компьютерные вирусы — эволюция или революция?
tagline: ретроспектива глобальных эпидемий

крис касперски ака мыщъх, no-email

чтобы выработать оптимальную стратегию борьбы с вирусами, необходимо не только учесть все технические аспекты проблемы, но еще и разобраться с философскими концепциями: откуда берутся вирусы, кто их пишет, кто с ними борется, как они изменяют мир, почему возникают глобальные эпидемии и какое будущее нас ждет — мир за каменной стеной, где в угоду безопасности все запрещено и шаг влево/шаг вправо карается расстрелом на месте без предупреждения, или же абсолютная ничем не ограненная свобода и кибернетическая демократия?

"Those who desire to give up freedom in order to gain security, will not have, nor do they deserve, either one Thomas Jefferson
(*"Тот, кто хочет променять свободу на безопасность не заслуживает ни того, ни другого" — Томас Джефферсон*)

/* полоса 1 */
введение

Компьютерные вирусы прошли длинный эволюционный путь, приспосабливаясь к изменчивому миру операционных систем и защитных механизмов. По самым скромным подсчетам хакерами было написано порядка полумиллиона вирусов и разработано множество технологий противостояния различным защитным механизмам (полиморфизм, стелсирование, etc). Вирусы освоили практически все "экологические ниши": начав с исполняемых объектов, они продолжили наступление на файлы данных: сначала это были робкие эксперименты с макросами в документах MS Office, а затем все более смелые атаки на переполняющиеся буфера в jpg/gif/mp3/midi и прочих форматах, считавшимися ранее _принципиально_ недоступными для заражения.

К концу XX века вирусы получили повсеместное распространение, освоив не только Windows, Linux/BSD, но и мобильные платформы. Сейчас нет практически ни одной системы полностью свободной от вирусов. Пожалуй, только контроллеры, управляющие лифтами да микроволновыми печами избавлены от этой напасти, но сколько такое спокойствие еще продлиться — сказать невозможно. Микроволновые печи, управляемые через Интернет, уже появились. Осталось добавить в них поддержку Java-апплетов для автоматизации приготовления своих любимых блюд и вирусы захват еще один ареал обитания.

Несмотря на все усилия и ожесточенную борьбу, развернувшуюся на антивирусном фронте, количество вирусов сокращаться не собирается даже наоборот. Чем активнее мы боремся с вирусами, тем стремительнее они совершенствуются и тем сложнее их оказывается отождествить и нейтрализовать. Вирусы превратились в объективную данность, с которой мы вынуждены считаться, сосуществуя в едином информационном пространстве.

/* полоса 2 (колонки 1, 2,3), полоса 3 (колонки 1, 2)*/
летопись вирусной хронологии

Первое семя было брошено в почву в далеком **1949 году**, когда Джон фон Нейман (John von Neumann) прочитал серию лекций по теории самовоспроизводящихся автоматов, изданную уже после его смерти в 1966 году ("The Theory of Self-reproducing Automata", A. Burks, ed., Univ. of Illinois Press, Urbana, IL), переведенную на русский язык издательством "Мир" в 1971 году.

Рисунок 1 Джон фон Нейман

В **1957 году** в престижном научном журнале "Nature" известный математик Роджер Пенроуз (Roger Penrose) опубликовал статью "A Self-reproducing Analogue" ("Самовоспроизводящиеся Модели"), исследующую проблемы кибернетической жизни (сам текст статьи можно найти на официальном сайте журнала www.nature.com/nature/journal/v179/n4571/abs/1791183a0.html).

В **1961 году** сотрудники компании "Bell Telephone Laboratories" придумали игру Darwin ("Дарвин"), моделирующими эволюцию посредством сражения между несколькими ассемблерными программами ("организмами") за системные ресурсы ("пищу").

В **1970 году** была зафиксирована первая программа-бомба по имени "Cookie Monster", написанная Крисом Таваресом (Chris Tavares) для компьютеров типа IBM 2741, работающих под управлением экспериментальной операционной системы MULTICS.

В **1973 году** Боб Томас (Bob Thomas) написал самовоспроизводящуюся программу Creeper (что переводится как "ползучие растение"), работающую под операционной системой Tenex в сети ARPANET (Проинтернет) и перемещающуюся от машины к машине с выдачей сообщения 'I'M THE CREEPER: CATCH ME IF YOU CAN.' ("Я Вьнок. Поймай меня, если сможешь!"). Creeper, изначально созданный в чисто демонстрационных целях, быстро вышел

из-под контроля и для борьбы с ним был написан Reaper (Жнец), бегающий по машинам в поисках вьюнка и делающий ему харакири. Имя создателя Жнеца так и осталось неизвестным.

В **1974 году** количество самовоспроизводящиеся программ (прозванных за свою плодовитость "кроликами" — Rabbits) резко возросло и их размножение приняло характер эпидемии. Тогда же появилась программа HIPBOOT, внедряющая в загрузочные сектора загрузочных дисков, и поражающая компьютеры Nova, производимые компанией Data General.

В **1975 году** вышла книга "The Shockwave rider" ("На шоковой волне") Джона Браннера (John Brunner), где он описал программу, самостоятельно распространяющуюся по сети, впервые употребив термин "червь" ("worm") ставший впоследствии общепринятым. В том же самом году Джон Уолкер (John Walker) дополняет написанную им ранее игру "Animal" ("Животное"), подпрограммой "Pervade" (от англ. распространяться, проникать), работающей на компьютерах Univac 1100/42 под управлением операционной системой Exec-8. Связка Animal/Pervade ведет себя, как файловый червь.

В **1980 году** Юрген Краус (Jurgen Kraus) защитил дипломную работу по теме "Самовоспроизводящиеся программы" ("Selbstreproduktion bei programmen"), а в исследовательском центре фирмы Xerox, расположенном в Пало-Альто, двое ученых Джон Шоч (John Shoch) и Йон Хапп (Jon Hupp) независимо от него провели серию экспериментов по распределенным вычислениям на основе программ-червей, закончившихся созданием вполне жизнеспособного червя Xerox-Worm.

Рисунок 2 Юрген Краус

В **1981 году** (по другим данным в 1982) на компьютерах Apple II появляется программа "Elk Cloner", написанная Ричардом Скрентой (Richard Skrenta), распространяющая через гибкие диски и вызвавшая первое масштабное заражение персональных компьютеров. Казалось бы — отличный повод задуматься о защите, но… история нас учит тому, что ничему не учит.

В **1983 году** студентом Фредом Коэном (Fred Cohen) была написана саморазмножающаяся программа, работающая на платформах VAX 11/750, TOPS-20, VMS

управляемых операционной системы UNIX, и продемонстрированная на конференции по компьютерной безопасности в ходе которой Лен Эдлманон (Len Addleman) впервые употребил термин "вирус".

Рисунок 3 Фред Коэн

В **1986 году** появился первый вирус для IBM PC-совместимых компьютеров, созданный двумя пакистанскими программистами Basit Farooq Alvi и Amjad Farooq Alvi, распространяющийся через загрузочные сектора и получивший название "пакистанского вируса" (он же Brain, он же Lahore). Отсутствие защитных средств привело к масштабной эпидемии, разрушительный характер которой усиливался тем фактом, что идея саморазмножающихся программ наконец-то вырвалась из лабораторий и стала "общенародным" достоянием программисткой общественности. Сотни хакеров по всему миру потрошили пакистанского вируса и совершенствовали его, создавая свои собственные версии.

В **1988 году** Роберт Таппан Моррис (Robert Tappan Morris) создал и выпустил в Интернет червя, поражающего компьютеры VAX, DEC и SUN под управлением ОС BSD. Различные источники приводят сильно неодинаковые оценки количества зараженных машин, но дело ведь не в количестве. Червь Морриса развеял иллюзию безопасности и заставил многих программистов всерьез задуматься о тех угрозах, которым они подвергаются при подключении к распределенным сетям.

Рисунок 4 Роберт Таппан Моррис

В **1991 году** в дикой природе был обнаружен первый полиморфный вирус, получивший название Tequila, и потребовавший от разработчиков антивирусов принципиально новых алгоритмов детекции.

В **1996 году** появилось сразу два вируса для операционной системы Linux – Bliss, написанный неизвестным хакером и Staog, созданный Quantum'ом (кстати говоря, под MS-DOS к тому моменту уже существовало порядка 4 тыс. вирусов, но — за исключением Червя Морриса — не было известно ни одного вируса под UNIX-подобные системы).

В **1998 году** мир содрогнулся под натиском Win95.CIH (он же "Чих", он же "Чернобыльский Вирус"), заражающего исполняемые файлы формата PE, и затирающего FLASH-BIOS, что "убивало" материнские платы, ломая устоявшееся мнение, что вирусов, выводящих оборудование из строя не существует и существовать не может (хотя еще до "чиха" проскальзывали сообщения о вирусах, ломающих некоторые модели древних мониторов, у которых при неправильных установках видеорежима действительно летел строчечник). В том же году появился первый вирус Strange Brew, написанный на "абсолютно безопасном" языке Java, и опубликованный в электронном журнале Codebreakers#4.

В **1999 году** был обнаружен первый макровирус, поражающий документы Microsoft Word/Microsoft Outlook и распространяющийся по планете со скоростью лесного пожара, что объясняется тем простым фактом, что вирусы, паразитирующие на файлах данных, до этого момента еще не были представлены широкой общественности и потому никто даже не пытался защищаться (на самом деле, первый макровирус появился еще в 1995 году, но по ряду причин не получил широкого распространения).

В **2000 году** появился первый псево-черв "ILOVEYOU", поражающий персональные компьютеры, управляемые операционными системами семейства Windows, и распространяющийся через вложение к электронному письму, написанное на языке Visual Basic Script. Строго говоря, по современной классификации это не червь, а обыкновенная троянская программа, получающая управление в том, и только том случае, если пользователь

оказывается настолько глуп, что соглашается _явным_ образом запустить вложение, полученные из ненадежных источников.

В **2001 году**, впервые после Морриса, появилось сразу шесть новых полноценных червей: Ramen (поражающий Red Hat Linux), Sadmind (поражающий OS Solaris и Microsoft Internet Information Services), Sircam (поражающий Microsoft Windows), CodeRed I/II (поражающий Microsoft Internet Information Services), Nimda (поражающий OS Solaris и Microsoft Internet Information Services) и, наконец, Klez (поражающий Microsoft Outlook и Microsoft Outlook Express).

В **2003 году** черви основательно потрясли сеть, перегрузив магистральны каналы так, что кое-кто даже начал поговаривать о скором конце Интернета. Одна эпидемия следовала за другой и практически никто не избежал заражения: SQL Slammer, Blaster, Welchia, Sobig и Sober атаковали владельцев операционных систем Windows NT используя две уязвимости: дыру в SQL-сервере и ошибку переполнения в службе DCOM RPC. Отдельные разновидности Blaster'a сохраняют свою активность и до сих пор, оккупировав незалатанные машины, количество которых исчисляется миллионами.

В **2004 году** активность червей несколько снизилась, но эпидемии все еще продолжали свирепствовать. MyDoom, Witty, Sasser и Santy своим бурным размножением перегружали каналы и причиняли пользователям множество неудобств, вплоть до полного паралича работы некоторых организаций. В том же году появился первый червь для мобильных телефонов — Cabir.

В **2006 году** вирусы "освоили" RFID-сканеры, используемые в торговле, и выпускаемые по миллиону штук в год, причем, их вычислительные мощности достаточно скромны, и производители антивирусов в них просто не "вписываются", что создает огромную проблему. Угроза масштабных атак вполне реальна, а потенциальные убытки исчисляются сотнями миллиардов долларов, что равносильно экономической катастрофе. Так что мы живем в очень интересное время, гадая пронесет ли нас в очередной раз или все-таки грянет глобальный гром и будет реальный потом, на обломках которого наши потомки будут отстраивать рухнувшую цивилизацию заново.

/ полоса 3, колонка 3 */*
>>> врезка вирус и оси

ось	фирма-создатель	кол-во известных вирусов	дата первого вируса
Amiga OS	Amiga, Inc.	775	?
Free BSD	The Free BSD Project	?	?
HP-UX	Hewlett-Packard	?	?
GNU/Linux	GNU Project, Linus Torvalds	30	?
Mac OS Classic	Apple Inc.	4 - 63	?
Mac OS X	Apple Inc.	0	-
Mac OS X Server			
MS-DOS	Microsoft	около 4,000	январь 1986
Net-BSD	The Net-BSD Project	?	?
Open-BSD	The Open-BSD Project	?	?
OS/2	IBM и Microsoft	?	?
Solaris	Sun	?	?
Windows	Microsoft	около 140,000	?
Black-Berry OS	Research In Motion	1	август 2006
Palm OS	Palm-Source, Inc.	4	сентябрь 2000
Symbian OS	Symbian Ltd.	83	июнь 2004
Windows Mobile	Microsoft	2	июль 2004

Таблица 1 количество вирусов, зарегистрированных в различныз операционных системах (по данным http://en.wikipedia.org/wiki/Virus_statistics)

/* полоса 3, колонка 3 */
>>> врезка основополагающая терминология

Вирус (Virus) — самовоспроизводящаяся программа, паразитирующая на других программах. Инфицированные программы приобретают способность заражать других.

Червь (Worm) — самовоспроизводящаяся программа, распространяющая по сети без участия человека. В отличии от вируса, не являются паразитом и представляет самостоятельную сущность.

Троянский Конь (Trojan Horse) — программа, не обладающая способностями к самовоспроизведению и распространяемая злоумышленником вручную. В другие программы не внедряется, но может прописывать себя в автозагрузку, получая управление при каждом запуске ОС.

Root-Kit – подпрограмма, прячущая другие программы (файлы, процессы, сетевые соединения) от антивирусов.

Малварь (Malware) — обобщенное название всего вредоносного программного обеспечения (червей, вирусов, троянский коней и т.д.).

Начинка (Payload) — подпрограмма, опционально входящая в состав малвари. При определенных условиях выполняет некоторые действия – от видеоэффектов до разрушения информации и установки удаленного shell'a.

/* полоса 4, колонка 1 */
кто и почему пишет вирусы

В 80х годах вирусы создавались высококвалифицированными программистами, освоивших ассемблер и досконально изучивших недокументированные возможности MS-DOS. Глобальных сетей тогда не существовало, сообщения о вирусах носили отрывочный характер и все технические детали приходилось добывать дизассемблером из чужих вирусов или додумывать их самостоятельно. Это было время великих идей, новаторских решений, интеллектуальных поединков и прочих красивых эпитетов. Моральный облик создателей вирусов, конечно, варьировался в очень широких пределах — от чисто исследовательского интереса до желания отомстить всему человечеству, однако, в целом данный период можно окрестить как эпоху романтизма. Большинство хакеров просто не осознавали того ущерба, который они причиняют, а, если даже осознавали, то воспринимали происходящее под углом кибернетических войн, где сильный имеет слабого.

С развитием коммуникационных сетей, между хакерами наладился устойчивый обмен информации, появились специализированные телеконференции и электронные журналы, посвященные вирусам, в результате чего к началу 90х написать вируса мог практически каждый программист, освоивший ассемблер, что он, собственно говоря, и делал. А для чего еще учить ассемблер? Бух и склад можно и на Fox Pro написать… Создание вируса не только являлось хорошим упражнением в системном программировании, но и становилось признаком крутости, возвышая программиста в его собственных глазах и в глазах окружающих. Естественно, качество вирусов, написанных в процессе изучения ассемблера, было невелико и большинство из них оказывалось нежизнеспособно. Агрессивность вирусов находилась в обратной пропорциональности с интеллектом их создателей, стремящихся в первую очередь к разрушению данных и только потом к техническому совершенству. Тем не менее, именно в 90х хакеры изобрели полиморфизм и stealth-вирусы и многие другие прогрессивные технологии.

К концу XX века программное обеспечение "разжирело" настолько, что вирусы, написанные на языках высокого уровня, перестали выглядеть уродами и необходимость корпеть над ассемблером отпала. Как следствие — появилось огромное количество вирусов, написанных на DELPHI, Visual Basic, etc. Хакеры мельчали и деградировали буквально на глазах. Молодое поколение не хотело думать, вирусы уже не воспринимались ни как упражнение в программировании, ни как занимательная головоломка. Они просто писались по инерции или, скорее, по устоявшейся традиции "крутизны" в стиле "пионеры меряются писками". Более опытные программисты находили себе занятие поинтереснее. В самом деле, какой интерес тратить время на разработку и тестирование вируса, если этот труд не будет должным образом оценен и оплачен? Более того, появилась реальная угроза сесть в тюрьму или быть жестоко

избитым коллегами по работе. Романтический ореол, витавших вокруг вирусов, развеялся… Вирусная сцена распалась. Но вирусный бум не прекратился и в обозримом будущем прекращаться не собирается.

/* полоса 4, колонки 2, 3 */
антивирус как часть защитного комплекса

Антивирусы входят практически во все современные защитные комплексы и это правильно, поскольку, один в поле не воин и для отражения атак необходим комплексный подход к проблеме. Антивирусы (при правильном с ними обращении) были и будут весьма эффективным средством подавления вирусных эпидемий, предотвращая "падеж" вычислительной техники, однако, в борьбе с локальными очагами заражения они недостаточно результативны. Антивирус — это что-то вроде полицейского подразделения, стабилизирующего рост преступности в стране на некотором уровне, но принципиально неспособным предотвратить преступление до его совершения. Впрочем, существуют специальные антивирусные вакцины, разработанные специально для этой цели, однако, широкого распространения они так и не получили. А жаль…

Первые антивирусы были устроены по принципу автономных сканеров, запускаемых пользователем (или стартующих вместе с системой) и последовательно проверяющих все файлы один за другим на предмет наличия известных последовательностей байт, идентифицирующих вирус и получивших название сигнатур. Недостаток такого подхода очевиден — стоит слегка переделать любой существующий вирус (причем иметь исходные тексты для этого необязательно) и он окажется незамеченным.

Поскольку, различные антивирусы используют в качестве сигнатуры различные последовательности байт, "правка" вируса существенно усложняется и для решения этой проблемы хакеры обычно прибегают к шифровке вирусного тела статическими или динамическими шифраторами. В первом случае, внутри вируса находится несколько десятков (а то и тысяч!) готовых шифраторов, выбираемых в произвольном порядке. Во втором — вирус конструирует шифраторы на лету, используя большой набор "заготовок" и разбавляя его при необходимости незначащими машинными командами или заменяя одну группу машинных команд блоком эквивалентных ей инструкций. Все эти способы относятся к полиморфным технологиям и эффективно противостоят сигнатурному поиску. В каждом новом поколении, тело вируса изменяется на 99% совершенно непредсказуемым образом. Крошечная часть, отвечающая за его расшифровку, намного более предсказуема. Даже если шифратор не выбирается из заранее заданного набора, а генерируется на лету, количество комбинаций его построения хоть и велико но все же конечно.

Часть разработчиков антивирусов (таких, например, как NOD32) пошла по пути наименьшего сопротивления — размножая каждый попавший к ним вирус в одном-двух миллионах экземпляров, они выделяли в них повторяющие последовательности байт и заносили их в базу, в результате чего для описания _одного_ вируса зачастую требовалось свыше тысячи _различных_ сигнатур, при этом ни у кого не было гарантии, что данный сигнатурный набор — окончательный и исчерпывающий, в результате, антивирус давал определенный процент ложных негативных срабатываний, пропуская от 0,1% до 0,01% штаммов известных ему полиморфных вирусов.

Отечественные разработчики пошли другим намного более технологичным путем, добавив в антивирус виртуальный процессор, эмулирующий выполнение основных x86-команд, и расшифровывающий основное тело вируса с помощью его же собственного шифратора. После завершения расшифровки мы получаем стабильный штамм с устойчивыми сигнатурами, обеспечивающий высочайшее качество детекции (от 99,999% и выше). Минусом данного решения стала резко возросшая сложность антивируса, и "членские взносы" для вступления в антивирусный клуб резко возросли. Если раньше антивирус мог написать практически каждый, то с появлением полиморфных вирусов требования к квалификации программистов ужесточились на пару порядков, и количество игроков на рынке, соответственно, сократилось.

Но даже самые лучшие антивирусные сканеры уже не удовлетворяли потребностей пользователей — вирусы появлялись быстрее, чем их успевали занести в базы и возник устойчивый спрос на превентивные решения (позднее переименованные по маркетинговым соображениям в проактивные технологии). Первыми появились так называемые "мониторы" (от английского "monitor" – радиоперхватчик), перехватывающие обращения к операционной системе на создание/удаление и запись в исполняемые файлы (а так же другие потенциально опасные операции, например, установку резидентной копии в памяти) и обращающиеся к

пользователю за подтверждением. Ох, и веселая же наступала пора! Хакеры быстро придумали кучу способов обхода мониторов, а пользователи были готовы убиться, отвечая на кучу подтверждений, смысла которых они все равно не понимали. Поэтому, через короткий (в масштабах компьютерной индустрии) отрезок времени, мониторы ушли в утиль и были заново воскрешены лишь в конце XX века, но… пользователи по-прежнему давят "yes", не вчитываясь в текст вопроса, и чем больше подтверждений от них требуется, тем сильнее они нервничают.

Намного более успешной оказалась судьба дисковых ревизоров, появившихся приблизительно в одно время со стелс-вирусам (названных по аналогии со Stealth-самолетами), скрывающих факт своего присутствия в системе, что достигается путем перехвата определенных системных функций (например, функции просмотра содержимого каталога) и фальсификации возвращаемого ими результата. Естественно, если спуститься на пару уровеней вглубь, обращаясь непосредственно к контроллеру устройства в обход операционной системе, стелс-вирус тут же появится на радаре.

Дисковые ревизоры реализовали две основных идеи: отслеживание появление новых файлов с контролем целостности старых и сравнение результатов сканирования средствами операционной системы с подлинными данными, полученными путем обращения к контроллеру устройства — любое различие в которых указывает на факт активной маскировки.

Ревизоры оказались удачным дополнением к сканерам — сканеры искали и удаляли до 99,999% известных им вирусов, а ревизоры "ловили" все то, что не поймали сканеры, включая еще неизвестных вирусов, которых пользователи тут же направляли на экспертизу в антивирусные лаборатории, откуда им через некоторое время спускали "вакцину" для сканеров. Плюс еще мониторы (для тех, кто ими умел пользоваться). Сложившая коалиция защитных комплексов оказалась чрезвычайно эффективна и хотя к тому времени на рынке появились аппаратные средства защиты (типа отечественной платы Sheriff) они не выдержали конкуренции, исчезнув так же незаметно как и появились.

Но прогресс не стоят на месте. Размер жестких дисков стремительно увеличивался и сканирование занимало все большее и большее время, тем более, что сканировать приходилось не только исполняемые файлы как раньше, но и файлы документов, в которые уже пробрались вирусы, а количество документов обычно намного превышает количество исполняемых файлов. Сканер, проверяющий диск по несколько часов — малоинтересен и каждый день его запускать никто не будет. Ну, может быть, раз в неделю. Или даже в месяц…

Стало ясно, что так жить нельзя и нужно что-то думать. Вот так и появились активные сканеры, "вгрызающиеся" в операционную систему и перехватывающие функции создания/открытия файлов, проверяя их на лету при первом же к ним обращении. Своеобразный гибрид автономных сканеров и мониторов, получивший повсеместное распространение, однако, вместе с ним пришли и проблемы. Сканирование выполняется не мгновенно, а занимает какое-то время, в результате чего скорость работы компьютера существенно замедляется. С этим еще можно было бы и смириться, если бы не многочисленные ошибки, допущенные создателями антивируса, при разработке перехватчика. Конфликты, критические ошибки приложений, голубые экраны смерти, зачастую сопровождающиеся потерей данных, создают серьезную угрозу для безопасности и ущерб от использования антивируса может быть весьма велик, что вынуждает пользователей отключать активную защиту, ограничиваясь ручной проверкой всех вновь поступивших файлов, однако, такой подход бессилен предотвратить вторжение червей, поскольку черви проникают на компьютер сами, без каких-либо действий со стороны пользователя, а потому полную проверку диска необходимо выполнять хотя бы раз в несколько дней (благо, ее можно перевести в фоновой режим).

/ полосы 5, 6 */*

интервью с Dark Avenger'ом

Рисунок 5 Dark Avenger (Черный Мститель) — легендарный болгарский хакер конца 80х, главным образом известный своим мощным полиморфным движком MtE и вирусом Eddie.

хакер: *вопрос первый, но концептуальный. почему, собственно, вирусы?!*
DA: знаешь, тогда в 80х, когда мы были молодыми, читали фантастику и фантазировали на темы компьютерной жизни, вирусы нам представлялись такими крутыми. Я сам чувак не вполне стерильный (ну ты понимаешь), вот однажды и подцепил заразу. Сейчас даже не помню, что это был за вирус. Помню только, что куча моих данных обратилась в прах, но вместо того, чтобы рыдать над убитыми файлами, я заинтересовался устройством вируса, на целую неделю выпав из жизни и проведя ее за листанием распечаток с карандашом в руках. Разобравшись, я сильно разочаровался, почувствовав, что сам мог бы написать намного лучше. Ну, написал, проиграл,

бросил на полку и забыл. Но потом "схватил" еще один вирус и угаснувший интерес мгновенно разгорелся с новой силой. На этот раз запала хватило на несколько лет за которые были опробованы различные технологии и создана вирусы, заметно выделяющиеся на фоне остальных и вошедшие в легенду еще при жизни.

хакер: *продолжаешь ли заниматься вирусами теперь?*
DA: я, конечно, слегка задвинутый, но все же не настолько! И не настолько умный, как это может показаться из моих интервью с Сарой Гродон. Чтобы не развенчать созданный ей миф, Dark Avenger отошел от дел еще в начале 90х в тот самый момент, когда вирусные технологии, достигнув пика своего развития, пошли на спад, а в "элитарное" сообщество вирусописателей стали вливаться толпы пионеров, пишущих вирусы на Бейсике! Какой интерес их анализировать? Свежих идей в них нет. Полный примитив. А если вас интересуют идеи – отправляйтесь на Black Hat, хотя упадок царит и там. Какое-то запустение ощущается. Это трудно передать словами, но хакерское общество за последнее время сильно опустилось и деградировало.

хакер: *твое напутствие молодым хакерам?*
DA: хакерство — это болезнь, которой нужно хотя бы однажды переболеть, чтобы выработать иммунитет. Вирусы были и остаются объектом серьезных научных исследований и пускай заткнуться тот, кто пытается приравнять хакеров к террористам, а в вирусах видит только вредоносные программы хулиганствующего типа. Разрушение данных — не есть основная сущность вируса. Скажу прямо: чтобы выжить, вирус должен стремиться к симбиозу с операционным окружением и не причинять ни прямого, ни косвенного вреда (в частности, не вызывать перегрузки магистральных каналов связи). К сожалению, хакеры свернули исследовательскую деятельность много лет назад. Мы были первооткрывателями, а молодое поколение только обезьянничает. И хотя вирусы осваивают новые платформы (мобильные телефоны, RFID-сканеры) они эксплуатируют технологии десятилетней давности, адоптированные под новые условия. Грустно. Очень грустно.

интервью с селеной

Рисунок 6 Selena (Селена, в переводе с греческого "Луна") — подпольный разработчик коммерческих root-kit'ов из холодных Нидерландов

хакер: *кто ты такая и чем занимаешься?*
Selena: проблемы самоидентификации меня не волнуют, назовите меня хоть богом, хоть дьяволом — что от этого изменится?! Компьютеры для меня — это все. То есть абсолютно все. Ничего другого у меня просто нет. Я совершенно асоциальный тип. Пиво не пью, на дискотеки не хожу, с парнями не встречаюсь, а мысли о "цивильной" работе приводит меня в ужас, граничащий с суицидом. Но ведь как-то же надо зарабатывать, верно? Сначала я экспериментировала с кредиткам. Потом попалась. Получила срок (условно). Задумалась. Крепко задумалась. Как дальше жить? Создавать шаровары (т.е. условно-бесплатные программы) это не для меня. Вот тогда и начала писать root-kit'ы и продавать их. Сначала осторожно, а затем все смелее и смелее. Сейчас уже подумываю о том, чтобы выйти из тени и легализовать свой бизнес.

хакер: *с этого момента, пожалуйста, поподробнее*
Selena: с точки зрения закона root-kit'ы находятся на пограничной зоне: с одной стороны они повсеместно используются для преступных целей (и мне трудно представить как их можно использовать иначе), с другой стороны — сам по себе root-kit это всего лишь библиотека безобидных функций. Полуфабрикат, непригодный к непосредственному использованию. В ней нет ни "зла", ни "добра", а потому любой вменяемый адвокат легко оправдает разработчика root-kit'а, доказав отсутствие состава преступления и злого умысла.

хакер: *кто твои клиенты? где ты их находишь? каковы цены на root-kit'ы?*
Selena: я исхожу из предположения, что мои клиенты — честные люди до тех пор, пока они не дадут повода подумать обратное. То есть, если человек просит написать root-kit, ничего не говоря зачем он ему нужен — это мой клиент. Если же кому-то нужна атакующая программа, то я отвечаю неизменным отказом. Клиенты ко мне обычно приходят сами. Я проявляю большую активность на хакерских форумах (на всякий случай каждый раз регистрируясь под разными псевдонимами), и потенциальный заказчик может без труда оценить уровень моего мастерства. На ценах подробно останавливаться не буду (пусть это будет моей маленькой коммерческой тайной), скажу лишь то, что они варьируются в очень широких пределах. Устоявшегося рынка нет и одни готовы платить $10.000 за серийный root-kit, уже попавший в антивирусные базы и детектируемый одним или несколькими антивирусами, другие же пытаются раскрутить меня на super-roor-kit'а, поддерживающего кучу операционных систем, и написанного с чистого листа всего за… $100. Что я, дура что ли?!

хакер: *но ты же ведь догадываешься где используются твои создания?*
Selena: догадываюсь? Едва ли… А если даже догадываюсь, то что с того?! Ну хорошо, строго между нами. Root-kit'ы широко используются в атакующих программах, нацеленных как на конкретные организации с целью похищения/уничтожения данных, так и для широкомасштабных заражений сотен тысяч случайных компьютеров, объединяемых в распределенные сети, занимающиеся рассылкой спама или атаками на другие компьютеры. Однако, мне не известно ни одного случая, чтобы для этой цели использовались _мои_root-kit'ы. Может быть, они используются. А быть может, и нет. Кто знает? У меня свой бизнес, основа выживания в котором — отсутствие любопытства. Я зарабатываю _намного_ больше среднестатистического системного программиста, и терять столь лакомый кусок не собираюсь, как не собираюсь оголять задницу, демонстрируя интимные подробности своей работы, особенно сейчас, когда я все еще нахожусь в подполье и просыпаюсь от каждого шороха и шума, преследуя непрекращающимися кошмарами, что меня сейчас повяжут, но ведь и бросить это дело не могу. Почему? Да потому, что ни на что другое я не способна. Увы. Стала бы я связываться с криминалом, если бы умела зарабатывать на жизнь по другому.

интервью с Kerry Noble

Рисунок 7 Kerry Noble – независимый экономист-консультант, проживающий в Норвегии, и специализирующийся на страховании систем обработки данных

хакер: *твои оценки вирусных угроз — насколько они серьезны?*
KN: если верить СМИ, то вирусы уже давно были должны сожрать весь Интернет, но этого почему-то не происходит. Почему? Да потому, что вирусы это не чума XX века, а что-то вроде легкого насморка. Критические инфраструктуры _всегда_ содержат мощные системы резервирования данных, обеспечивающими безболезненный "подъем" после падения. Мелкие компании, обслуживаемые "администратором", только-только научившимся устанавливать Windows Server, конечно, страдают намного больше и мне известно множество фирм, так и не

сумевших "поправиться" после падения и просто свернувших свой бизнес или продавших его конкурентам. Однако, вирусы — далеко не главные виновники. У нас просто принято списывать все проблемы на вирусы. Детальный анализ ситуации не выгоден никому, особенно, если в ходе разбирательств выяснится, что потеря данных произошла, например, из-за сбоя питания или ошибок администратора и/или оператора. Оценки ущерба повсеместно завышаются на несколько порядков. Ни для кого не секрет, что фиктивные убытки, наносимые вездесущими вирусами — превосходный повод для "оптимизации" налогов. Страховые компании, с которыми мне приходилось иметь дело, только в исключительных случаях выплачивают страховку по обозначенному ущербу, превышающего стоимость системы резервирования данных. Действительно, как можно заявлять об убытке в миллиард долларов, если система резервирования стоимостью менее чем в тысячу могла бы предотвратить его? Почему-то считается нормальным покупать сейф за сто тысяч долларов для хранения одного миллиона, но на средства резервирования жалко выделить даже сотую долю от _заявленной_ стоимости потерянных данных.

хакер: *но ведь же отмечены случи смерти людей из-за вирусных атак?*
KN: да, мне известно, когда из-за сбоев медицинского оборудования умирали люди или вирусы парализовали работу информационной службы спасательных организаций и люди погибали уже из-за того, что им не была во время оказана помощь. Конечно, это трагедия. Обелять вирусы никто не собирается, но если говорить о глобальных угрозах, то вирусы тут не при чем. Медики ошибаются гораздо чаще, чем мог бы предположить посторонний наблюдатель. Спасательным организациям вообще свойственно опаздывать, да и спасенных — единицы. Более того, мне вообще непонятно, как вирусы оказываются внутри критических инфраструктур и кого нужно привлекать к ответственности в первую очередь — создателя вируса или лицо (группу лиц), допустивших его вторжение. Это сейчас мы живем в мирное время, а представьте себе, что завтра случится война (в том числе и информационная) — тогда слепые вирусные набеги уступят место целенаправленным профессиональным атакам. Сможем ли мы им противостоять? И хватит ли разрядности у 64-битных компьютеров для подсчета ущерба? Сомневаюсь.

хакер: *какой все-таки ущерб наносят вирусы по твоим оценкам?*
KN: ущерб? Я склоняюсь к мысли, что в глобальном экономическом масштабе вирусы приносят прибыль. Они не только дают пищу разработчикам антивирусов и прочих защитных комплексов, не только позволяют компаниям "оптимизировать" налоги, но и являются мощным маркетинговым оружием, используемым для продвижения новых технологий на рынок, например, операционных систем, да и не только их. Если бы не вирусы, никто бы вообще не задумывался о безопасности и распределенные сети превратились бы в огромную пороховую бочку с термоядерным зарядом, способную взорваться в любой момент. Как говорится, если не можешь изменить ситуацию, то измени свое отношение к ней. Но, к сожалению, безопасность операционных систем все еще не является превалирующим потребительским критерием и вместо того, чтобы мигрировать на платформу, под которой вирусов нет или практически нет (например, Open BSD), все "голосуют" за Windows, а потом, прослезившись, начинают считать убытки. Windows – самая вредоносная система во всех смыслах этого слова, но увы… данный факт все еще никак не дошел до сознания народных масс.