



Визитка

МИХАИЛ КАЛИНИЧЕНКО,
генеральный директор компании StarForce Technologies

Они – не Робин Гуды

Их можно уважать за ум, но не за поступки

Безусловно, звание хакера несет в себе некий налет романтики. Сразу вспоминается Робин Гуд, который грабил богатых, чтобы отдавать деньги бедным. Но сегодня хакерство в основном – это криминальное действие. Ведь хакеры портят результаты иногда многолетней работы других людей, из спортивного интереса ломают программное обеспечение или получают доступ к секретным данным.

Например, после взлома программного обеспечения разработчик или издатель получает намного меньший доход, который мог бы пойти на внедрение новых фиш или создание и продвижение современных продуктов. Особенно пагубно хакерство отражается на индустрии компьютерных игр: многие талантливые разработчики популярных игр разорились, потому что их создание сегодня недешево. Хотя то же можно сказать и про другое программное обеспечение. Например, в конце 2008 года на портале Snews.ru появилось сообщение о взломе одного из самых популярных в России картографических приложений. Это привело к падению продаж на 15%.

Конечно, хакеров можно уважать за их ум и способность решать сложные технологические загадки, но не за то, что они делают и какой вред приносят. В то же время нужно разделять хакерство как профессиональный вид деятельности и как стиль жизни и способ получения доходов. Уровень пиратства зависит и от административных мер наказания, и от менталитета населения. В благополучных европейских странах процент пиратства меньше, в азиатских странах больше. Однако не секрет, что в разных странах спецслуж-

бы создают специальные подразделения по борьбе с кибертерроризмом. По сути, сотрудники таких подразделений нередко являются профессиональными хакерами. Поэтому говорить, что хакер – это однозначно плохо, неправильно, ведь многие из них состоят на службе государства.

Наша компания косвенно сталкивается с хакерами каждый день. Потому что ее основная цель – защита наших клиентов, а точнее, их программного обеспечения от взлома.

Защищать информационную сеть компании следует сразу комплексом мер. Конфиденциальные документы нужно защищать от нелегального открытия, распространения и копирования. Для этого есть специальные инструменты защиты, которые не позволяют открывать защищенный электронный документ в обычно используемых программах. Чтобы открыть защищенный документ, необходимо иметь специальный выювер, серийный номер и собственно документ. Человек, защитивший документ, сможет увидеть отчет по активации документа. Для безопасной же работы сети нужно использовать обязательно и антивирусное программное обеспечение, и проактивную защиту, и защищенные корпоративные приложения.

Сегодня проблема борьбы с хакерством заключается не столько в несовершенстве законодательства РФ, сколько в средствах и институтах контроля над выполнением законов. Например, в Уголовном кодексе прописано, что взлом защищенного приложения с последующей продажей программы является уголовно наказуемым преступлением. Однако на деле этот закон выполняется нечасто. **БОФ**

ТОП10 крупнейших хакерских атак (2008-2009 гг.)

Apple iPhone. Механизм защиты Apple, который «привязывал» каждый смартфон к отдельному оператору мобильной связи, оказался несостоятельным. Во многих странах мира продавались «Айфоны» без защиты, а Интернет полон хакерских прошивок.

Goldman Sachs. Проживающий в США эмигрант Сергей Алейников совершил кражу программного обеспечения банка Goldman Sachs. Это код системы, которая считалась одной из самых совершенных способов торговли на фондовых биржах в режиме онлайн. Ущерб составил порядка миллиона долларов.

Гарвардский университет. Взломав серверы университета, хакеры по-

лучили доступ к персональным данным десятков тысяч студентов. Помимо прочего, там хранились номера полисов социального страхования, с помощью которых можно оформить кредит или даже сделать новую кредитную карточку.

Город Вэйфан. Из-за хакерских атак сервера фирм-провайдеров китайского города Вэйфан были недоступны в течение двух суток. Все это время 400 тысяч пользователей не имели доступа к Интернету. Это самый масштабный сбой работы провайдеров в истории.

Bank of Scotland. Хакеры взломали компьютерную систему банка и получили сведения о полутора миллионах клиентов. Создали клоны карт и наняли людей, которые с фальшивыми копиями могли забирать деньги из банкоматов. Ущерб банка составил 9 млн долларов, организаторы не найдены.