Недавно я решил продать гараж. Разместил объявление в Интернете, где из личных данных указал только номер сотового и собственное имя, чтобы удобнее было общаться с потенциальными покупателями. Казалось бы, в чем риск?
Я вполне грамотный человек, прессу читаю… Поэтому сразу прервал все разговоры с мошенниками, пожелавшими не глядя приобрести мою недвижимость, только бы я им сообщил реквизиты своих банковских карт. Таковых «умников» нашлось аж пять человек. Потом нашелся, вроде, настоящий покупатель, с которым договорился о встрече. Правда, меня смутил номер его сотового, явно зарегистрированный не в нашем регионе, но мужик задавал много вопросов по делу, никаких сомнительных предложений не высказывал. Замысел афериста открылся, когда по дороге на встречу мне перезвонил потенциальный покупатель и попросил перечислить на номер его сотового телефона пару-тройку тысяч. Уже не помню, что он мне плел, но отвечать на его звонки с этого момента я перестал. Ближе к вечеру, когда проснулась средняя полоса России и Европа, мне стали поступать sms примерно одинакового содержания. Вот одно из них: «Ув. Иван, по обяв-ю, обмен возможен? Фото: http://foto3o/biz» Я преднамеренно не указываю полностью адрес ссылки, дабы никому из читателей не пришло на ум пройтись по ней. Дело в том, что данное, на первый взгляд, вполне невинное предложение содержит в себе вредоносный вирус.
Тут как раз пресс-служба краевого УМВД сообщила, что трое камчатцев стали жертвами интернет-мошенников, распространяющих по электронной почте вложения, содержащие опасные вирусы. Наверняка, активных пользователей Интернета поразила смехотворная цифра пострадавших. Скорее всего, это количество тех, у кого лопнуло терпение, и они вознамерились хотя бы попытаться найти и наказать злоумышленников. Во всех случаях отправителем значился «Сберегательный банк», поскольку это крупнейшее финансовое учреждение страны и вероятность «попадания» на его клиента значительно выше, чем других банков. В письме содержалось сообщение, что на владельца электронной почты был оформлен кредит на сумму 500 тысяч рублей, по которому имеется задолженность, в связи с чем составлен иск в суд. К письму прилагались файлы «Судебный иск», «Договор займа». Потерпевшие скачали их на свои компьютеры и запустили вирус.
Зачастую, это вирусы-шифровальщики, которые кодируют и делают недоступными находящиеся на компьютере пользователей файлы с «популярными» расширениями: .doc, .docx, .xls, .xlsx, .pdf, .jpeg, .jpg, а также некоторых программ, используемых в бухгалтерских учетах и т.п. Рядом с ними вредоносная программа создает текстовое сообщение, в котором злоумышленники предлагают за определенную плату приобрести у них расшифровщик, который позволит вернуть файлам первоначальный вид.
Данные технологии используются злоумышленниками для внедрения в систему вредоносного кода скрытно, не привлекая внимания владельца компьютера. Осуществляется это через уязвимости в системе безопасности операционных систем и в программном обеспечении. Наличие уязвимостей позволяет изготовленному злоумышленником сетевому червю или троянской программе проникнуть в компьютер-жертву и самостоятельно запустить себя на исполнение.
В настоящее время написание вирусов и вредоносных программ стало превращаться в индустрию отъема денег, причем не только у обычных домашних пользователей, но и у работников известных компаний. При этом активность киберпреступников растет год за годом, и сейчас можно говорить о настоящей «гонке технологий», которая развернулась

между антивирусной индустрией и индустрией вирусной. Одновременно растет количество хакеров-индивидуалов и преступных групп, а также их профессионализм. С каждым годом вирусные программы усовершенствуются и, проникнув в ваш компьютер, начинают активно размножаться и распространяться по сетям. Чтобы компьютер был хорошо защищен от проникновения такого рода программ, придется потратить некоторые средства на программы защиты. А еще, как посоветовали в краевой полиции, не запускать файлы, прикрепленные к электронным письмам, даже от знакомых людей, если ранее об этом не было договоренности.

Иван ТИМОФЕЕВ.