

«Воруют все, что можно украсть»»



Пожалуй, найдется немного имен IT-специалистов, которые были бы на слуху и у профессионалов, и у обычных пользователей. Исключение — Евгений Касперский, создатель «Лаборатории Касперского», чей самый известный продукт — антивирусная программа, завоевавшая популярность не только в России, но и далеко за ее пределами.

Евгений, не могли бы Вы немного рассказать о том, как создавалась Ваша самая известная разработка — Антивирус Касперского?

Коротко вряд ли получится, потому что история достаточно длинная, ей уже 16 лет. Все произошло случайно, я работал в одном из институтов Минобороны Советского Союза. И мой компьютер вдруг начал вести себя странно: буквы стали сыпаться по экрану. И я подумал, что это, видимо, вирус Cascade. А к тому моменту уже было известно, что это такое, существовало около 10 антивирусных программ на тот момент (1989 год). Я полечил свой компьютер, но один файл сохранил, чтобы потом с ним поиграться, посмотреть, как работает этот вирус. Мне просто это было интересно. А это любопытство потом превратилось в хобби, потому что потом был второй, третий, деся-

тый, пятидесятый вирус. Многие из них были разные, и было любопытно смотреть, как работают всяческие вирусные алгоритмы, что из этого получается. И одновременно с этим мне было очень любопытно написать программу, которая бы восстанавливала зараженные файлы в их исходное состояние. Это продолжалось года два, за это время я успел несколько статей написать, на конференциях выступить, оказалось, что это хобби у меня занимает все больше и больше времени, и в 1991 году я решил, что пора этим заниматься профессионально. К тому же это был расцвет кооперации, появлялись разные компании, в одну из которых я и пошел работать в специально созданный для этого антивирусный отдел, который состоял из одного человека — меня. Я быстро понял, что один такую работу тянуть не в силах, и появился у меня помощник, потом второй, третий. И к

1997 году у нас было, по-моему, человек 19. Мы зарегистрировали независимую компанию, куда и перешел весь отдел, который занимался антивирусными разработками. Сначала нам было очень тяжело, потому что денег было совсем мало. Но год за годом мы строили свою дистрибьюторскую партнерскую сеть, развивали наш бренд в России, затем начали международную экспансию. Сегодня в компании почти 400 человек, офисы у нас в США, Англии, Германии, Франции, Голландии, Польше, Румынии, Японии, Китае, может, что-нибудь и забыл. Партнеры у нас по всему миру. Можно сказать, что у нас международный бизнес, уникальный, построенный с нуля, без внешних инвесторов, который достаточно динамично развивается, что показала выставка СЕБИТ 2005. К нашим продуктам и павильонам большой интерес, всегда толпа народа совершенно разных национальностей и рас, что особо приятно.

Основные моменты, этапы развития компании следующие. В 1991 году, когда я начал набирать себе помощников, я поставил перед ними задачу сделать самую мощную, самую сильную антивирусную программу с точки зрения качества защиты. В 1994 году мы достигли этой цели, начали побеждать в разных международных тестах по качеству (российских тогда не было и до сих пор нет) и с того времени лидируем практически во всех. Невозможно побеждать во всех тестах, невозможно бежать 100 метров всегда быстрее всех. Но если в целом давать картинку, мы — Антивирус №1 по качеству защиты. И это было нашей самой сильной отличительной чертой, помогающей нам строить наш бизнес.

Другой момент, который дал нам сильный толчок, — это 1996–1997 годы, когда мы заключили первые серьезные контракты с финской и немецкой компаниями на лицензирование наших технологий. То есть они берут наш движок (так называемое антивирусное ядро) и встраивают его в свои продукты. Это придало ускорение развитию нашего бизнеса.

Было еще много важных моментов, которые нам помогали. Были и ошибки, и провалы — как без этого. Но все развивается очень хорошо. Мне нравится.

Насколько сложно было справиться с самым первым вирусом?

Очень просто. С большинством вирусов и троянскими программами (на самом деле сейчас вирусов практически нет, идут троянские программы, рекламные системы, масса всего) — с большинством из них справляться было очень легко. Большая их часть достаточно проста, и их не сложно расколоть и занести в антивирусную базу данных. В день у нас работает примерно до десятка вирусных аналитиков, и в день мы добавляем 100–150, иногда 200 записей. Несмотря на то что идет вал новых вирусов, и их становится больше и больше, но они в общей массе достаточно простые.

А написать вирус Вам никогда не хотелось?

Зачем? Правда, были три случая. Первый — когда появились вирусные конструкторы. То есть специальные программы, где в окошках выбирается, какой вирус вы хотите сделать, и он автоматически генерируется. Поскольку можно автоматически создать вирус, то все эти вирусы можно автоматически детектировать и пролечить. Я написал процедуру обнаружения и лечения для всех типов вирусов, которые можно было создать. А потом взял и поигрался с этим конструктором, чтобы определить, работает моя процедура или нет. И все вирусы, которые я нагенерил, были убиты. Второй случай,

когда был спор в интернет-конференциях по поводу самой короткой программы, которая может себя воспроизвести, я написал досовскую программу, которую условно можно назвать вирусом. При запуске она копировала себя в файл с именем «5». И длина ее была 12 байт — короче я не видел. И третий раз меня приперли журналисты на одной из пресс-конференций, говорят: «Касперский, ты же писал вирусы!» Я сказал: «Нет, не писал, но специально для вас сейчас напишу». Я подошел к доске и написал фломастером вирус из одной строчки.

«Разработкой вредных программ занимаются взрослые дяди, которые за это получают деньги»

На самом деле в том возрасте, когда дети пишут вирусы, у меня не было компьютера, да и вряд ли я бы занимался подобной ерундой. Все-таки есть хулиганы, и есть не хулиганы. Первые, если они получают доступ к компьютеру, — да, начинают писать. А вторые никогда этим заниматься не будут.

Но на самом деле вирус сейчас не настолько важная тема. Именно вирусы сейчас составляют примерно 5–10% всего зловредства, которое появляется в Интернете. Пишутся они детьми, школьниками, просто чтобы напакостить кому-то, испортить информацию, отформатировать диск своему соседу. И их становится все меньше и меньше. Потому что сейчас разработкой вредных программ занимаются взрослые дяди, которые за это получают деньги.

Какие виды техноугроз Вы считаете сейчас наиболее опасными для пользователей?

Сейчас 80–90% всех вирусов, червей, троянских программ, которые попадают к нам в руки, пишутся не просто так, а с определенным интересом. И можно сказать, что сейчас в Интернете есть несколько типов бизнеса, которые построены на написании вредоносного ПО. Вирусы эти нелегальные, естественно. Они криминальные. И не могу сказать, какое количество денег сейчас там крутится, но иногда сталкиваюсь с довольно интересной информацией.

Первый тип бизнеса, который сейчас является наиболее горячей темой, — это кража банковской информации, которая строится следующим образом. Интернет сейчас очень популярен. В России еще нет, но будет, безусловно. Вся Европа, Штаты пользуются доступом к банковским счетам через Интернет. Это удобно: никуда не надо ходить, ни к какому банкомату, ни в какую сберкасса, сидишь дома и со своего компьютера делаешь все необходимые операции. Есть несколько технологий кражи подобной информации.

Первая — разработка специальных троянских программ, которые следят за тем, что происходит в компьютере. И как только появляются банковские странички, троянцы их узнают и начинают перехватывать все, что вводится с клавиатуры, — таким образом можно узнать логин и пароль. Или они выводят ложную банковскую страничку вроде как из банка, который просит: была утеряна важная информация, и чтобы вам можно было работать с банком, введите вашу информацию. Или приходит письмо, которое имитирует эту бан-

ковскую страничку. И как только вы вводите логин и пароль, они попадают злоумышленникам. И после этого эти люди получают доступ к банковскому счету, и денежки — тью-тью. При этом очень часто они не могут перевести деньги с банковского счета, но могут купить что-нибудь. И покупают: софт, видеокамеры, все что угодно — и перепродают за полцены. Объемы этого бизнеса неизвестны. Прошлой осенью было арестовано около 30 бразильских мошенников, почему-то бразильские и испанские банки наиболее популярны, и оказалось, что эти 30 хакеров за год украли от 30 до 80 млн долларов. За точность информации ручаться не могу — за что купил, за то и продаю. Но бизнес очень денежный.

Второй вид — рэкет. Выбирается компания, зависящая от веб-сайта: интернет-магазин, казино, букмекерская контора, то есть такая, чей бизнес зависит от работоспособности сайта. Организуются атака на сайт, он падает, и после этого приходит письмо: «Платите деньги». Я видел такие письма, некоторые очень вежливые и приятные, мол, Интернет — такая ненадежная структура, тра-та-та, с Вас 4 тыс. евро. Кто-то платит, кто-то заявляет в полицию. Но, судя по тому, что таких атак становится все больше, народ платит.

Третий вид бизнеса — поддержка спамеров. Для своих рассылок спамеры используют так называемые зомби-сети. Они не могут рассылать спам с одного компьютера, так как его легко вычислить. Поэтому они используют сети из 1000 зараженных компьютеров, причем пользователи ничего не знают о том, что их машина заражена. Бороться с таким количеством компьютеров невозможно. И спамеры, поскольку это бизнесмены, работают с клиентами, получают деньги, но сами писать такие системы не могут, поэтому они обращаются к хакерам, которые делают такие зараженные сетки и продают их. Подобных спамерских сетей очень много. Спам — это вообще отдельный вид бизнеса, в котором может быть все что угодно. Вот, например, недавно был случай. Спамеры начали играть на бирже на повышение-понижение акций. Они скупают какую-нибудь фирму, потом рассылают спам с хорошими новостями про нее, которые ничего общего с реальным положением дел на этой фирме не имеют. Акции ее взлетают вверх — и фирма продается.

«Вирус I love you был фантастическим примером социального инжиниринга»

Четвертый вид криминального бизнеса в Интернете — так называемые звонилки. Вам подсовывают троянскую программу, которая периодически звонит по какому-то телефону, поднимает трубку и держит ее. А с той стороны — платный сервис. Потом приходит внушительный счет.

И подобных махинаций очень много. Поэтому вирусы — это бизнес. И большинство червяков созданы не для того, чтобы плодиться и размножаться, а чтобы притащить с собой какого-нибудь троянца. Они заражают массово компьютеры, рассылают себя с этих компьютеров, но при этом ставят полезную часть: либо зомби-сервер, либо шпиона, либо что-то еще. И сейчас уже около 90% того, что ползает по Интернету, — это криминальный бизнес.

Дальше будет еще хуже, потому что хакеров, заинтересованных в подобных деяниях, будет больше и больше. Будет ли этому предел? Скорее всего, да. Есть какое-то количество компьютеров в сети, часть из них заразить достаточно сложно, потому что они хорошо защищены. А есть другая часть, которую заразить легко. И они заражаются. И троянские программы начинают драться между собой. Допустим, если с компьютера рассылается спам, он идет через какой-то канал. Если будет стоять 10 специальных программ, рассылающих спам, то через этот канал им будет труднее пробиться. Поэтому клиенты будут недовольны качеством сетей и в компьютерном андеграунде будут происходить войны. Такие войны уже происходят среди рекламных систем. Пока рекламные системы — это легально. Это компании, в основном американские, которые занимаются разработкой программ, которые внедряются в компьютер, а потом показывают рекламу. И такие системы начали драться между собой.

Идет война между разными компаниями, которые занимаются написанием разных рекламных систем. В чем она заключается. На компьютер устанавливается новая рекламная система, обычно через зараженную веб-страницу, полувиральными, полутроянскими методами, и первым делом она сносит с компьютера всех конкурентов, а потом уже устанавливает себя.

В будущем аналогичная война может начаться между троянцами. Когда мы это увидим, если увидим, то это будет говорить о том, что количество троянских программ дошло до некой критической массы и дальше они просто не могут работать.

Другая тема, которая мне кажется важной, это мобильные телефоны. Потому что смартфон ничем не отличается от обычного компьютера, есть только единственная деталь, в которой они разнятся, — отсутствие мыши. И уже появились первые вирусы для «Симбиана». Что будет? Будет то же самое, что с компьютером, только хуже. Почему все то же самое? Можно ли воровать банковскую информацию с мобильного? Можно. Есть уже доступ к банковским счетам через мобильный телефон.

Можно ли организовывать рэкет-атаки? Можно. Можно ли рассылать спам? Звонить на платные сервисы? Все можно. Почему будет еще хуже? Потому что количество мобилок больше, чем компьютеров. Сейчас пока тихо, потому что количество смартфонов составляет 1% от всего числа телефонов, — это мало, негде развернуться. Но в этом году, насколько мне известно, планируется продать столько, чтобы доля смартфонов относительно мобильных телефонов составила 2%. То есть эта цифра растет. И естественно, они будут дешеветь. И количество смартфонов дойдет до черты, когда хакерам станет интересно работать с ними. У нас уже есть решения для смартфонов и карманных компьютеров. Мы ждем.

Можете ли вспомнить интересный случай из Вашей практики?

Тут не бывает интересных случаев, бывают интересные проблемы. Наверное, вирус СІН, или «Чернобыль» его еще называли, потому что 26 апреля — годовщина трагедии в Чернобыле и заодно день рождения автора этого вируса. И 26-го числа он стирал флеш-память компьютера. Для того чтобы восстановить работоспособность ПК, нужно было достать микросхему, перепрограммировать ее и вставить обратно. Но, как оказалось, на многих ноутбуках эта микросхема была впаяна в материнскую плату. И отпаять ее обратно стоило дороже, чем купить новую материнскую плату. Оказалось, что на многих ноутбуках на эту же материнскую плату впаяны и вин-

честер, и видеокарта, и звуковая, и прочее оборудование. И если этот вирус заражал такой ноутбук и он включался 26-го числа, то после этого его можно было взять и выбросить.

Другая история — I love you. Глупый вирус, написанный на скрипт-языке, который остановил работу громадного количества компаний по всему миру. Это была детская шалость, которая бахнула так, что стоила миллиарды долларов. Многие вирусы и троянские программы, для того чтобы проникнуть в компьютер, используют различные хитрости, чтобы заставить пользователя кликнуть по ссылке или запустить файл. Вирус I love you был фантастическим примером социального инжиниринга. Приходит письмо, в котором написано: «I love you», и в нем вложенный файл — подробнее смотри в аттаче. И на это попадали сотни людей, у которых несчастная судьба, что-то не сложилось, проблемы в личной жизни. Как пели битлы: «All you need is love». И народ кликал на вложения, причем иногда и не по одному разу.

Еще одна история была с вирусом «Серкам». Когда он рассылал себя с компьютера, то цеплял документ: совершенно случайный вордовый или экселевский файл. Такая информация прилетала!!! Заказ бронированного автомобиля на завтра одним из банков города Москвы с указанием маршрута и времени следования. Причем это один из самых безобидных примеров. Это происходило по всему миру. Даже из ФБР мы получали информацию.

Эти вирусы были просто хулиганством. Это было в конце прошлого века, тогда в Интернете было особо нечего воровать. Банковские системы не были настолько развиты, как сегодня. И воровали доступ в Интернет, ключи программ. Сегодня же воруют все. Ключи к софту. Причем особой популярностью почему-то пользуется игра «КонтрСтрайк». Ключи к виртуальному миру. Не говоря уже о электронных деньгах типа WebMoney.

Одним словом, воруют все, что можно украсть. И сегодня смешных историй практически не происходит. По сравнению с древними эпидемиями, которые бабахали по полной программе. Уже не так интересно.

Сильно ли изменилась для обычного пользователя ситуация с компьютерной безопасностью за последние 5–7 лет?

Да, очень! Кардинально изменились. На самом деле 5–7 лет назад народ не защищался никак. Антивирус был абсолютно обязательной штукой на компьютере. 5 лет назад, я помню, даже слышал такие комментарии: «Если вдруг мой провайдер поставит антивирус на свой почтарь, уйду к другому провайдеру. Не хватало еще, чтобы кто-то копался в моих письмах». Сейчас антивирус — обязательная часть компьютера, потому что ходить по Интернету без него просто опасно. Антивирусные решения ставятся везде, даже есть специализированные антивирусные «железки», которые ставятся на трафик, чтобы снижать его, — это такая предварительная зачистка. Антивирусные программы стали сложнее, потому что сейчас нужно ловить не только вирус и троянские программы, но и рекламные системы, бороться со спамом. Эти изменения связаны с тем, что окружение стало более агрессивным. То есть в Интернете все больше и больше хакеров, туда все опаснее ходить, методов нападения все больше, поэтому приходится применять разные способы защиты. При этом ущерб, который может «поиметь» пользователь оттого, что машина заражена, самый разнообразный.

Бывают и вообще казусные случаи. На одну из прибалтийских компаний была организована спам-атака. Они позвонили в полицию. Та расследовала-расследовала и обнаружила, что один из компьютеров, который атакует эту компанию, находится в той же самой прибалтийской стране. Потом была специальная акция, как в кино. 6 утра, дом окружили полицейские машины. И компьютеры были арестованы. Так что есть риск попасть в милицейское-полицейское расследование, не как сообщник или подозреваемый, а потому, что с вашего компьютера производились незаконные действия.

Что можно сделать обычному пользователю, чтобы обезопасить свой компьютер от таких вторжений?

Существует три стандартных правила. Но, во-первых, безусловно, это «правило ноль», должен стоять антивирус — если он не стоит, то и разговора никакого мы не ведем.

«В Интернете все больше и больше хакеров, туда все опаснее ходить»

Правило номер 1. Антивирус должен быть самой свежей версии и с самыми-самыми свежими антивирусными базами. Как часто скачивать апдейты, нужно решать в зависимости от того, как часто вы работаете с сетью. Мы выпускаем апдейты раз в час, а иногда даже раньше. Я рекомендую так. Если вы находитесь в сети непрерывно, то лучше скачивать апдейты раз в час. Если отключены — это уже не так критично.

Правило номер 2. Не верить информации от незнакомых, не заслуживающих доверия источников. Неважно, какой информации. Письмо пришло, сайт какой-то незнакомый, эсэмэска прискакала, по ICQ или другому пейджеру прислали объявление — верить нельзя. К такой информации нужно относиться крайне осторожно. Скорее всего, если приходит письмо заманчивого содержания от незнакомого человека, вы — потенциальная жертва злоумышленника.

Правило номер 3. Больше внимания нужно уделять информации от антивирусных компаний. Очень часто мы сообщаем о новых методах мошенничества в сети, о новых угрозах, поэтому нужно поглядывать за тем, о чем мы рассказываем.

Если коротко: антивирус должен быть самый свежий, и верить никому нельзя, кроме нас.

Конечно, лучше не кликать куда угодно. Делать так — все равно что ходить по минному полю.

Нужна ли какая-то защита компьютеру, который не имеет доступа в Интернет?

На самом деле защита не нужна только тогда, когда компьютер постоянно выключен. Робинзону Крузо тоже, наверное, прививки от гриппа были необязательны. На самом деле риск «залететь» исходит от всех источников общения ПК с внешним миром: CD, DVD, флешки... Любой источник информации, который поступает извне, — это риск. Максимальную опасность представляет, конечно, Интернет. Минимальный риск — CD-ROM и флешки. Но все равно он есть.

Беседовала Светлана Панина