ХАКЕРЫ: «ПОГОДА» НА ЗАВТРА

Арсений
Замостьянов

Слово «хакер», которое появилось в русском языке, стало буревестником больших перемен. Тогда, в начале девяностых, на телезрителей и читателей газет и журналов посыпались: брокеры, дилеры, спикеры, риэлторы, дистрибьютеры, бесконечные менеджеры и супервайзеры лизинга, а также всяческого франчайзинга... Диковинные звуки подчас отвлекали общество от криминального лица героев нового времени. Так, вместо привычных «капиталовложений» появились хитрые «инвестиции». Эти буревестники перемен для тысяч и тысяч российских семей обернулись стервятниками. В то же время страну охватила компьютеризация. Упростившийся язык программирования стал родным для детей девяностых. Ребята, выросшие с пластмассовой «мышью» в руке, оказались куда более сведущими в этих премудростях, чем их отцы и деды. Труд и развлечения (последних всё-таки было больше), связанные с компьютером, стали паролем молодого поколения. Конечно, компьютеризация общества — явление сложное, неоднозначное, но если говорить о его криминальной стороне, то не обойтись без изучения феномена хакерства.

Хакеры — радикальные рыцари компьютерной субкультуры по навязчивости своего арго могут поспорить с беспризорниками двадцатых. Овеянные романтикой риска, они обогащают (или засоряют?) русский язык новыми понятиями, пытаясь заявить о себе прочно, всерьёз и надолго. Что-то важное незаметно изменится в окружающем мире, когда мы станем привычно употреблять в обыденной жизни глагол «хакнуть». Такие слова утверждают право на существование опасной и модной «профессии». Модной во многом в силу ореола запретности, тайны. Мы представляем малую часть хакерского сленга, который красноречиво рассказывает о своих юных апологетах:

Компьютер – комп, тачка, железный друг, железный конь.

Клавиатура – клава, кейборд.

Мышка – мышь, крыса, маус.

Коврик для мыши – мышкодром, крысодром.

ОЗУ – память, мозги, димы, симы, римы.

Винчестер – хард, винт, жестянка, блин, хардрайв.

Материнская плата – мамка, мать.

Монитор – монька, моника, моня, экран.

CD-ROM – сидюк, подставка для кофе, вертушка.

Шнур – интерфейс, шнурок.

Парень – перец, крендель, дядька, амиго, пельмень, чел.

Девочка – пельмешка, матрёшка, лапочка.

Хакер – хацкер, ксакеп, 31337, Ветеран 139-го порта.

Положительные эмоции – описюнительно, рулез, кул, зашибись, в шоколаде, рулит, мегаваттно, колбасит.

Отрицательные эмоции – отстой, сакс, не фантан, сукс, шняга, гимор, подстава.

Почтовый клиент – мейлер, мылер, почтовик, почтальон.

Послать письмо – замылить, намылить, мыльнуть, отмылить.

Скачать что-нибудь – слить, залить.

Интернет – инет, сеть, паутина.

Игрок – гамер, геймер, гейм бой, квакер.

Играть – гамиться, рубиться.

Игра – гамес, игруха, гама.

Пользователь – юзер, юзверь, юзарь.
Использовать что-то – юзать, поиметь, поюзать, пощупать.
Какое-то действие хакера – хачить, ломать, крякать.
Украсть – скомуниздить.
Найти – наковырять, надыбать, нарыть.
Доллары – баки, баксы, зелёные, крокодилы, зелень, американские президенты, зелёные президенты, грины, баказоиды, вечнозелёные.
Деньги – бабки, лавэ/лавэшки, бабло.
Прозвище – ник, кликуха, никнейм.
Не работает – глючит, бажит, двинула кони, склеила ласты.
Наплевательски отнестись – забить, положить, задвинуть.
Развлекаться – отрываться, отлетать, угорать, торчать, кайфовать, колбаситься, зажигать, оттягиваться.
Сумасшедший – крэзи, шизо, шибанутый, гость из Белых Столбов, мэдди.
Обидеть – поиметь, натянуть, вздрючить, кинуть, обломать.
Врать/обманывать – прогонять, гнать, заливать, мозги тараканить.
Думать – включать мозгу.
Встретиться – сконнектиться, законнектиться.
Старый – поюзаный, юзаный, битый, древний.
Программировать – кодить, шкодить.
Что-то необычное – фишка, фенька, феня.

А теперь — несколько сюжетов из криминальной хроники, связанной с деятельностью юных хакеров. Самое невинное развлечение — это, конечно, оплата собственных развлечений (в том числе — и компьютерных) из чужого кармана. Вот сюжет из новостной ленты 2005 года:

...По словам Евгения Ялдышева, заместителя прокурора Тюменского района, в ноябре прошлого года железнодорожная больница станции Тобольск, имея по телефону доступ в Интернет, стала получать завышенные счета от «Уралсвязьинформа» за пользование этой услугой. Пока деньги были невелики, руководство организации оплачивало расходы. С каждым месяцем счета всё увеличивались. Бухгалтер больницы, заподозрив неладное, запросил у провайдера распечатку пользователей. Там фигурировало до десятка различных телефонов.

Оперативники отдела «К» живо отреагировали на заявление бюджетной организации и вскоре вычислили владельцев телефонов. Самым активным «телефонистом-захребетником» оказался 19-летний студент Тюменского колледжа связи, информатики и управления, живущий в посёлке Винзили Тюменского района. Он активнее всех посещал Интернет за счёт больницы. Парня взяли дома. В его компьютере было найдено соединение с поликлиникой.

Под гнётом улик парень рассказал, что с осени прошлого года скопировал программу «переборщик паролей», нашёл способ взломать код больницы-пользователя и стал посещать Интернет за её счёт. Начал с семи рублей в день. На момент задержания парнишка до того осмелел, что зависал в сети на 130 рублей в сутки. В общей сложности ущерб больнице от его вторжения составил 1309 рублей. По самым скромным подсчётам хакер взломал коды около 50 организаций и пользовался услугами Интернета за их счёт. Из-за малочисленной суммы многие потерпевшие организации не стали обращаться за помощью в правоохранительные органы.

Чтобы как-то загладить свою вину, молодой человек возместил ущерб больнице. Но всё равно он будет привлечён к уголовной ответственности по статье 165 УК РФ «Причинение имущественного ущерба собственнику путём обмана без признаков хищения». Такое преступление считается тяжким и равноценно краже с незаконным проникновением в жилище. И наказание за него полагается нешуточное — до шести лет лишения свободы.

Кстати, он поделился криминальным опытом со своим однокурсником, который таким же способом стал взламывать коды доступа организаций в глобальную сеть. Теперь и в отношении его деяний возбуждено уголовное дело.

Год назад на всех языках мира звучало имя хакера Джозефа Макэлроя, из шалости державшего в панике секретные службы Соединённых Штатов:

...Британский хакер взломал код доступа в сверхсекретную американскую военную лабораторию, вызвав панику в рядах учёных и военных. Американцам показалось, что ядерной лаборатории грозит террористический акт.

Восемнадцатилетнего Джозефа Макэлроя, который в сети был известен как Deathserv, подвела щедрость. Ему удалось незамеченным проникнуть сквозь электронные системы безопасности и сгенерировать пароль доступа, который позволил ему незаметно хозяйни-

чать в компьютерах лаборатории. Американским военным из Fermi National Accelerator Laboratory (штат Иллинойс) повезло: юному Макэлрою не нужны были секретные данные, мощной сетью лаборатории он пользовался только для того, чтобы качать фильмы и музыкальные файлы MP3 из Интернета.

Однако он не только сам пользовался этим паролем, но и раздал его всем своим друзьям, и те стали качать столько файлов, что перегрузку сети заметили рядовые сотрудники лаборатории. Только тогда на это обратили внимание службы безопасности и Deathserv был пойман. Правда, до этого момента вся лаборатория жила в страхе из-за вполне реальной опасности теракта.

Как сообщает Daily Telegraph, Джозефу очень повезло на суде: ему удалось избежать тюремного заключения, судья приговорил его к 200 часам общественных работ, так как в момент взлома пароля лаборатории ему было всего 16 лет.

Другое развлечение рыцарей «компа и клавы» связано с более злыми умыслами. Речь идёт о рассылке вирусов, которыми «награждают» ни в чём не повинных пользователей сети Интернет ради хакерского самоутверждения. Одна из самых громких историй связана с вирусами «Я люблю тебя» и «Анна Курникова». Любопытно, что толчком для создания вируса «Анна Курникова» послужило безумие вокруг идола массовой культуры, новоявленного секс-символа. Безусловно, манящий глянцевый мир стал контекстом работы многих хакеров.

Ответственность за создание и распространение почтового вируса «AnnaKournikova» взял на себя голландский хакер OnTheFly. Подобно другим почтовым вирусам, таким, как Melissa или ILOVEYOU, «AnnaKournikova» представляет собой электронное письмо, к которому приложен файл, с первого взгляда напоминающий изображение в формате jpeg (файл-картинка), однако на самом деле являющийся скриптом на языке Visual Basic. Чтобы привести вирус в действие, пользователь должен собственноручно запустить его. «AnnaKournikova» почти безвреден, единственное, что он делает, — отсылает свою копию по всем адресам из адресной книги Outlook. В понедельник вирус попал во все новости, всего за несколько часов с огромной скоростью распространившись по всему миру.

По словам автора вируса, его целью было проверить, насколько беспечно люди относятся к опасности заражения почтовыми вирусами. «На прошлой неделе я прочёл в одной статье про какие-то исследования влияния вируса LoveLetter, — сообщил он в интервью Wired», — Статья была озаглавлена: «Пользователи Интернета ничему не научились на примере вируса ILOVEYOU». Однако даже он был удивлён, узнав из новостей, насколько успешно прошёл его «эксперимент». «Вирус распространялся очень быстро, верно? — говорит OnTheFly, — На самом деле я не ожидал такого!»

OnTheFly уверяет, что никому не собирался причинять вреда. «Я уверен, что никогда в будущем не стану писать или распространять вирусы снова, — заявил он — Не знаю, почему эти невежественные люди продолжают открывать такие письма. В конце концов, если их компьютер оказался заражен вирусом AnnaKournikova, — вина полностью на них самих».

Автор вируса испытывает тёплые чувства по отношению к теннисистке Анне Курниковой, и именно поэтому решил назвать вирус в её честь. «Просто потому, что я её большой фанат, — поясняет он, — Она заслуживает некоторого внимания, верно?»

Информационное общество, погружённое в хитросплетение современных технологий, уязвимо перед сетевыми преступниками. Их шалости способны парализовать деятельность самой влиятельной организации, а то и жизнь целого города. То и дело имена российских хакеров мелькают в мировой прессе:

...Суд города Сиэтл (США) приговорил российского гражданина Василия Горшкова, обвиняемого в компьютерном мошенничестве, к трём годам лишения свободы и штрафу в размере $700 тыс. в пользу компаний, пострадавших от его действий. Арестованный вместе с Горшковым другой российский хакер Алексей Иванов ждёт своего суда в тюрьме штата Коннектикут.

Хакеры Горшков и Иванов обвиняются в похищении и незаконном использовании номеров нескольких десятков тысяч кредитных карт клиентов американских платёжных систем и электронных банков, в частности Pay Pal. Хакеры использовали украденные номера кредиток «для получения наличности и оплаты компьютерных комплектующих в Интернет-магазинах». При этом дело не ограничивалось мошенничеством; как считают американские правоохранительные органы, Василий

Горшков и Алексей Иванов виновны во взломе сайтов нескольких компаний с целью вымогательства. После взлома «компьютерные гении» из Челябинска связывались с руководством фирм и предлагали за плату закрыть сделанные ими же дыры в системе безопасности.

ФБР вышло на след преступной группы в 2000 году. Детали операции по их задержанию и степень участия в нём российских МВД и ФСБ держатся в тайне, однако в общих чертах она выглядела так: создав в Сиэтле подставную компанию по компьютерной безопасности Invita, агенты ФБР выступили в качестве работодателей Горшкова и Иванова и пригласили их на работу в США. В офисе компании сотрудники ФБР предложили программистам продемонстрировать свои навыки по взлому сайтов, что россияне и сделали, после чего были арестованы.

Рассмотрение дела русских хакеров обернулось международным конфликтом ФБР и ФСБ. Адвокат Горшкова обвинил агентов ФБР в получении улик против своего подзащитного незаконным путём. Сотрудники ФБР запустили на тестовом компьютере Invita программу-шпион, отследившую пароли челябинца, которые тот вводил для входа на свой компьютер. После ареста один из представителей ФБР «побывал» на компьютере Горшкова и скопировал программы и куски кода (исходные материалы для написания программ), которые затем послужили решающим доказательством в суде. После этого весной 2002 года челябинское УФСБ объявило о возбуждении против агента ФБР Майкла Шулера (Michael R. Shuler) уголовного дела по факту незаконного проникновения в компьютер, находящийся на территории РФ. Согласно существующей между двумя спецслужбами договорённости, ФБР должно было сначала направить в ФСБ запрос о проведении обыска. Этого сделано не было, и действия Шулера квалифицировались как взлом российских компьютерных систем. Однако госдепартамент США посчитал действия агента вполне законными.

Второй подозреваемый по делу русских хакеров, Алексей Иванов, пока находится под следствием в штате Коннектикут. Его дело более сложное: именно он считается инициатором преступных деяний. В настоящее время делом Иванова занимаются судебные органы пяти штатов, в которых располагаются компании, ставшие объектами хакерских атак.

Разумеется, юных хакеров нередко вовлекают в большие криминальные операции, когда требуются их знания и сноровка. Их имена встречаются и в уголовной хронике, апогеем которой стало сенсационное убийство свидетеля.

...В феврале этого года в США преступникам удалось изменить режимы работы аппарата искусственной вентиляции лёгких и кардиостимулятора у пациента одного из госпиталей ФБР, проникнув через Интернет в информационную сеть больницы. Важный свидетель, которого ФБР специально прятало в закрытой клинике, умер. Правда, уже летом американские сыщики вычислили хакера-убийцу...

Мы обречены жить в мире высоких технологий. Это подразумевает особую опасность именно *технологических* преступлений, в которых наиболее опасны вундеркинды, чьи технические способности значительно обгоняют моральную зрелость, да и просто благоразумие. Хроника хакерских преступлений — это своеобразный прогноз погоды на завтра. Сегодня злоумышленнику не составляет труда вовлечь молодых людей в преступление. Задача общества — максимально затруднить этот процесс, объясняя юным программистам, что любое, даже самое высокотехнологичное, преступление карается законом без снисхождения. И преступная хакерская деятельность не остаётся безнаказанной. **НО**