УДК 004

Силуянова О.П.,
студент магистратуры
1 курс, Инженерно-экономический институт
Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнёва,
Россия, г. Красноярск

КИБЕРПРЕСТУПНОСТЬ КАК ОСНОВНАЯ ПРОБЛЕМА РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Аннотация: *XXI век - это век информационного общества, поэтому телекоммуникационные и компьютерные системы стали неотъемлемой частью всех сфер деятельности людей и государства. Однако, разработав глобальную компьютерную сеть и службы телекоммуникации для своих нужд, люди даже не предполагали, что со временем это станет объектом больших проблем и начнёт причинять им вред.*

Ключевые слова: *киберпреступность, информационная безопасность, компьютер, информационное общество.*

Annotation: *The twenty-first century is a century of the information society, so the telecommunications and computer systems have become an integral part of all spheres of human activity and the state. However, developing a global computer network and telecommunications service for their needs, people did not expect that it will be eventually subject to major problems and begin to harm them.*

Key words: *Cybercrime, Information Security, a computer, Information society*.

Понятие киберпреступности имеет международное значение и означает совершаемые людьми преступления, в процессе которых информационные технологии используются в преступных целях. Уровень развития этого вида преступлений напрямую зависит от степени развитости информационных

технологий и глобальных сетей, а также открытости доступа к ним. Киберпреступление принято считать уголовно наказуемые действия, подразумевающие несанкционированное проникновение в работу компьютерных сетей, компьютерных систем и программ, с целью видоизменения компьютерных данных. При этом компьютер выступает в качестве предмета преступления, а информационная безопасность – объекта. К событиям, связанным с преступлением можно отнести ситуации, при которых компьютер – орудие для свершения преступлений, с целью нарушения авторских прав, общественной безопасности, прав собственности, нравственности. [1]

В зависимости оттого, с какой целью киберпреступник использует компьютерные системы, можно выделить три основных типа киберпреступлений:

- компьютерные преступления, когда компьютер используется как предмет преступления;

- действия, в которых компьютер выступает в роли орудия преступления, например, электронные хищения;

- преступления, при которых компьютер выполняет роль интеллектуальных средств.

Этапы реализации атак:

1) Предварительная разведка.

Если речь идёт о целевой атаке на конкретную компанию, то сначала организатор заказывает у подрядчиков сбор информации об атакуемой компании, которая позволит разработать более правдоподобные схемы социальной инженерии, задействованные на первом этапе атаки.

В случае если речь идёт об атаке на частных пользователей, этап предварительной разведки отсутствует либо ограничивается выбором «целевой аудитории» атаки и формированием фишинговых писем и фишинговых сайтов соответствующего содержания.

2) Заражение.

Проникновение во внутреннюю сеть осуществляется с помощью целевой (spear-phishing) или массированной рассылки фишинговых писем, содержащих в качестве вложения специальным образом сформированный документ или вредоносную ссылку на сторонний ресурс. Открытие вложенного документа или переход по ссылке приводит к инфицированию системы вредоносной программой.

3) Разведка и реализация.

На взломанные компьютеры загружаются программы скрытого удалённого администрирования и управления, используя которые преступники пытаются завладеть учётными данными администраторов систем. Широко используются легальные программы удалённого управления и администрирования, функциональность которых известна многим пользователям.

4) Похищение денег.

На заключительном этапе реализуется доступ к системам взаимодействия с финансами и перевод денег со счетов атакованной организации на счета дроп-проектов, либо снятие денег в банкоматах напрямую. [2]

По прогнозам экспертов «Лаборатории Касперского» число преступников будет только возрастать, что может привести к созданию организованной глобальной группировки.

Атаку на электронные кошельки пользователей и компаний начал троянец ibank (2006), потом появились ZeuS (2007) и SpyEye (2009), затем в группу добавились Carberp (2010) и Carbanak (2013). И это далеко не полный список троянцев, с помощью которых злоумышленники воруют деньги и данные пользователей.

Чем более распространёнными становятся финансовые онлайн-операции, тем привлекательнее для киберпреступников становятся организации, вовлечённые в подобные операции. Последние несколько лет киберпреступники все чаще атакуют не только клиентов банков и интернет-магазинов, но и непосредственно финансовые организации: банки и платёжные системы.

История группы Carbanak, специализирующейся на атаках на банки и раскрытой «Лабораторией Касперского» – наглядное подтверждение этой тенденции. [3]

Эксперты «Лаборатории Касперского» следят за российскими хакерами с самого начала его существования. «Лаборатория Касперского» регулярно выпускает отчёты о ландшафте финансовых киберугроз, которые отражают изменение количества атак, проводимых с помощью финансового вредоносного ПО за определённый период времени. Однако сведения о количестве атак могут обозначить только масштаб проблемы, но ничего больше.

2018 год стал годом стремительного развития программ-вымогателей. По данным «Лаборатории Касперского», за 12 месяцев число пользователей, атакованных подобными программами, выросло в 1,7 раза. При этом Россия оказалась в первой тройке стран, наиболее подверженных риску столкновения с этой угрозой.

Столь высокую популярность у злоумышленников вымогатели снискали, прежде всего, благодаря своей прямой финансовой выгоде: программы блокируют нормальную работу устройства или шифруют данные пользователя с требованием заплатить выкуп за восстановление доступа к ним. Причём все более активно киберпреступники осваивают новые платформы. Кроме того, в уходящем году был обнаружен первый преступник, взломавший Linux.

Наиболее существенный рост демонстрируют программы-шифровальщики в 2018 году с ними столкнулось в 1,5 раза больше пользователей, чем годом ранее. При этом 20% атак шифровальщиков пришлось на корпоративный сектор. Всего за последние 12 месяцев появилось десять новых семейств шифровальщиков, а количество модификаций этих программ увеличилось более чем в два раза. [4]

Отсутствие налаженных механизмов международного взаимодействия также играет на руку преступникам. И наоборот, граждане соседних государств, вовлечённые в преступную деятельность, нередко находятся и действуют на территории РФ.

Инициированное компанией международное расследование деятельности группы Carbanak – первый пример успешного международного сотрудничества, но для серьёзных позитивных изменений таких примеров, несомненно, должно быть больше.

За время, которое существует этот рынок, набор предлагаемых «продуктов» и «услуг» менялся, все более ориентируясь на финансовые атаки, причём на все более и более высоком уровне. Одним из распространённых видов преступлений является оборот украденных данных о платёжных картах. С появлением интернет-магазинов и прочих сервисов, в которых задействованы электронные платежи, большую распространённость получили DDoS-атаки и финансовые киберпреступления, цель которых – либо кража платёжных данных пользователей, либо воровство денег напрямую со счетов пользователей и компаний.

Выявляемые свидетельства инцидента, которые в основном представлены в виде цифровых данных, должны быть собраны и зафиксированы таким образом, чтобы при обращении пострадавшего с заявлением о совершенном в отношении него преступлении, они не вызвали сомнений у следствия и суда.

В процессе реагирования на инциденты компьютерной информационной безопасности и экспертного сопровождения следственных действий и оперативно-розыскных мероприятий приходится работать с большими массивами данных, анализ которых, в совокупности со статистической информацией о вредоносных объектах, выявляет закономерности развития преступного поведения в киберпространстве.

Для киберпреступника сложившиеся условия оказываются очень благоприятными: низкий риск уголовного преследования и потенциально высокий доход, который сулит удачное криминальное предприятие. В результате количество преступлений и ущерб от них растет, а рынок киберкриминальных услуг набирает обороты.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Киберпреступление. [Электронный ресурс]. URL: http://thelocalhost.ru/cyberprest/ (дата обращения: 10.03.2019).

2. Русскоязычная финансовая киберпреступность: как это работает. [Электронный ресурс]. URL: https://securelist.ru/analysis/obzor/27338/russkoyazychnaya-finansovaya-kiberprestupnost-kak-eto-rabotaet/ (дата обращения: 05.03.2019).

3. 5 крупнейших групп киберпреступников из СНГ [Электронный ресурс]. URL: http://www.rospres.com/specserv/17141/ (дата обращения: 05.03.2019).

4. «Лаборатория Касперского» подводит киберитоги года: число жертв атак программ-вымогателей стало больше в 1,7 раза. [Электронный ресурс]. URL: http://www.kaspersky.ru/about/news/virus/2018/number-of-attacks-increased (дата обращения: 11.03.2019).