмитента в электронном виде, которые находятся на электронном носителе в распоряжении пользователя, базируются на не меньшем количестве *традиционных* денежных средств, находящемся в распоряжении эмитента и принимаются в качестве оплаты третьими лицами.

По данным отчёта IC3 за 2008 г. основная часть киберпреступлений (около 92%) происходят с использованием инструментария электронной коммерции.

Как средство для совершения преступления ЭД можно разделить на 3 условные группы:

- **пластиковые дебетовые или кредитные карты.** *Обычно служат злоумышленникам для совершения преступлений с банковскими счетами. Чаще всего такие преступления затрагивают относительно малое число пострадавших, но при этом ущерб на одного пострадавшего составляет достаточно крупные суммы денег.*
- **валюты систем для Интернет-платежей.** *Чаще всего используются для разовых платежей при мошенничестве в Сети, а также для сокры-*

тия следов киберпреступлений. Здесь преступникам помогает возможность автоматизации транзакций, а также конфиденциальность открываемых в таких системах счетов.

- **микроплатежи;** *Используются для масштабных по количеству пострадавших преступлений, но при этом с минимальным ущербом для одной жертвы, регистрация таких преступлений и обращение пострадавшего в правоохранительные органы происходит редко. Но, тем не менее, по общей сумме денег преступление может быть достаточно крупным и значимым.*

Отличительными чертами киберпреступлений в области ЭД и ЭК являются:

- целенаправленный характер;
- организованность и высокая координация при совершении преступления;
- групповой характер;
- международный состав, как преступной группы, так и пострадавших;
- почти всегда, предпринимаются действия по сокрытию следов преступления;
- чаще всего, требуют особых знаний и навыков, часто одним из соучастников является злонамеренный инсайдер, а также осуществляется квалифицированное юридическое сопровождение;
- трудно доказать преступный состав действий, даже если эти они носят явно асоциальный/преступный характер;

Невозможно дать исчерпывающий перечень способов совершения преступлений в области ЭК и ЭД, так как наряду с известными способами, постоянно появляются новые, более изощрённые и комбинированное использование известных способов.

Рассмотрим перечень наиболее часто встречающихся преступлений:

- фишинг - представляет широкий спектр преступлений. Используется в качестве основного или вспомогательного средства в подавляющем большинстве случаев
- фальсификация электронных платёжных средств;
- мошенничество с использованием пластиковых карт;
- удалённый НСД к серверам платёжной системы и доступ с использованием служебного положения;
- перехват трафика, чтение почты, а также вирусы и троянские программы для сбора платёжной информации и ключей доступа;
- скиминг – получение данных пластиковых карт посредством физической установки на банкоматы специальных накладок для считывания данных карт и PIN-кодов;

- взлом интернет-магазинов и плохо защищённых платёжных систем;
- фиктивные покупки в Интернет-магазинах и -казино;
- легализация незаконно приобретённых денежных средств;
- сбор и торговля конфиденциальной информацией или незаконными товарами и услугами, используя сервера страны с более "свободным" законодательством и правовой обстановкой;
- преступная небрежность при функционировании точек продаж ЭК;
- продажа заведомо некачественных/не соответствующих описанию/несуществующих товаров;

и многие другие виды и подвиды преступлений…

Основным мотивом для рассматриваемого класса преступлений является материальная заинтересованность злоумышленника. Другие мотивы не исключаются, но чаще всего объектом являются именно деньги, либо товары и услуги которые можно приобрести путём злонамеренных действий.

ОРМ по киберпреступлениям, *совершающимся при помощи коммуникаций и каналов связи удалённо* могут содержать:

1. Исследование и перехват трафика по установленным каналам связи;
2. Поиск следов на сервере и системе (месте преступления);
3. Установление иных коммуникационных средств, вовлечённых в преступление;
4. Установление принадлежности IP-адреса или домена злоумышленника ;
5. Поиск следов подготовки преступления во внешней среде;
6. Установление лиц имевших доступ к системе, либо располагавших сведениями о недостатках системы;
7. Установление текущего местоположения незаконно полученных денежных средств и проверка цепочки операций, совершённых с ними после преступления;
8. При необходимости, расследование преступления в международном масштабе, если есть причины полагать, что преступник действовал не только в рамках государства, а и за его пределами, обычно так и происходит в случаях крупного мошенничества и хищения.

ОРМ по киберпреступлениям, *совершающимся при физическом контакте с оборудованием или коммуникационными сетями платёжных систем,* могут содержать:

1. анализ системы пропусков и системы слежения за оборудованием, при их наличии;
2. поиск следов на сервере и в системе;

3. анализ предшествующих инцидентов, зарегистрированных в платёжной системе;
4. исследование, оставленных на месте преступления следов монтажа, оборудования, исходящих каналов передачи данных;
5. исследование вещественных доказательств и, в случае если они были произведены промышленным путём, установление производителя;
6. установление лиц, имевших отношение к разработке аппаратно-программного комплекса для работы платёжной системы.

Предотвращение преступлений в ЭК может быть очень эффективным при использовании общих и специальных стандартов *(стандарты серии ISO/IEC, PCI/PA DSS, PCI PED и т.д.)*. Для всех преступлений в ЭК внедрение стандартизации может значительно снизить риски возникновения инцидентов. На уровне государства это должно решаться принятием национальных законов об регламентации отношений в области ЭК и законов, касающихся информационной безопасности в соответствии с действующими международными стандартами и Конвенцией Совета Европы по борьбе с киберпреступностью.

Закалючение

Для борьбы с преступностью в сфере ЭК *платёжным системам и банкам* необходимо эффективно внедрять общеотраслевые и внутренние корпоративные стандарты безопасности и постоянно осуществлять контроль конфиденциальности, целостности, доступности и аутентификации при работе с информацией, а также регулярно проводить внешний и внутренний аудит безопасности и тщательно расследовать каждый инцидент.

В государственных масштабах необходимо позаботиться о правовой ситуации, а также вывести процедуру расследования преступлений в сфере ЭК на должный уровень, что поможет повысить их раскрываемость, а также снизит скрытую преступность. А международное сотрудничество в сфере расследования киберпреступлений может значительно повлиять на эффективность работы по раскрытию преступлений.

Литература

1. Закон РМ Nr. 284 от 22.07.2004 об электронной торговле
2. *Юрасов А.В.*, Основы электронной коммерции. Учебник для вузов. Телеком, 2008.
3. *Евтодиенко. Д.*, Пластиковые Карточки – один из способов Интернет-мошенничества *http://www.ase.md/~osa/publ/ru/pubru107/Evtodienco_D.pdf*