За матеріалами ІІІ- ї
міжнародної науково-практичної конференції
ІНФОРМАЦІЙНА ТА ЕКОНОМІЧНА БЕЗПЕКА (INFECO-2010)

УДК 343.98

ПОДПОЛЬНАЯ ИНФОРМАЦИОННАЯ ИНДУСТРИЯ

Охрименко С.А., д.э.н., профессор (МЭА, Кишинев, Молдова)
Саркисян А.С., к.э.н., доцент (ХА им. Д.А. Ценова, Свиштов, Болгария)

У статті представлений аналіз підпільної інформаційної індустрії, що ґрунтується на використанні "тіньових" інформаційних технологій. Формалізовано основні елементи "тіньової" економіки, напрямки діяльності "тіньового" ринку, основні протиправні функції.

Ключові слова: інформаційна індустрія, "тіньові" інформаційні технології, "тіньова" економіка.

Постановка проблемы и ее связь с научными и практическими задачами. Развитие информационных и коммуникационных технологий коренным образом изменило повседневную жизнь, управление экономическими и социальными процессами, превратилось в доминирующий фактор устойчивого развития общества. В настоящее время средства информатизации составляют значительную долю мирового рынка и в существенной мере определяют структуру инвестиционных потоков. Но необходимо видеть не только положительные изменения, но и возможную опасность и риски, невнимание и недооценка которых, могут иметь серьезные последствия. Рынок информационных технологий по объему превысил рынок природных ресурсов. Но одновременно с этим, потери, связанные с правонарушениями в среде сбора, обработки и распространения информационных продуктов и услуг составляют астрономические цифры. Информационные технологии все глубже проникают в нашу повседневную жизнь, а вместе с ними – киберпреступность. Непонимание серьезности данной проблемы, совершенно не означает, что ее не существует. Негативное воздействие теневых информационных технологий объективно существует и возрастает, и к этому необходимо готовиться.

«Теневые» информационные технологии. Не является секретом, что параллельно с официальным многомиллиардным рынком информационных и коммуникационных технологий существует и развивается «теневой» рынок продуктов и услуг.

Анализ последних исследования и публикаций. В специальной литературе используются множество терминов, характеризующих данную сферу деятельности. В частности, используются такие категории, как «криминальная», «противоправная», «теневая», «подпольная», «неосязаемая», «нелегальная», «скрытая и фиктивная экономика», «черная», «серая», а также «параллельная экономика» [1,3,7,11,13 и др.].

Выделение нерешенных частей общей проблемы. Во всех существующих определениях по-разному очерчиваются границы данной экономики, но отмечается главный признак – скрытый и антиобщественный характер. Сложность и общественная значимость проблем «теневой» экономики информационных технологий, по нашему мнению, предопределяет необходимость междисциплинарного подхода к их исследованию.

Формирование целей статьи. Целью статьи является проведение всестороннего анализа подпольной информационной индустрии, которая основывается на использовании "теневых" информационных технологиях.

Основной материал. Истоками «теневой» информационной экономики следует считать переход от индустриальной эры начала 80-х годов к информационной, когда производство и распределение информации обеспечивало генерацию конкурентного преимущества. С 1992 г. по 2002 г. просуществовала «Экономика, основанная на знаниях». После этого этапа текущее состояние определяется как «неосязаемая экономика» [8].

Основными элементами «теневой» экономики являются: незаконные экономические отношения, скрытая экономика, сфера

нелегального бизнеса, связанного с производством, реализацией и потреблением запрещенных товаров и услуг; сфера нелегальной занятости и сфера уголовного промысла, в рамках которых криминальные доходы извлекаются путем систематического совершения кибепреступлений. Теневая экономика включает в себя «скрытые, неформальные и нелегальные» виды деятельности, она может быть представлена как саморегулируемая и управляемая система, в которой разрабатываются экономико-математические модели прогнозирования и управления поведением вовлеченных в данную систему. В рамках «теневой» экономики информационных технологий можно четко выделить [12-17]:

- противоправное производство;
- противоправный экономический обмен;
- противоправное потребление и удовлетворение деструктивных и асоциальных потребностей;
- собственно киберпреступления.

Структура данного «теневого» рынка весьма разнообразна и включает множество сегментов [3,6,10]. В первую очередь, это относится к деятельности, связанной с такими категориями, как «фишинг», «спам», «хакинг», «крэкинг», «кардинг», «присвоение системы», «спуфинг», «теневые вычисления», «инсайдер», «оффшорная индустрия», «оффшорный кибертерроризм» и многими другими. Отмечается создание специализированных групп «по интересам». К ним относятся группы, специализирующиеся в следующих направлениях деятельности:

- написание вредоносного кода для реализации различных действий в отношении несанкционированного доступа к информационным ресурсам пользователей и информационных систем;
- рассылка спама;
- организации удаленных и распределенных атак на информационные системы (DoS и DDoS);
- создание ботнетов в качестве «стартовой» и «вычислительной» площадок и сдача их в аренду для реализации комплекса противоправных действий [15-17];
- кража идентификаторов пользователей кредитных карт и изготовление поддельных кредитных карт;
- снятие средств защиты с лицензионного программного обеспечения;
- торговля нелицензионным программным обеспечением;
- торговля несуществующими продуктами и услугами, "мошенничество-как-услуга" (по аналогии с "программным обеспечением как услугой") и многие др.

Данные группы и их противоправная деятельность характеризуется одним емким определением – киберпреступность.

К основному инструментарию киберпреступников можно отнести такие действия, как создание ботнетов и «зомбирование» персональных компьютеров и информационных систем, использование перехватчиков клавиатуры, организация распределенных атак, использование анализаторы пакетов, шпионских программ, троянских программ, компьютерных червей, вирусных механизмов и т.д. Следует отметить, что инструментарий кибермошенников постоянно совершенствуется – от использования механизмов угадывания и взлома паролей, до многоэтапных атак на информационные системы [9].

Удаленная атака – несанкционированное информационное воздействие на информационную систему, программно осуществляемое по каналам связи. Выделяется два подтипа удаленных атак. Первый направлен на инфраструктуру и протоколы сети. Второй – на телекоммуникационные службы с использованием уязвимостей. Для оценки эффективности атаки используют три измерения: интенсивность атаки; длительность атаки и эволюция атаки во времени. Дополнительной характеристикой может служить отношение «эффективность-стоимость» [10,11]. Организация эффективной атаки по стоимости может быть весьма низкой, но может иметь непропорционально огромные последствия, что является преимуществом нападающей стороны. При сохранении максимальной эффективности может последовать следующее нападение с использованием нового инструментария. Отражение атак, соответственно, влечет увеличение расходов защищающейся стороны. Основными результатами атак являются следующие:

- расширение прав доступа в сети;
- искажение информации;
- раскрытие информации;
- кража сервисов;
- снижение производительности сети или блокировка доступа к информационным ресурсам и многие другие.

Сложность проводимой атаки определяется уровнем программных, технических и коммуникационных возможностей или общим уровнем знаний атакующего. Выделяют четыре вида подобных возможностей:

- низкий, атакующий запускает программное обеспечение взлома, компилирует легкодоступный код или использует известный метод атаки;
- средний, атакующий использует широко известный метод нападения, но разворачивает атаку с модификацией стандартного набора средств;
- сложный, атакующий обладает определенным опытом, что позволяет долго скрывать свое присутствие за счет использования собственного написанного кода;

- очень сложный, атакующий использует ранее неизвестные разработки, умело заметает следы атаки и оставляет скрытые входы для повторного проникновения.

Полная и достаточная классификация удаленных атак по видам, в том числе таких, как анализ трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над рабочей станцией в сети, приведена в [2,4,5].

В общем виде распределенная атака реализуется следующим образом:

- атакующий компрометирует несколько машин, получивших название «зомби», вместе они образуют сеть, называемую ботнет;

- устанавливает на них программное обеспечение, которое будет впоследствии соединять «зомбированные» машины для реализации атак;

- соединяется с ними и объединяет их возможности для реализации атаки.

Основными противоправными функциями, выполняемыми ботнетами, являются следующие [12-17]:

- рассылка спама. С помощью зараженных компьютеров осуществляется массовая рассылка электронных писем. Это наиболее распространенный и один из самых простых и доходных вариантов эксплуатации ботнетов;

- кибершпионаж и кибершантаж. Ботнеты используются для проведения распределенных атак типа «отказ в обслуживании». Данные действия обеспечивают массовую перегрузку сайта и приводят к их блокировке за очень короткое время. Соответственно, за прекращение атаки киберпреступники требуют выкуп. Вместе с тем, подобного рода действия могут рассматриваться как средство информационного давления на государственные и коммерческие структуры;

- выуживание информации. Рентабельность вредоносного программного обеспечения для выуживания информации многократно превышает рентабельность электронных писем;

- кража конфиденциальных данных. Специальное программное обеспечение позволяет получать пароли пользователей для доступа к электронной почте, информационным ресурсам и т.д.;

- кража программного обеспечения.

Данный, далеко не полный перечень действий, направлен на «извлечение» денег, или создание реальных условий для потенциальных действий с тем, чтобы соответствующую информацию превратить в деньги или услуги.

Следует отметить также, что произошли определенные сдвиги в конечных целях киберпреступников. Если в начале процессов развития информационных и коммуникационных технологий, широкого внедрения персональных компьютеров, а также появления первых признаков информационных войн главной целью являлось нанесение опустошительного ущерба владельцам информационных систем за счет организации несанкционированного доступа, уничтожения информации, сбоев в работе коммуникационного оборудования и программного обеспечения и т.д. В настоящее время основная цель – «финансовые» стимулы и получение не просто выгоды, а получение прибыли. Поэтому в основу анализа действий кибермошенников, атакующих информационные системы и их ресурсы, а также действий защищающейся стороны и использования средств противостояния должна быть положена экономическая теория. Основой для оценки подобных действий должно стать сопоставление затрат и выгоды (прибыли). И в том случае, если выгода от данного вида деятельности превышает затраты, то можно предположить, что действия обязательно буду выполнены.

Следует также отметить, что с появлением ботнетов появился и развивается их «черный» рынок, они продаются, передаются в аренду, определяются соответствующие показатели «эффективности» (например, стоимость создания ботнета, размер оплаты для отключения веб-сайта жертвы в результате проведения атаки типа «отказ в обслуживании», стоимость аренды ботнета и др.). Кроме того, подпольная индустрия предлагает достаточно широкий набор готовых средств – программное обеспечение, готовые сети и анонимный хостинг. Снижение доходности подобных действий, в конечном счете, по нашему мнению, должно привести к уменьшению привлекательности процессов создания ботнетов и реализации распределенных атак и, в конечном счете, к их исчезновению.

Для успешной борьбы с подобным явлением необходимо лишить «теневых информационных предпринимателей» возможности получать прибыль и сделать данный вид бизнеса неэффективным. Необходимо создать условия, чтобы участники теневого интернет-рынка сталкивались с повышенным риском (технологическим, уголовным и т.д.).

Выводы. Теневой рынок информационных технологий обладает высоким интеллектуальным потенциалом, большим количеством материальных и финансовых средств и огромными экономическими возможностями. По своей структуре он неоднороден.

Представленный материал не исчерпывает всего многообразия проблем подпольного рынка информационных технологий. Поставленная задача – рассмотрение экономики теневого рынка информационных и коммуникационных технологий может считаться выполненной только при условии комплексного исследования всех сегментов, начиная от анализа действий, способствующих поиску уязвимостей в

программном обеспечении, организации атак на информационные ресурсы государственных и коммерческих систем, до – формирования условий создания и функционирования кибертерроризма.

СПИСОК ЛИТЕРАТУРЫ

1. Благодатских В.А., Середа С.А., Поскакалов К.Ф Экономико-правовые основы рынка программного обеспечения. – М.: Финансы и статистика, 2007.

2. Девятин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. – М.: Радио и связь, 2006.

3. Джеймс Л. Фишинг. Техника компьютерных преступлений. -М: НТ Пресс, 2008.

4. Информационная безопасность открытых систем: В 2 т. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия-Телеком, 2006.

5. Информационная безопасность систем организационного управления. Теоретические основы: В 2 т. – М.: Наука, 2006.

6. Лукацкий А. Стратегия безопасности Cisco Self-Defending Network 3.0. 2006. CISCO Systems Inc.

7. B.K.Edwards, S.J.Flaim. Measuring and Integrating the Shadow Economy: A Sector-Specific Approach. Los Alamos National Laboratory, June30, 2008.

8. J.Robbins. Information Security Automation: Proactively Managing Risk and Compliance. ISACA, June 2008.

9. Julia Allen, CERT Guide to System and Network Security Practices, Addison-Wesley, 2001

10. L.A.Gordon&M.P.Loeb. The Economic of Information Security Investments. ACM Transaction on Information and System Security, 5, No 4, November 2002.

11. Libicki M. Cyberderrence and Cyberwar. RAND Corporation. 2009.

12. Dagon D. Botnet Detection and Response. The Network is the Infection. OARC Workshop, 2005.

13. M.J.G van Eesten, J.M. Baurer. Economics of Malware: Security Decisions, Incentives and Externalities. STI Woring paper 2008/1.

14. Malicious Software (Malware): A Security Threat tj the Internet Economy. Ministerial Background Report. DSTI/ICCP/REG (2007)5/Final.

15. Security Research Unpick Botnet Economics.
(http://www.theregister.co.uk/2009/07/24/botnet economics/.

16. Namestnikov Y. The Economics of Botnet. (http://www.viruslist.com/
en/analysis?pubid=204792068.

17. Wilson C. Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. 2008.

Аннотация. В статье представлен анализ подпольной информационной индустрии, которая основывается на использовании "теневых" информационных технологиях. Формализованы основные элементы "теневой" экономики, направления деятельности "теневого" рынка, основные противоправные функции.

Ключевые слова: информационная индустрия, "теневые" информационные технологии, "теневая" экономика.

Summary. In the article the analysis of the underground information industry which is grounded on usage "shadow" information technologies is presented. Key elements of "shadow" economy, an area of activity of the "shadow" market, the main illegal functions are formalized.

Keywords: the information industry, "shadow" information technologies, "shadow" economy.

Эксперт редакционной коллегии *к.э.н., доцент УкрГАЖТ Токмакова И.В.*