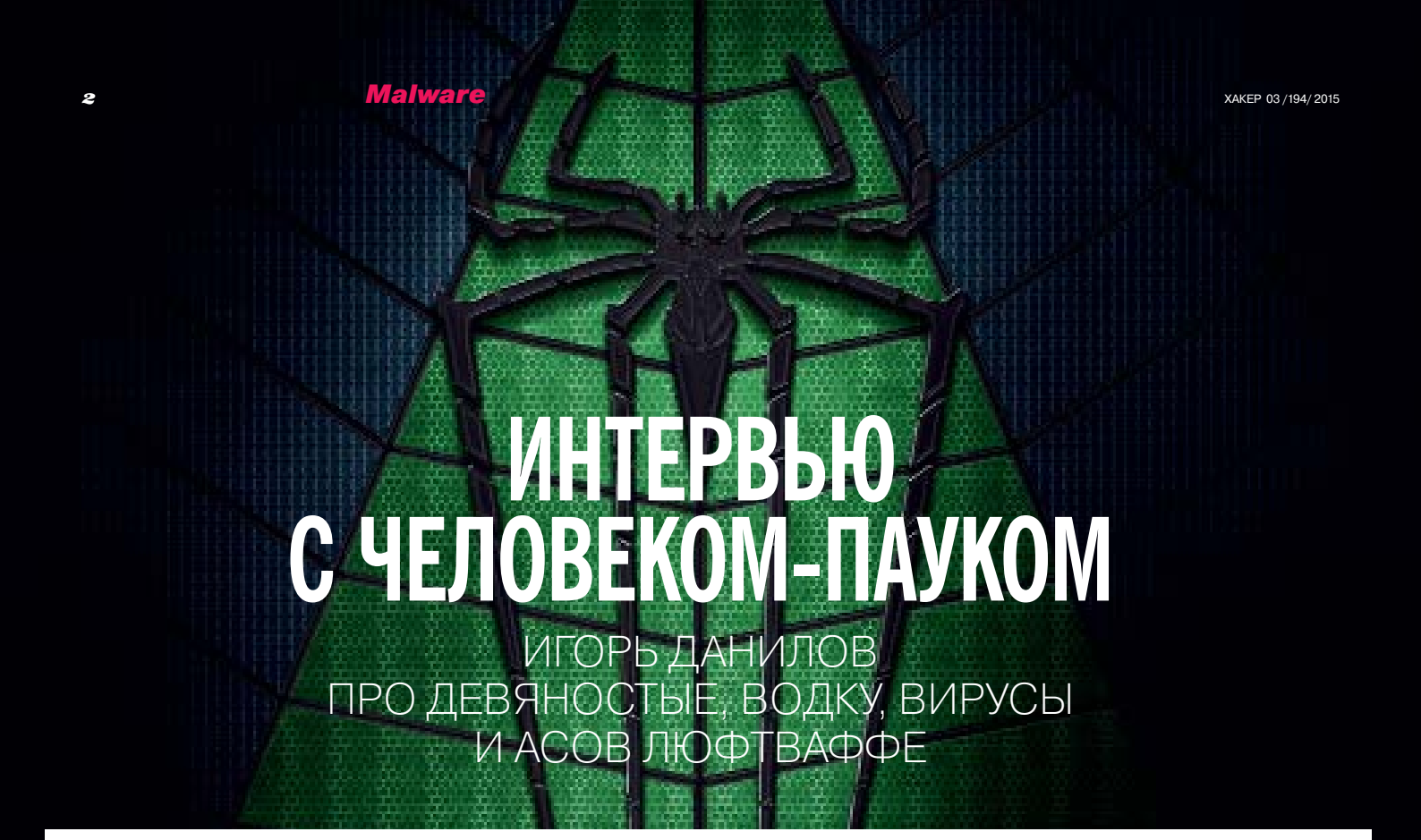


ИНТЕРВЬЮ С ЧЕЛОВЕКОМ-ПАУКОМ

ИГОРЬ ДАНИЛОВ ПРО ДЕВЯНОСТЫЕ, ВОДКУ, ВИРУСЫ И АСОВ ЛЮФТВАФФЕ

Однажды, слушая радио в машине, я вдруг обнаружил, что весьма актуальные на моей школьной дискотеке композиции теперь передают по радио Ретро. Я вспомнил школьные годы, командную строку, синие панели Нортон Коммандера, Turbo Pascal, Turbo Debugger, ассемблер для IBM PC Питера Абеля... вирусы, гнев учителя информатики... AidsTest, Dr. Web. Да, сегодня, в 2015-м, я имею полное право ностальгировать!
И вот я еду в «Сапсане» на встречу с культовым господином — Игорем Даниловым, автором Dr.Web, чьим вирлистом зачитывались в девяностые годы все начинающие вирмейкеры ex-USSR. Он был уважаем тогда, он работал в двухтысячные, и он все так же успешен сейчас. Чем не повод с ним побеседовать?

Беседовал
Александр Лозовский
lozovsky@glc.ru

Как вы пришли в мир антивирусов? С чего начался ваш творческий путь?
Это вышло случайно... Я был ведущим инженером в НПО «Ленинец», занимался бортовыми процессорами военных самолетов.

В то время появились вирусы. У нас было всего два компьютера, с флоппи-дисководами. Периодически через дискеты с драйверами из Тайваня и с игрушками проникали вирусы. Лечились Aidstest'ом, но потом начали попадаться вирусы, которые Aidstest не знал. Тогда я купил книгу, могу показать — Безруков, «Компьютерная вирусология».

О, я такую с BBS'ки в свое время качал, на бумаге впервые вижу...
Так вот, приехал я на дачу, прочел ее за ночь, появились идеи. Она послужила толчком к тому, что я начал программировать «Спайдер» — резидентный сторож. Дело в том, что сканеры, или, как их в то время называли, полифаги, уже были достаточно распространены. Из наших тогда были Женя Сусликов (больше известен как автор HIEW) из Кемерово и его полифаг Goalkeeper, впоследствии названный SOS. Кстати, был у него и резидентный сторож — Inspector. Дмитрий Грязнов из Переславля-Залесского и его Ambulance (сейчас он главный разработчик в Microsoft, недавно ушел из McAfee)... Евгений Касперский. Основным конкурентом для меня тогда был Евгений Сусликов, у него был самый шустрый сканер (полифаги Касперского и Лозинского значительно медленнее). Поэтому свой сканер я назвал «Торнадо» — он был реально быстрым.

А релиз, конечный продукт? Когда он вышел и как назывался?
Это был, кажется, конец 1991 — начало 1992 года, назывался он Spider's Web. У нас была такая наклейка с паучком. Здесь (в Питере. — Прим. ред.), в Гавани, у нас была компьютерная выставка, мы там выставлялись и впервые даже продали программу.

Мы?
Был у меня товарищ, начальник моей лаборатории в институте. И когда случился распад СССР, работы не стало, мы работали с ним вместе. Он искал рынок сбыта, помогал финансово, я разрабатывал.

На CeBIT 1993 вы ездили с ним? Как все прошло?
История сложная. Во-первых, денег у нас не было абсолютно. Во-вторых, нам не хотели давать паспорта, у нас была форма секретности, и выпускать нас не полагалось. С этим мы разобрались, а вот вопрос проживания встал особенно остро.

Сергей был знаком с одной девочкой из Ганновера, она писала диссертацию. Он с ней договорился, что мы будем жить в доме ее друга, кстати, олимпийского чемпиона, который должен был быть в отъезде. Этот вариант сорвался. Поэтому мы жили в ее доме. А надо сказать, что это был огромный дом — ее папа полковник вооруженных сил Германии...

А как насчет языкового барьера?
Ну, у меня был на каком-то небольшом уровне английский, а Сергей Пяткин очень хорошо знал немецкий.

Какое впечатление произвела Германия?
Единственное, что меня поразило: я с собой взял щетку, гуталин, чтобы чистить ботинки... и они мне за все время нашего пребывания не понадобились. Так было чисто. Ну и отношение людей к войне, кстати. Ее папа очень открыто говорил о войне. Я думал, что эта тема будет замалчиваться, но он показывал

нам книги с Гитлером, рассказывал, как тот основал «Фольксваген»... и так увлекся, что пришлось напомнить ему про Сталинград.

Вот вы вернулись из Германии — и? Как пошел бизнес?

Ситуация была очень странная. Я сделал антивирус, поехали мы в Германию, там выставились, но продолжения не было. Он не продавался.

Как раз тогда появились первые полиморфные вирусы, против которых не справлялись другие антивирусы. Я написал эмулятор и первую версию Dr.Web'а, который лечил от этих вирусов. Надо было ее как-то распространять. Тогда я пришел в «Техническую книгу», это у нас на Пушкинской, там продавались диски. Я попросил ребят просто бесплатно записывать на тот же диск с Aidstest'ом мою программку. Тогда как раз бушевал полиморфный вирус «Фантом», и «Доктор Веб» моментально стал популярен, хотя тогда он знал всего 21 вирус. Большую роль в распространении сыграло Фидо.

Вирус «Зараза»

В тот момент Сергей Пяткин по какой-то программе уехал в Германию, проходить какую-то практику по менеджменту. Я остался один и стал сотрудничать с «ДиалогНаукой» — надо сказать, что они были единственными, кто, что называется, «продавал». Тот же антивирус Сусликова был то ли бесплатный, то ли условно бесплатный.

О, вирус Phantom! Мне в те времена больше повезло поймать другой полиморфный вирус, One Half. Помню, что «Веб» первым научился его лечить, но первые версии забывали расшифровать половину диска, которую он шифровал.

О, это интересная история. Как я говорил, в этом году мой продукт стал популярен в СССР, на Украине и даже в Восточной Европе и... Сирии, как раз потому, что он хорошо боролся с полиморфными вирусами и в нем была эвристика. Так вот, был один парень, Хубинский, он держал ББС-ку в Словакии. Он прислал мне оттуда два вируса, которые показались ему очень интересными. А я как раз ехал в Москву, в «Диалог-Науку», и заодно встретился с Касперским, у меня с ним тогда нормальные отношения были. Я показал ему эти вирусы, а сам поехал в компанию. А он мне звонит и говорит: жутко интересные вирусы, ты смотри, шифруют диски. Я вернулся домой, взялся за них и выпустил лечение для вируса без расшифровки... Думал — кому это надо, а мне отдельную подпрограмму расшифровки писать... А меж тем вирус распространялся, пошел на Украину... и мне по Фидо пошли фидбэки. Когда их количество превысило некоторую критическую массу, Лозинский сказал мне: давай уже пиши расшифровку. Я сделал отдельную подпрограмму лечения. Сначала она ничего не выводила, кроме предупреждения «Идет расшифровка диска», но оказалось, народ начал паниковать из-за того, что компьютер в это время активно шуршал диском, и пользователи начали жать на кнопки, выключать и перезагружать компьютер. В итоге мы с Севкой сделали версию, которая выводила проценты и надпись о том, что расшифровка может занять длительное время.

Извинения. Респекты. Приглашение к переписке

С онхалфом была еще одна интересная история. Продается, значит, мой антивирус. Вяло продается, помню, шесть рублей он стоил. И вдруг смотрю — один за одним подходят курсанты в военной форме и, ни слова не говоря, один за другим его покупают. Я спрашиваю: что случилось? Оказалось, что они учились в Можайке и One Half зашифровал все их дипломы. Они расшифровали диски пиратской версией Web'а и вот — дали себе зарок купить лицензию, вернуть долг.

Вирмейкеры девяностых очень любили высказать свой дизреспект авторам антивирусных программ

Я смотрю, в нашем разговоре появились два человека — культовый Дмитрий Николаевич Лозинский, известный как автор AidsTest, и Всеволод Лутовинов, который стал вашим соавтором по Dr.Web. Как вы познакомились с Дмитрием Николаевичем?

С Лозинским мы познакомились осенью 1993-го, когда Ростовский университет позвал нас на сборище в Абрау-Дюрсо. Туда были приглашены все антивирусные ребята: Зуев, Лодыгин, Лозинский, Касперский... Я поехал тоже и со всеми ними познакомился.

А какой формат мероприятия?

Программистская тусовка. Какие-то доклады, семинары. В основном это было море, водка, пляж, разговоры, преферанс. На следующий год мы опять собирались.

Отличный формат, на такое мероприятие и я бы не отказался вернуться! А как с Лозинским вы впоследствии стали работать?

Сперва мы работали просто под одной вывеской — «ДиалогНаука», а потом уже начали сотрудничать, я стал его кое-чем нагружать...

Чем нагружать?

Он мне предлагал кое-какие лечилки, свою базу вирусов, но код я его в основном не брал, были больше советы, подсказки. А он делал для «Веба» кое-какие вещи, отладчики под базы например. Он человек очень дотошный, трудоголик.

Помню, в одном из интервью Дмитрий Николаевич говорил примерно то же самое про вас. Вы из тех наших коллег, которые могут сутками программировать, питаясь только пивом и сосисками?

Сутками сейчас уже не могу. Только если с перерывами на сон. Вот когда мы с Севкой занимались антивирусом под Novell Netware на Благодатной, в подвале, мы столько чайников сожгли... Они ведь тогда сами не отключались. Мы ставили чайник и садились программировать. Мы жгли эти чайники один за одним, так что эбонитовый запах от них потом совершенно не выветривался.

И кстати, когда я программирую, я не пью. Если я пью, то я не работаю. Раньше, в молодости, я если выпил, то и книжку читать не мог. Насчет работы и выпивки у меня жена даже смеялась — бывали моменты, что я выпивал, у меня появлялась идея, я лез программировать, затем все это летело в помойку, и жена уже мне потом говорила: куда ты, все равно ведь выкинешь.

И вообще, пиво — это нью дженерейшн продукт. Я летчик-истребитель бывший, я пью водку. Ну, то есть я пью пиво в Германии или Чехии. Но вообще ребята советского времени не пьют пиво, потому что это неинтересно.

Вот так поворот! А как же Фидо, «напиток наш — пиво, его только пей, Фидо нас навеки друг с другом сплотила, никто не отнимет у нас сеть друзей»? Вижу, у вас есть все признаки классического хардкорного программиста: вы курите, пьете черный кофе без сахара... и вдруг — пиво не уважаете! Тогда посоветуйте хорошую водку! Как будет выглядеть топ-3 водок от Игоря Данилова?

1. «Юрий Долгорукий». Дорогая, но хорошая.
2. «Иван Калита».
3. «Финляндия».

Получается, в этом вопросе я отдаю предпочтение продукции как раз московского завода (смеется).

Я тут вдруг осознал, что вы сказали «летчик-истребитель». Я не ослышался?

Да, я учился в КВВАУЛ (Качинское высшее военное училище летчиков).

В нашем разговоре уже дважды всплыло слово «продавать», но мне прямо не верится в него в контексте девяностых годов… Я не видел ни одного живого человека, который покупал в те времена программы. Даже в зеркале :).
Денег у меня поначалу не было. У меня была жена, двое детей, я писал «Доктор Веб»… Сложные времена были. Летом девяносто четвертого мы договорились с «Диалогом». Мой продукт уже был популярен во всей стране и в Европе, но они не знали, выстрелит ли он, думали, что его придется долго раскручивать. Мы договорились так: они начинают продавать и платят мне двести долларов, если он не продается. Если продается — тогда еще процент с продаж.

Двести долларов? По ценам девяносто четвертого года… это же… ого-го!
Это отлично! Я шел с ними и думал, что я миллионер. Я купил себе колеса для старой машины, то, се, пятое, десятое, оделись, обулись. То ли два, то ли три месяца я получал двести долларов, а потом мне заплатили около двух тысяч долларов.

Когда я принес эти деньги домой, жена сказала мне: зачем так много, нам и двухсот долларов хватало. «Диалог» продавал очень много на уровне страны, и это при том, что покупали от силы 5%.

Почти двадцать лет хочу спросить, что вы чувствовали, когда переписывали в своем вирлисте все те оскорбления и пожелания, которые авторы вирусов вам адресовали? С какими эмоциями вы копировали все эти «privet, muDAniloff» или «Жили у бабуси три веселых гуся — Лоз, Данилов и Касперский, я от них тащуся»?..
Я пытался быть объективным всегда. Это документ, если в вирусе это есть, в документ я пишу все, как там. Если я допускал какой-то укол в сторону вирусописателя, то старался, чтобы он был необидный, в рамках.

Все-таки это можно по-разному делать — тот же Лозинский в своем вирлисте писал что-то типа «а также содержит оскорбления в мой адрес», а вы перепечатывали все полностью. И кстати, очень подробно расписывали вирусные алгоритмы. Как думаете, не подвигли ли они каких-нибудь людей на написание собственной малвари?
Да конечно, подвигли, только это была не моя идея, а Лозинского.

А кто из вирмейкеров девяностых вам запомнился и чем?
Вот, запомнился один (достает из шкафа и показывает мне зажигалку с надписью **Zhengxi**). Писал стелс-полиморфные вирусы с таким названием. А эту зажигалку он мне через людей передал (есть мнение, что автор этого вируса учился в те времена в Питере. — Прим. ред.).

Еще запомнился **Dark Avenger**, который придумал полиморфный движок MtE. Антивирусным ребятам пришлось хорошо над ним поработать.

А вообще как к вам относились вирмейкеры девяностых? Письма писали, по телефону названивали, почтовый ящик поджигали?
Тогда это просто была виртуальная битва. Они были деструктивны, они уничтожали информацию, но чтоб ко мне шел какой-то негатив — такого не было. Это нынешняя мафия совершенно другая, это уже криминал в чистом виде, они за деньги мать родную убьют.

То есть в любви с помощью вирусов теперь не признаются?
В наши временна это чисто коммерция. Какая сейчас любовь, сейчас это насос для денег, информации. Время то немножко ушло. Совсем даже ушло. Правда, тогда и качать было нечего.

Вот вы говорите, время ушло. Ностальгируете?
Нет, не ностальгирую.

А по играм? Вот, Doom 2 был — вещь, дизайн уровней какой! А сейчас что за игры? Идешь-идешь-идешь по компасу, заблудиться даже не получится, игра сама тебя по карте тащит, только заставки показывает.
Играл я, когда инженером был, помню, в симулятор F-117. А потом некогда стало. И до сих пор я считаю, что играть в компьютер — идиотизм. Я и детей в этом всегда ограничивал. Внуков вот, конечно, не ограничишь, они айпэд сами берут. Сам я играю только в хоккей.

Ого! И сколько раз в неделю играете? Есть достижения?
Два — пять раз в неделю. Из достижений — СПБХЛ, играл на чемпионате города.

Кстати, а произвела ли на вас какая-нибудь малварь положительное впечатление?
Назову два интересных вируса — **Анархия** и **Зараза** (см. скриншоты из virlist.dvb от 1997 года. — Прим. ред.). С «Анархией» вообще интересная история приключилась. Как потом оказалось, его автор учился в Питере на матмехе, мы познакомились в Фидо. Он спросил меня: а ты понял, почему точка останова стоит внутри обработчика 21-го прерывания? Нет? А потому, что при всех других вариантах он падал и я не мог его отладить. А с автором «Заразы» мы тоже, как я подозреваю, пересекались. Он занимал очень хороший пост в одной известной IT-компании. Мы с ним на одном семинаре контактировали, он мне показывал кое-какие фрагменты кода, очень увлеченно о нем рассказывал, ну я и проинтуичил, что, скорее всего, он его и написал.

А расскажите про вирусы, которые писали лично вы. Вы же участвовали в конкурсе на самый маленький TSR-вирус?
Соревновался… Доктор Соломон назвал их семейством Dinky — изящные. Сначала мой вирус был самым маленьким, потом рекорд мой побили, я завелся, написал еще меньше, но уже не публиковал, так как пошли слухи о том, что я пишу вирусы. Было 70 байт, я сделал 59… Он продержался очень долго, я уже думал, что его не побьют… А потом какой-то человек взял явно мой вирус, применил некоторые интересные ходы и сделал короче. И я уже потом для себя сделал другой, еще короче, но никому не показывал.

Вирус «Анархия»

Часы с американской подводной лодки сорок первого года. Плоский монитор образца начала века. Компакт-диск с инсталлятором «дела всей жизни», зачем-то висящий на трубе. Системный блок без боковой стенки (и еще один вне поля зрения, бесшумный, с чисто радиаторным охлаждением). Обстановка офиса намекает, что его хозяин — тру олд хакер, а не какой-нибудь стартапщик с iMac'ом. Кстати, на обоих компах у него Win 7, так что делаем выводы!

Кроме того, перед тем как написать «Доктор Веб», я наваял собственный вирус и на нем отрабатывал технологии. Еще мы с Севкой, когда докручивали свой эвристик, написали полиморфный вирус, который размножали на специальном сервере. «Доктор Веб» выкашивал то, что получилось, а мы с интереом наблюдали, что останется. Там были случайные подмены команд, и, естественно, многие копии оказывались битыми. Мы даже с Евгением Касперским этой информацией обменивались.

Размер в 59 байт (без приставки кило-) в 2015-м кажется чем-то нереальным. А сейчас вы больше менеджер или все-таки остаетесь технарем?
Наверное, больше менеджер. Хотя в последнее время стараюсь прибрать к рукам техническую часть.

А квалификацию повышаете? Что читаете?
Вам прямо про алгоритмы рассказать?

Давайте не про алгоритмы! Давайте лучше про книжки.
Вот, пожалуйста (открывает книжную полку): книги «Асы Люфтваффе», «Асы Третьего рейха». Я историей Второй мировой и финской войн увлекаюсь.

(заглядываю поглубже в книжную полку) Дмитрий Анатольевич, так у вас тут коньяк, коньяк… арманьяк… горилка?!
А это мне Андрюха Былев принес. Сейчас он в Сан-Франциско уехал. Обещал со мной ее выпить, так вот и стоит уже пятнадцать лет как память о хорошем человеке.

Андрей Былев? Кто это?
Он жил в Киеве, работал на какие-то европейские компании, постоянно ездил в командировки в Германию. После того как он разработал концепт драйвера VxD для SpIDer, уехал жить и работать в Сан-Франциско. С тех пор я с ним ни разу не встречался и даже не знаю, как он там поживает.

История войны, говорите… А есть у вас тайное хобби? Спортивные машины, например, коллекционируете?
Надеюсь, я от комплексов этих нуворишских все-таки избавлен. Зачем мне спортивные машины? Я и в квартире живу в той же, что и двадцать лет назад. Вот если бы я жил в Америке, то я бы купил, наверное, летающий истребитель Второй мировой войны. Только их нет, летающих. Точнее, есть одна штука, но его вряд ли продадут.

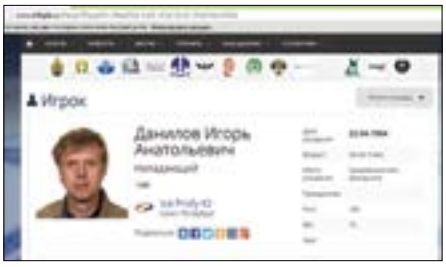
Я тут вспомнил, что вы говорили в интервью Хабру, что с Евгением Касперским вы «знакомы. Наверное, сможем узнать друг друга на улице. Никаких отношений между нами нет». А получается, что вы достаточно плотно общались?
Я ночевал у него, когда в Москве был! Мы нормально контактировали, встречались, обсуждали, делились. Это у нас позднее случилась размолвка.

Что за размолвка?
Мы по-разному смотрим на этот круглый мир. Это нормально.

А вот в Infected Voice, помню, писали, что их боец якобы перешел на другую сторону баррикад и устроился к Касперскому. А вы бы могли взять на работу человека с (кибер)криминальным прошлым? Ну, если бы он раскаялся…
Был у меня такой человек. Очень хороший специалист, эрудированный чувак. Очень жалею, что я его взял. Я его подозревал, но он каялся, говорил, «да я, да ни в коем случае». Пришлось его выгнать, а осадок до сих пор остался. Так что — нет.

То есть вы разделяете точку зрения о криминальном типе личности? Что человек, если он занимается криминалом, то ему какую зарплату ни положи, все равно «в лес смотреть» будет?
Разделяю.

Игра F-117: лучший выбор инженера оборонного завода. Школьники девяностых тоже ее уважали. Она же от Microprose!



Профиль виновника торжества действительно гуглится на сайте СПБХЛ

Артефакт: зажигалка вирмейкера. Интересно, если носить ее в инвентори, она добавляет какие-нибудь способности?

Смотрите, антивирусное ПО стоит на миллионах компьютеров. Код закрыт, трафик шифрован в обе стороны. «Полномочия» — неограниченны. Антивирус защищает компьютер от малвари, но что он делает еще? Сможете ли вы убедить читателей в том, что антивирус не часть огромного «легального» ботнета?
Насчет этого я абсолютно спокоен. Бери снифер, смотри. Меня французские спецслужбы так же пытали. Международная обстановка сейчас осложненная, поэтому они думали, что раз Россия, значит, все должно уходить в ФСБ, в разведку. Ничего не нашли.

Когда сертификацию Минобороны проходили, тоже проверка была. Они должны были мониторить исходные коды на предмет закладок.

Приехали трое парней, говорят: не было ни одной компании, чтобы мы чего-нибудь да не нашли.

Дали им закрытые компьютеры, вот исходные тексты, говорим, смотрите.

Работали неделю. Достаточно грамотные ребята. Ничего не нашли, ни закладок, ни шлюзов отладочных, ничего.

Погодите, как «смотрели»? Это же года не хватит.
У них были тулзы специальные, анализирующие код, это уже их наработки. Глазами застрелишься, конечно. Разумеется, если я захочу скрыть что-то в исходных текстах, я скрою так, что вы ничего не найдете… Но зачем мне это? Зачем мне эти данные, кому я должен их отдавать? Поэтому я никому ничего не дам.

Надавят? Подкупят? Шантаж?
Это практически невозможно. Никогда не говори «никогда», но «практически».

Какие вообще у вас отношения со спецслужбами?
Нет никаких отношений, кроме официальных, нормальных. Сертификация — пожалуйста. Помощь экспертной оценке, в работе — пожалуйста. Нас знают все полиции мира. Это есть.

Серьезный вопрос. У нас тут в редакции вышел спор. Я пообещал нашим сотрудникам, что если они не пришлют мне свои ответы на новогодний опрос, то я от их имени пропечатаю в журнале признание в стиле Тима Кука. А одна из коллег считает, что шутить про геев в журнале «Хакер» — это «по-человечески недостойно». Рассудите нас, пожалуйста, как авторитетный человек.
Да мне все равно, кто гей, кто не гей… зачем это все выпячивать. Я же не выпячиваю, что я гетеросексуал, что я лесбиян там…

Ага, а говорили, что ночевали у Евгения Касперского :). Я уже даже заголовок придумал: «Шок! Игорь Данилов ночевал у…».
Там жена была, Наталья Касперская, мама его, дети :). В общем, шутите. Общество сейчас немножко зомбировано… Шутите!

И напоследок: ваши пожелания читателям.
Думать, думать, думать. И творить. Потому что ничего круче творчества в жизни нет. Кроме любви. Я считаю, что человеческое счастье — это возможность творить. Неважно что. Найти любой элемент творчества. Если этой возможности нет, то нет никакого драйва. ✠