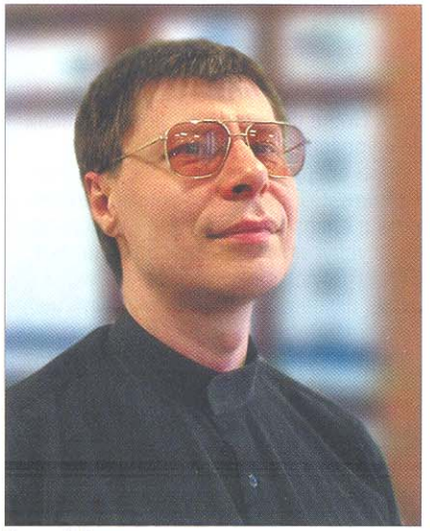
"Ловить злохакеров экономически невыгодно"

Тема киберпреступности и перспектив борьбы с нею сегодня волнует многих. Своим мнением на сей счет с читателями PC Week/RE делится ***Николай Федотов****, специалист по компьютерной криминалистике, главный аналитик компании InfoWatch.*

Не преувеличивается ли сегодня опасность компьютерных преступлений?
Преувеличения наблюдаются в основном в художественных произведениях, где ради драматизма злохакерам приписывают почти магические возможности. В связи с мощной компьютеризацией всей нашей жизни слишком много данных стало доступно через компьютеры и сети. Теоретически доступно. Однако на практике компьютерные преступления направлены не на любую конфиденциальную информацию, а ограничиваются лишь наиболее рентабельными её типами. Ведь на 95% защищаемой информации никто даже не пытается посягать. Потому что продать её нельзя, невыгодно или хлопотно. Или потому, что теми же усилиями можно достать более дорогую и более ликвидную информацию.

Какая же информация пользуется наибольшим спросом при совершении компьютерных преступлений?
Разумеется, та, которую легко обратить в деньги. Атрибуты банковских карт, пароли к платёжным системам, игровым аккаунтам. На чёрном рынке США хорошо сбываются номера соцстрахования (SSN). Прочая информация составляет незначительный процент чёрного рынка.

А если злоумышленник крадёт не информацию, а напрямую деньги? Может хакер обокрасть банк, например?
Упрощённо говоря, не может. Если у него нет сообщника в банке, причём среди ответственных, доверенных работников. Если же такой сообщник есть, то в принципе можно обойтись и без хакера.
Или возьмём, например, подложные кредиты. Много сетований, что, дескать, зная некоторые персональные данные или имея копию паспорта, мошенники могут оформить такой кредит, а субъект персональных данных будет вынужден его отдавать или получит иные неприятности — страшилка, имеющая мало общего с действительностью. Простого знания данных вкупе с копией паспорта в России недостаточно даже для самого незначительного кредита. Необходимы ещё фальшивые документы весьма высокого качества или подкуп нескольких работников банка. Фальшивки обычно стоят дороже суммы кредита, которую можно под них получить (банки хорошо умеют просчитывать риски), а при наличии коррумпированных должностных лиц за сканами паспортов никто охотиться не станет — их в любом банке навалом.


Николай Федотов

Но считается, что информация об имуществе граждан используется ворами и грабителями для выбора жертвы...
Используется. Только она обычно влияет именно на выбор объекта, а не на то, будет ли совершено преступление. Доступность персональных данных об имуществе не повышает вероятность преступлений. А всего лишь перераспределяет такую вероятность на более состоятельных граждан. С точки зрения общественной опасности — неоднозначная ситуация. Не уверен, что стоит вкладывать ресурсы государства в защиту такой информации ради обратного перераспределения, когда можно те же ресурсы потратить на поимку воров и грабителей.

А насколько эффективно вылавливаются компьютерные злоумышленники?
В развитых странах — достаточно эффективно. Профессии кардера, вирмейкера, фишера и спамера, по нашим оценкам, приносят доход лишь немного выше, чем зарплата "штатского" айтишника той же квалификации при несравнимо большем риске. В России доходы киберпреступников также чуть выше среднеайтишных, но риск существенно ниже из-за неэффективности правоохранительных органов (и в сфере высоких технологий особенно).

А вы сами не думали перейти на тёмную сторону Силы?
Думал, конечно. Но я, в отличие от среднего киберзлоумышленника, знаю обе стороны медали. И могу оценить риск более полно. Всё-таки честно работать сегодня выгоднее. К тому же синхронно с ростом доходов киберпреступников растут и расходы на защиту от них, следовательно, доходы киберкриминалистов и информзащитников.

Есть мнение, что большинство киберпреступлений расследовать невыгодно: на мероприятия тратится намного больше денег, чем можно вернуть украденных. Это действительно так?
С экономической точки зрения расследование большинства преступлений невыгодно. Государству было бы дешевле возмещать потерпевшим стоимость похищенного и уничтоженного преступниками, чем содержать правоохранительный аппарат. Но дело здесь не в возмещении. Опасность преступлений не сводится к материальному ущербу; такие ценности, как свобода, достоинство личности, здоровье и жизнь, — не сводятся к деньгам. Кроме того, неподавляемая преступность очень скоро станет претендовать на власть в стране, с этим ни одно государство мириться не намерено. Поэтому, невзирая на нерентабельность, борьба с преступностью ведётся из принципиальных соображений. Киберпреступления тут не исключение. Ловить злохакеров экономически невыгодно, поэтому такую задачу нельзя поручать частным службам безопасности — у них есть возможности, но нет стимула.
Возьмём простой пример. Кардеры провели несанкционированную операцию по чужой карте. Держатель карты об этом вовремя узнал и обращается в банк, чтобы сделали возврат платежа (Chargeback). Что ему ответит банковская служба безопасности? Первым делом постарается убедить, что он сам виноват, а возвращать деньги ему "не положено". Хотя на самом деле очень даже положено. И по договору, и по правилам международной платёжной системы, которым все банки подчиняются. Более того, в случае возврата платежа банк-эмитент карты своих денег не теряет, он получает их назад от банка-эквайрера, а тот — от продавца. По подложной транзакции деньги потеряет продавец, продавший кардеру товар (услугу), прочие участники цепочки должны получить возмещение ущерба. По идее.
По факту же сама операция по возврату платежа и расследованию мошеннической операции обходится участникам настолько дорого, что дешевле компенсировать украденное держателю карты из собственных средств. Что иногда и делают, если потерпевший не поведётся на вышеупомянутые "сам виноват" и "не положено".
Сама система построена так, что ей выгодно скрывать мелкие хищения. Профессиональные кардеры этим пользуются, не совершая слишком крупных и слишком частых операций. И потому благополучно существуют на протяжении более 30 лет.
У спамеров и вирусописателей такой удобной экономической ниши нет.

Не является ли такая терпимость к кардерам исключением из правил? Вот, например, к спаму и спамерам в ИТ-сообществе наблюдается просто какая-то безграничная ненависть.
Киберпреступники, как и, к примеру, всякие паразиты, не заинтересованы в гибели организма-хозяина. И стараются причинять ему меньше беспокойства и брать от него в меру. Стараются, но не у всех выходит. Вот, в частности, вредоносные программы за последние годы сильно "подобрели" к зараженным компьютерам. В 1990-е почти все вирусы выводили из строя ПО инфицированной машины. Во всяком случае старались.
А ныне современные вредоносы (агенты ботнетов) маскируются, пытаются не выдать своего присутствия, а захваченные ресурсы (производительность компьютера, место на диске, полосу канала связи) стараются использовать в меру, чтоб пользователь не чувствовал неудобств.
Их усилия оправдались: заразившиеся пользователи и их провайдеры сейчас не слишком заинтересованы в антивирусной защите. Приходится её буквально навязывать. А при обнаружении заразы — долго убеждать провайдера и пользователя предпринять меры и грозить им дискоммуникацией. Потому как носители ботнета почти не несут ущерба, страдают все остальные.
Спамерам же так и не удалось найти компромисс с получателями навязчивой рекламы. Взломщики платёжных систем и фишеры также не сумели приспособиться. С ними идёт борьба со всех сторон, у них земля горит под ногами.

Для криминалиста преступная среда — объект изучения. Вы, будучи криминалистом, заводите там знакомства? Имеете какие-то дела с "чёрными шляпами"? Оказываете юридические консультации подозреваемым и обвиняемым в компьютерных преступлениях?
Для криминалиста и жертва — тоже объект изучения (раздел криминалистики, изучающий жертв преступлений, называется виктимология). Но становиться жертвой преступления "ради науки" никто не спешит. Связи с киберпреступниками, конечно, неизбежно образуются. Как и связи с правоохранительными органами. Правда, на тусовки киберзлодеев меня не зовут. А вот на судебные процессы в качестве специалиста — приглашают. В половине случаев инициатива исходит от стороны защиты. Как и большинство, о защите вспоминают, когда уже поздно.

Вы намерены и дальше работать в компьютерной криминалистике? Или видите более перспективные области?
Наша область очень перспективна. Спрос сильно превышает предложение. Правда, далеко не весь спрос — платёжеспособный. Много консультаций приходится давать бесплатно. Но с каждым годом рынок увеличивается.