УДК 004.056

ИНТЕРНЕТ-МОШЕННИЧЕСТВО. СТАРЫЕ И НОВЫЕ УГРОЗЫ*

Е.А. Заплатина, Ю.В. Калинина, Е.А. Еремина, Д.В. Лопатин

В статье рассмотрена актуальная в последнее время информационная угроза – Интернет-мошенничество. Проведен анализ основных видов данной угрозы. Для различных групп пользователей показано к кому ущербу приводит реализация угрозы.

Ключевые слова: информационная угроза, интернет-мошенничество, фишинг.

Проблема мошенничества стремительно перешла в сеть Интернет. Этому способствует с одной стороны онлайн платежные операции с реальными и даже виртуальными деньгами, с другой стороны, привлекательность ИТ-технологий для ввода в заблуждение и скрытия следов преступления. Особую опасность интернет-мошенники представляют для

* Работа выполнена при поддержке гранта РГНФ № 12-16-68005.

неопытных в сфере финансовых операций пользователей. Цель данной работы – провести анализ механизмов реализации информационной угрозы интернет-мошенничество.

Выделяют [1, 2] большое количество видов мошеннической деятельности в глобальной сети, среди них яркими представителями являются фишинг, лотереи, подарочные акции, благотворительность, спам с заманчивыми предложениями, «волшебные аккаунты» платежных систем и все возможные их комбинации. Также мошенники эксплуатируют легальные способы заработка в интернете – фрилансинг (удаленная работа), онлайновые инвестиционные схемы, схемы проведения аукционов и розничной торговли в режиме он-лайн.

Наиболее крупным же стимулятором мошенников представляются деловые операции в глобальной сети. Рассмотрим подробнее такой вид инернет-мошенничества, как фишинг. Фишинг основан на незнании пользователями норм сетевой безопасности, целью которого является получение доступа к конфиденциальным данным, часто финансового характера [3]. Уже в первом полугодии 2011 г. антифишинговая рабочая группа (Anti-Phishing Working Group, APWG) [4, 5] зарегистрировала свыше 112 тысяч фишинговых атак (для сравнения в 2010 г. было зарегистрировано около 70 тыс.). Организованной атаке фишеров могут подвергнуться не только рядовые пользователи, но и руководители компаний. В 2011 г. системы безопасности MessageLabs [6] перехватили порядка 500 электронных писем, адресованных высокопоставленным руководителям известных компаний и организаций, в которых содержались элементы фишинговой атаки.

Фишинговые сообщения, как правило, содержат информацию о сведениях, вызывающих тревогу (например, закрытие банковских счетов); обещаний большой денежной выгоды с минимальными усилиями со стороны жертвы; сведениях о привлекательных сделках; запросах о пожертвованиях от лица благотворительных организаций. Ключевое отличие фишеров от хакеров в том, что они пользуются исключительно обманом доверия граждан. Таким образом, они стремятся получить пароли, коды доступа, номера кредиток и прочую конфиденциальную информацию, в зависимости от ситуации, разными путями. Самый распространенный способ получения доступа к данным банковских карт – имитация рассылки от имени банка или почтовой службы. Под благовидным и волнующим клиента поводом (например, тестирование нового ПО или восстановление базы данных, верификации данных) у пользователя запрашивается ключевая информация, которую нередко клиенты отправляют мошеннику.

В более сложном варианте создается точная копия официального сайта реально существующего банка, интернет-магазина или платежной системы. При этом либо пользователь изначально попадает на фишинговый сайт, либо встраивается фишинговая ссылка в подлинный сайт. В любом случае пользователь переход на сайт-имитатор. Подобный механизм был реализован группой мошенников, которая похищала денежные средства клиентов банка ВТБ24, разработав для этого копию оригинального web-сайта для удаленного банковского обслуживания [7].

Другим видом интернет-мошенничества являются так называемые «волшебные аккаунты» или «волшебные кошельки» платежных систем. Через спам, сообщения на форуме, комментарии в блогах, гостевые книги, объявления или каким-либо другим способом человек узнает про существование так называемых «волшебных» кошельков, которые работаю по принципу финансовой пирамиды. Длинные циклы увеличения сумм невыгодны мошенникам, вследствие чего пользователь теряет деньги либо сразу, либо через первый или второй перевод денег на «волшебный кошелек».

Мошенники часто используют интернет для рекламы предполагаемых деловых возможностей, которые якобы позволят пользователям зарабатывать большие денежные средства при помощи «надомной работы». В таких схемах обычно предусмотрен первичный платеж, но не предоставляются материалы или информация, необходимые для того, чтобы надомная работа стала потенциально жизнеспособным предприятием, приносящим прибыль.

Преступники в интернете используют два основных метода манипулирования рынками ценных бумаг для получения личной выгоды – онлайновые инвестиционные махинации. Во-первых, на ресурсах, близких к интернет-биржам, злоумышленники распространяют ложную и вводящую в заблуждение информацию о росте и падении котировок,

стремясь вызвать резкое повышение цен на определенные заранее приобретенные акции, вслед за этим они продают принадлежащие им акции. Естественно, покупатели акций не осведомлены о мошенническом характере информации. Второй метод онлайн-махинаций реализуется как финансовая пирамида, где пользователям предлагается вложить деньги в проект, приносящий колоссальные проценты ежемесячно. Как известно, вклад средств в такие проекты гарантирует прибыль только верхушке финансовой пирамиды.

Отдельный интерес представляют мошеннические предложения, фигурирующие на сайтах онлайновых аукционов. В таких схемах, а также аналогичных махинациях в области розничной торговли, обычно предлагаются дорогостоящие товары, которые могут привлечь много клиентов. Мошенники предлагают своим жертвам выслать деньги в оплату обещанного товара, затем либо крадут деньги, либо доставляют подделку или другой товар.

Тамбовский регион не является исключением. Практически каждый день в сводке преступлений и происшествий управления МВД России по Тамбовской области регистрируются факты интернет-мошенничества. За 1-й квартал 2012 г. зафиксировано более 70 мошеннических действий со стороны злоумышленников [8]. «Местные» мошенники реализуют различные механизмы [9], например, могут играть на искренних чувствах пользователей, регистрируя себя в социальных сетях под именем остронуждающихся в средствах людей без их ведома, организовать разного рода благотворительные компании.

Подводя итог, авторы констатируют, что сегодня интернет-мошенничество – одно из основных экономических угроз в интернет-пространстве, намечается рост как количества видов интернет-преступлений, так и число их жертв. Необходимо привлекать к проблеме интернет-мошенничества внимание сетевого сообщества, разрабатывать новые и действенные механизмы безопасности, развивать культуру компьютерной безопасности пользователей.

Литература

1. Основные интернет-мошенничества [Электронный ресурс]. URL: http://www.wmchat.ru
2. Мошенничество в Интернете [Электронный ресурс]. URL: http://avail.ucoz.ru
3. Фишинг [Электронный ресурс]. URL: http://www.saferunet.ru
4. Фишинг: количество сайтов-ловушек растет [Электронный ресурс]. URL: http://nskpc.ucoz.com
5. APWG: Увеличение роста числа фишинговых атак [Электронный ресурс]. URL: http://it-sektor.ru
6. Кибермошенники атакуют руководителей компаний [Электронный ресурс]. URL: http://www.securitylab.ru
7. Фишеры из Петербурга похитили 13 миллионов рублей [Электронный ресурс]. URL: http://www.securitylab.ru
8. Как нас обманывают мошенники и как не стать их жертвой [Электронный ресурс]. URL: http://www.tmbtk.ru
9. Тамбовские полицейские задержали мошенника из социальной сети «Одноклассники» [Электронный ресурс]. URL: http://www.vesti-tambov.ru