РЕФЕРАТ

На тему

«Эволюция компьютерных вирусов»

Выполнили: Каримов Темирлан,

Изизов Дамир

Шавдунова Ирада

Содержание

ВВЕДЕНИЕ

Компьютерные вирусы сегодня – явление столь обыденное и привычное, что редко кто задумывается, почему эти формы жизни названы именно вирусами, а не, скажем, паразитами. Ответ прост: название позаимствовано из биологии, потому что жизненные циклы вирусов компьютерных и биологических совпадают - внедрение в программу/клетку и дальнейшее размножение. Однако прежде чем выяснять, где и когда появился первый вирус, было бы неплохо узнать четкое определение термина «компьютерный вирус». Такое определение дал в 1986 году Фред Коэн: «Компьютерный вирус есть программа, способная заражать другие программы путем добавления в них собственной копии». Ф.Коэн вообще личность примечательная - первый человек в истории, защитивший докторскую диссертацию по теме компьютерных вирусов. Он доказал невозможность написания программы, которая, глядя на файл, могла бы со стопроцентной точностью сказать, вирус ли это. Теперь можно начинать копаться в истории вычислительной техники, отыскивая первое упоминание о программе, подходящей под определение Коэна.

1 ПЕРВЫЙ ВИРУС

Такое упоминание относится к концу 60-х - началу 70-х годов, когда на машине Univac 1108 появилась программа «Pervading Animal». Собственно, вирусом ее назвать было нельзя, однако это была первая программа, выполнявшая не те действия, которых ожидал от нее оператор, и пытающаяся создавать свои копии. Мысли о создании саморазмножающихся программ начали приходить в голову некоторым людям еще в конце 40-х, когда появилось несколько теорий, связанных с созданием таких программ. Однако первая успешная реализация относится лишь к концу 60-х годов. Доступ к ЭВМ в те годы имели немногие, писать программы для них могли лишь избранные, поэтому впереди у компьютерного сообщества было больше десяти лет спокойствия.
Но вот в середине 80-х компьютеры, теперь уже персональные, становятся общедоступными. С тех пор и ведет свое начало вирусная история.
Первыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II. Оба вируса очень схожи по функциональности и появились независимо друг от друга с небольшим промежутком во времени в 1981 году.

С появлением первых персональных компьютеров Apple в 1977 году и развитием сетевой инфраструктуры начинается новая эпоха истории вирусов. Появились первые программы-вандалы, которые под видом полезных программ выкладывались на BBS, однако после запуска уничтожали данные пользователей. В это же время появляются троянские программы-вандалы, проявляющие свою деструктивную сущность лишь через некоторое время или при определённых условиях.

2 РАСПРОСТРАНЕНИЕ ВИРУСОВ

2.1 (1986) Brain и VIRDEM

Два пакистанских программиста (Basit и Amjad), владеющих компанией Brain Computer Services, создают вирус Brain – первый вирус для MS-DOS. Brain был загрузочным вирусом, и, попав в память при запуске компьютера, заражал boot-сектор всех вставляемых 360-килобайтных дискеток. Вся его полезная нагрузка заключалась в том, что зараженные дискеты имели метку «(c) Brain». Вирус сразу же проявлял себя, поэтому крупномасштабной эпидемии он не вызвал. К тому же, после того как дискеты на 360 Кб ушли в прошлое, вирус стал бесполезен. Но на базовом коде этого вируса было создано целое семейство вирусов, не все из которых были так же безобидны, как Brain. Зачем братьям понадобилось писать и распространять вирус? Существует много точек зрения, но большинство экспертов склоняются к мысли, что идея с вирусом – просто рекламный ход, призванный привлечь внимание к небольшой пакистанской компании. Ведь в коде вируса содержались имена авторов и их адрес.
В том же 1986 году Ральф Бургер пишет безвредный демонстрационный вирус VIRDEM, заражающий *.com-файлы, и представляет его общественности. Интерес к теме столь велик, что Бургеру приходится писать книгу, посвященную вирусам.

2.2 (1987) Jerusalem

В 1987 году появился Jerusalem («иерусалимский вирус»), запрограммированный на удаление зараженных файлов по пятницам 13-го. Первые его версии содержали ошибку, благодаря которой он повторно действовал на уже зараженные файлы. В последующих версиях ошибка была исправлена. Хотя к тому времени уже появились материалы, посвященные безопасности информации, все это воспринималось не более чем игрушкой, экспериментом. Атака застала

пользователей врасплох, так как мир еще не был готов к таким явлениям. Вскоре появились вирусы для ПК Macintosh, Unix-машин и мэйнфреймов IBM.

2.3 Червь Морриса

В 1988 году Робертом Моррисом-младшим был создан первый массовый сетевой червь. 60 000-байтная программа разрабатывалась с расчётом на поражение операционных систем UNIX Berkeley 4.3. Вирус изначально разрабатывался как безвредный и имел целью лишь скрытно проникнуть в вычислительные системы, связанные сетью ARPANET, и остаться там необнаруженным. Вирусная программа включала компоненты, позволяющие раскрывать пароли, имеющиеся в инфицированной системе, что, в свою очередь, позволяло программе маскироваться под задачу легальных пользователей системы, на самом деле занимаясь размножением и рассылкой копий. Вирус не остался скрытым и полностью безопасным, как задумывал автор, в силу незначительных ошибок, допущенных при разработке, которые привели к стремительному неуправляемому саморазмножению вируса.

По самым скромным оценкам инцидент с червём Морриса стоил свыше 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на восстановление работоспособности систем. Общая стоимость этих затрат оценивается в 96 миллионов долларов (в эту сумму, также, не совсем обосновано, включены затраты по доработке операционной системы). Ущерб был бы гораздо больше, если бы вирус изначально создавался с разрушительными целями.

Червь Морриса поразил свыше 6200 компьютеров. В результате вирусной атаки большинство сетей вышло из строя на срок до пяти суток. Компьютеры, выполнявшие коммутационные функции, работавшие в качестве файл-серверов или выполнявшие другие функции обеспечения работы сети, также вышли из строя.

4 мая 1990 года суд присяжных признал Морриса виновным. Он был приговорён к условному заключению сроком на два года, 400 часам общественных работ и штрафу размером 10 тыс. долларов.

2.4 DATACRIME и AIDS

В 1989 году широкое распространение получили вирусы DATACRIME, которые начиная с 12 октября разрушали файловую систему, а до этой даты просто размножались.
Эта серия компьютерных вирусов начала распространяться в Нидерландах, США и Японии в начале 1989 года и к сентябрю поразила около 100 тысяч ПЭВМ только в Нидерландах (что составило около 10 % от их общего количества в стране). Даже фирма IBM отреагировала на эту угрозу, выпустив свой детектор VIRSCAN, позволяющий искать характерные для того или иного вируса строки (сигнатуры) в файловой системе. Набор сигнатур мог дополняться и изменяться пользователем.

В 1989 году появился первый «троянский конь» AIDS. Вирус делал недоступными всю информацию на жёстком диске и высвечивал на экране лишь одну надпись: «Пришлите чек на $189 на такой-то адрес». Автор программы был арестован в момент обналичивания чека и осуждён за вымогательство.

Также был создан первый вирус, противодействующий антивирусному программному обеспечению — The Dark Avenger. Он заражал новые файлы, пока антивирусная программа проверяла жёсткий диск компьютера.

3 90-Е – ВОЗНИКНОВЕНИЕ ПОЛИМОРФНОГО КОМПЬЮТЕРНОГО ВИРУСА

В 1991 году зарегистрирован первый полиморфный вирус, который, чтобы не быть обнаруженным, видоизменял свое тело. В 1992 году появился первый вирус для ОС Windows. Когда операционная система Windows 95 была практически готова, и ее beta-версию разослали 160 тестерам. Все диски оказались зараженными загрузочным вирусом Form, и только один тестер не поленился проверить диск антивирусом. В пресс-релизе, посвященном выходу принципиально новой операционной системы, было сказано, что она полностью защищена от вирусов всех типов. Через несколько месяцев эти заявления были разнесены в пух и прах неожиданным подарком – первым макровирусом, представлявшим собой не привычный исполняемый файл, а сценарий, который заражал документы Microsoft Word. В течение месяца макровирус Concept облетел вокруг земного шара, внедрился в компьютеры пользователей Microsoft Word и парализовал работу десятков компаний по всему миру. В следующие годы вирусописатели активно работали и изобрели множество оригинальных способов проникновения в систему.

Вирусы постоянно расширяют свою «среду обитания» и реализуют принципиально новые алгоритмы внедрения и поведения. Так, в 1995 году появились представители, опровергающие ключевые принципы антивирусной защиты – то, что компьютер, загруженный с заведомо чистой системной дискеты, не может содержать вирус; и то, что вирусы не заражают файлы с данными. Первым появился вирус, который таким образом корректирует конфигурацию компьютера, что при попытке загрузки с дискеты он все равно загружается с зараженного жесткого диска, и вирус активизируется в системе.

Так же год 1995-й запомнился тем, что тогда впервые был создан макровирус. Он заражает документы, подготовленные в системе MS Word for Windows – файлы типа DOC. Так как такие файлы ежедневно десятками тысяч циркулируют в локальных и глобальных сетях, эта способность вируса обеспечила его мгновенное распространение по всему свету в течение нескольких дней и 25 августа 1995 года он был обнаружен в Москве. Вирус написан на макроязыке пакета Word. Он переносит себя в область глобальных макросов, переопределяет макрос FileSaveAs и копирует себя в каждый файл, сохраняемый с помощью команды Save As. При этом он переводит файл из категории «документ» в категорию «шаблон», что делает, невозможным его дальнейшее редактирование. Обнаружить наличие этого вируса можно по появлению в файле winword6.ini строки ww6i=1.

4 ПОЯВЛЕНИЕ СЕТЕВЫХ МАКРОВИРУСОВ

В 1996 году появился макровирус Laroux для Excel, а в 1998 — для Access. Годом позже вирусы добрались до электронной почты, и печально знаменитая Melissa почти мгновенно проникла на сотни тысяч компьютеров, рассылая себя через адресную книгу Outlook Express. В 1997 году на свет появились новые виды вирусов – FTP– и mIRC-черви, в июне 1998 года – вирус Win95.CIH. Этот вирус активизировался 26 апреля (впервые – в 1999 году) и уничтожал информацию на жестком диске, записывая на него мусор. Кроме того, он перезаписывал Flash BIOS, если переключатель находился в положении, разрешающем запись, и выводил из строя материнскую плату.

В следующем году эта же идея, правда, существенно модернизированная, нашла воплощение в черве Love Letter, который парализовал работу электронной почты во всем мире. Тогда же отмечены первые масштабные DDoS-атаки на ряд известных Web-сайтов, вызвавшие отказ в обслуживании пользователей. В прошлом году появилось сразу несколько вирусов, которые распространялись не через электронную почту, а непосредственно через сетевые порты, используя брешь в системе безопасности Windows. Главная их особенность — огромная скорость распространения.

5 ТРОЯНСКИЕ ПРОГРАММЫ НОВОГО КЛАССА

Следует отметить, что в те же дни были замечены первые признаки объединения создателей вирусов и спамеров. «Троянские» программы нового класса внедряли на зараженном компьютере прокси-сервер, который затем без ведома владельца ПК использовался для рассылки спама. Это опасное явление свидетельствует о нарастающей криминализации Интернета. Теперь вредоносные программы пишут не из хулиганских побуждений, а ради наживы — заработать можно, например, на рассылке спама или используя так называемое «шпионское» ПО. Новым словом в вирусологии стал вирус под названием «Чернобыль» или WIN95.CIH. Данный вирус в отличие от своих собратьев в зависимости от модификации мог уничтожать MBR жесткого диска, таблицу размещения данных и не защищенную от перезаписи Flash-память. Волна эпидемии этого вируса прокатилась по всему миру. Громадный материальный ущерб был нанесен в Швеции. 26 апреля 1999 года пострадало большое количество пользователей и в России. Эпидемия вируса Win95.CIH была на тот момент самой разрушительной. Червь I love you, выпущенный на Филиппинах в мае 2000 года, нанес владельцам компьютеров ущерб на сумму, по некоторым оценкам превышающую $10 млрд. Следующий червь, вошедший в историю как Code Red, за 14 часов сумел заразить более 300 тыс. компьютеров, подключенных к Интернету. После них были и другие, часто – первые в определенной категории. Например, Nimda (слово admin, прочитанное наоборот), многовекторный червь, распространялся сразу несколькими способами, включая «черные ходы», оставленные другими червями. MyDoom был признан самым быстрым червем, распространяющимся по электронной почте. До этого большая часть вирусов была написана на языке низкого уровня – ассемблере, позволявшем создать небольшой оптимизированный вирус. Автором червя AnnaKournikova, который поразил Интернет в феврале 2001 года, оказался голландский студент, который вообще не умел программировать, даже на таком простом языке, как Basic.

6 ВИРУСЫ В WINDOWS

В 1995 году официально вышла новая версия Windows — Windows 95. На пресс-конференции, посвящённой её выходу, Билл Гейтс заявил, что с вирусной угрозой теперь покончено. Действительно, на момент выхода Windows была весьма устойчива к имеющимся вирусам для MS-DOS. Однако уже в августе появляется первый вирус для Microsoft Word (Concept), который за несколько недель распространился по всему миру.

В 1996 году появился первый вирус для Windows 95 — Win95.Boza. В марте 1996 года на свободу вырвался Win.Tentacle, заражающий компьютеры под управлением Windows 3.1. Эта была первая эпидемия, вызванная вирусом для Windows. Июль 1996 отмечен распространением Laroux — первого вируса для Microsoft Excel. В декабре 1996 появился Win95.Punch — первый резидентный вирус для Win95. Он загружается в систему как VxD-драйвер, перехватывает обращения к файлам и заражает их.

В феврале 1997 года отмечены первые макровирусы для Office97. Первые из них оказались всего лишь «отконвертированными» в новый формат макровирусами для Word 6/7, однако практически сразу появились вирусы, ориентированные только на документы Office97. Март 1997: ShareFun — макровирус, поражающий MS Word 6/7. Для своего размножения использует не только стандартные возможности MS Word, но также рассылает свои копии по электронной почте MS-Mail. Он по праву считается первым mail-червём. В июне появляется и первый самошифрующийся вирус для Windows 95.

В апреле 1997 года появляется и первый сетевой червь, использующий для своего распространения File Transfer Protocol (ftp). Так же в декабре 1997: появилась новая форма сетевых вирусов — черви mIRC.

Начало 1998 года отмечено эпидемией целого семейства вирусов Win32.HLLP.DeTroie, не только заражавших выполняемые файлы Win32, но и способных передать своему «хозяину» информацию о заражённом компьютере.

Февраль 1998: обнаружен ещё один тип вируса, заражающий формулы в таблицах Excel — Excel4.Paix. В марте 1998 года появился и AccessiV — первый вирус для Microsoft Access, также в марте был обнаружен и Cross — первый вирус, заражающий два различных приложения MS Office: Access и Word. Следом за ним появились ещё несколько макровирусов, переносящих свой код из одного Office-приложения в другое.

В феврале-марте 1998 отмечены первые инциденты с Win95.HPS и Win95.Marburg, первыми полиморфными Win32-вирусами. В мае 1998 началась эпидемия RedTeam, который заражал EXE-файлы Windows, и рассылал заражённые файлы при помощи электронной почты Eudora.

В июне началась эпидемия вируса Win95.CIH (из-за даты активации 26 апреля также известного как «Чернобыль»), ставшая самой разрушительной за все предшествующие годы. Вирус уничтожал информацию на дисках и перезаписывал Flash Bios, что вызвало физические неисправности у сотен тысяч компьютеров по всему миру.

В августе 1998 появилась широко известная утилита BackOrifice (Backdoor.BO), применяемая для скрытого администрирования удалённых компьютеров и сетей. Следом за BackOrifice были написаны несколько других аналогичных программ: NetBus, Phase и прочие.

Также в августе был отмечен первый вирус, заражающий выполняемые модули Java — Java.StangeBrew. Этот вирус не представлял какой-либо опасности для пользователей Интернет, поскольку на удалённом компьютере невозможно использовать необходимые для его размножения функции. Вслед за ним в ноябре 1998 появился и VBScript.Rabbi. Интернет-экспансия скриптовых вирусов продолжилась тремя вирусами, заражающими скрипты VisualBasic (VBS-файлы), которые активно применяются при написании Web-страниц. Как логическое следствие VBScript-вирусов стало появление полноценного HTML-вируса (HTML.Internal).

1999 год прошёл под знаком гибридного вируса Melissa, побившего все существовавшие на тот момент рекорды по скорости распространения. Melissa сочетал в себе возможности макровируса и сетевого червя, используя для размножения адресную книгу Outlook.

Правоохранительные органы США нашли и арестовали автора Melissa. Им оказался 31-летний программист из Нью-Джерси, Дэвид Л. Смит. Вскоре после ареста Смит начал плодотворное

сотрудничество с ФБР и, учтя это, федеральный суд приговорил его к необычно мягкому наказанию: 20 месяцам тюремного заключения и штрафу в размере 5 000 долл. США.

В апреле был найден и автор вируса CIH (он же «Чернобыль»), которым оказался студент Тайваньского технологического института Чень Инхао (陳盈豪, CIH — его инициалы). Однако, из-за отсутствия жалоб на действия вируса со стороны местных компаний, у полиции не было оснований для его ареста.

Также в 1999 году был отмечен первый macro-вирус для Corel — Gala. в начале лета 1999 грянула эпидемия Интернет-червя ZippedFiles. Этот червь интересен тем, что являлся первым упакованным вирусом, получившим широкое распространение в «диком» виде.

2003-2012 эпидемия вируса Win32.Sality (авторское название КуКу). Данный полиморфный вирус состоит из нескольких частей, использует систему шифрования и маскировки. Изменяет содержимое исполняемых файлов, что делает невозможным их полное восстановление. В связи со сложным поведением и средствами маскировки, лечение данного вируса представляет собой невыполнимую задачу для обычного пользователя. Зараженный компьютер становится частью сети Sality, являющейся одной из самых крупных ботнет сетей в мире.

7 ВИРУСЫ XXI ВЕКА

7.1 2001 — атака на сервера

После неимоверного успеха «почтовых вирусов» антивирусные компании закрывают дыры в безопасности и вирусы переключаются на публичные сайты и сервера. Собственно с 2001 года и можно отсчитывать современную эпоху в компьютерной безопасности. Один за одним идут «серверные вирусы»: Code red — вирус, использующий уязвимости Microsoft Internet Information Server. Также известный как Bady, Code Red предназначался для нанесения максимального ущерба, все зараженные им сайты выглядели соответственно. После этого вирус начинал поиск других уязвимых сайтов. Приблизительно через 20 дней все веб сайты должны были начать DDoS (distributed denial of service) атаку на определенные IP адреса, включая Web-сервер Белого Дома. Меньше чем через неделю, вирус заразил около 400,000 серверов. Ущерб составил $3 миллиарда.

7.2 2003 — заражение сайтов

Сразу два червя начинают массовое заражение интернет-сайтов: Blaster и Sobiq. За первые же сутки Собик производит более миллиона собственных копий. Цель вируса — получить все возможные электронные адреса хранящиеся на компьютере и передать им свою копию. Ну а MSBLAST.exe не нуждается в представлении, думаю, все помнят его в лицо:

Главной задачей мсбласта была DDOS атака на сайт windowsupdate.com — все зараженные машины с 16 августа начинают беспрерывно отправлять запросы на обновление системы и сайт падает, не выдержав нагрузки.

Совокупный ущерб от червей составил $20 миллиардов. Microsoft объявило награду в 250,000 $ для любого, кто может предоставить информацию о создателе Sobiq.F. Ищут до сих пор. Побочным эффектом обоих червей стал колосальный рост интернет-траффика. Этот эффект нашел свое применение уже в следующем году.

7.3 2004 — интернет останавливается

Неизвестная группа хакеров запускает цепную реакцию из трех коварных червей. 18 января интернет поражает 100 модификаций червя Bagle. Он рассылает себя по почте как и Собик, но

при этом на зараженном компьютере открывается доступ к порту TCP, который может использоваться для выуживания злоумышленником любой интересующий его информации. Все копии вируса самоуничтожаются 28 января 2004 года.

А уже 26 января начинается эпидемия MyDoom. Распространялся по почте и через пиринговую сеть Kazaa. Но в этот раз эффект почувствовали не только пораженные машины — на пике эпидемии червь увеличил загрузку интернета на 10 процентов, а время загрузки Web-сайтов на 50%.

Результат был настолько успешен, что в первые часы инфицирования на каждые 10 отосланных писем приходилось одно инфицированное этим вирусом. MyDoom был запрограммирован на прекращения своего распространения после 12 февраля 2004 года.

30 апреля интернет добивает третий червь — Sasser. Используя уязвимости Windows 2000 и XP вирус достиг значительных успехов и вызвал отключение спутниковой связи для нескольких французских новостных агентств. Также этот вирус вызвал отмену нескольких авиарейсов копании Delta Airline и отключение компьютеров многих компаний во всем мире. После успешного копирования, червь начинал поиск других незащищенных систем и копировал себя. Зараженные этим вирусом компьютеры отличались редкой нестабильностью работы и частыми перезагрузками, вызванными в сбое процесса lsass.exe:

В итоге расследования автором вирусов был назван 17-летний школьник из Германии, запустившим мировую эпидемия в качестве подарка себе на день рождения. Из-за несовершеннолетия он избежал какого-либо наказания.

С этого момента эксперты перестают подсчитывать ущерб от вирусов, т.к. суммы переваливают за десятки и сотни миллиардов долларов.

В ноябре 2004 года появляется и первый червь распространяющийся только через веб-сайты. Santy был написан на скриптовом языке Perl и использующий уязвимости форумов на phpBB. Вирус просто отправлял в гугл запрос, содержащий строку «Powered by phpBB», и получал таким образом адреса атакуемых форумов. Затем, сформировав некорректный запрос к файлу viewtopic.php, получал возможность выполнять на сервере произвольный код и заменял содержимое всех файлов с расширением asp, htm, jsp, php, phtm, shtm на «This site is defaced!!! This site is defaced!!! NeverEverNoSanity WebWorm generation X», где X — номер поколения червя.

Уже за сутки с момента своего появления 20 декабря 2004 червём было удачно атаковано 40 тысяч сайтов. На вторые сутки Google уже не проводил поиск по фразе «Powered by phpBB». После этого появились модификации червя, использующие другие поисковые системы.

7.4 2007 — эра ботнетов

Теперь вирусы не просто инфицируют сайты, они создают ботнеты и защищают их. Червь Storm появился 17 января 2007 года и только за первую неделю заразил два миллиона компьютеров.

По инерции Storm называют «червём», хотя на самом деле эта зараза комплексного характера, и помимо метода распространения, характерного для почтовых червей, Storm Worm имеет функции трояна/бэкдора, а также может выполнять роль «DDoS-бота» — программы, используемой для проведения DDoS-атак.

Но главной проблемой является даже не сам червь, а созданная им сеть заражённых компьютеров. Её точные размеры точно не известны, но по некоторым оценкам, количество

компьютеров-«зомби» уже перевалило за несколько десятков миллионов. Таким образом, совокупная вычислительная мощь ботнета, созданного Storm, может в разы превосходить самые мощные суперкомпьютеры планеты.

Известный специалист в области компьютерной безопасности Брюс Шнайер в октябре утверждал, что размеры ботнета по-прежнему колеблются между 1 и 50 миллионами. По мнению Шнайера, Storm — это будущее вредоносных программ как таковых. Ботнет Storm ведёт себя как колония муравьёв с чётким распределением ролей между машинами.

Эпидемия червя началась с компьютеров в Европе и Соединенных Штатах 19 января 2008 года, когда, прикрываясь темой урагана в Европе, пользователям повалились письма с предложением открыть вложенный файл с названиями Full Clip.exe, Full Story.exe, Read More.exe или Video.exe.

Все попавшиеся на удочку машины автоматически объединялись в ботнет, но в отличие от других сетей, он не использовал специальный управляющий сервер, доступ к которому легко перекрыть. Принцип управления Storm больше напоминает пиринговую сеть, в которой зараженные ноды подключаются к своему управляющему хосту (он руководит обычно 30-45 зомби), а хосты взаимодействуют между друг другом. Причем роль хоста в случае необходимости может занять любая из нод. Вся сеть устроена так, что полного списка нодов нет ни у кого, поэтому точные размеры ботнета так и остались загадкой.

Помимо функций по работе с ботнетом, Storm устанавливает в системе руткит: Win32.agent.dh, посредством которого держатели ботнета могли стащить любую конфиденциальную информацию, рассылать спам и устраивать мощные DDoS-атаки.

Как утверждает Джош Корман, сотрудник подразделения IBM Internet Security Systems, червь Storm отслеживает IP-адреса, с которых совершаются попытки зондирования его управляющих серверов, и организует DDoS-атаки на эти адреса. По словам эксперта, в результате исследователи, которым удалось собрать какие-то факты о Storm, боятся их публиковать.

7.5 2010 — это война

Этот год стал поворотным пунктом в истории компьютерной безопасности, т.к. вирус Stuxnet вывел из строя атомную программу Ирана. Используя уязвимость Microsoft Windows, вирус заражал компьютеры, но ничем себя не выдавал — его целью были контроллеры марки Simatic Step 7, использующиеся в центрифугах для обогащения урана. Stuxnet скрытно прописывает себя на программируемые чипы (их используют для контроля за производством), маскируется и убивает какой-то важный процесс. Не случайный процесс, а возвращающий определенный код. К сожалению, что этот код значит, пока неизвестно. Но именно в 2009-2010 годах на иранских урановых фабриках начались массовые поломки центрифуг, приведшие к остановке всей ядерной программы.

Причем для создания вируса явно были приложены усилия крупной организации с неограниченным бюджетом. Вирус занимает полмегабайта кода на ассемблере, C и C++. Более того — вирус был подписан краденой цифровой подписью. Злоумышленники скорее всего украли подписи из тайваньских отделений фирм MicronJ и RealTek. Странный факт, но офисы этих фирм находятся в одном и том же здании в городе Шинчу. Если это не простое совпадение, то это значит кто-то физически проник в комнаты, зашел на соответствующие компьютеры, выкрал ключи. Тут уже никак не списать произошедшее на действия школьника-одиночки.

8 САМЫЕ ИЗВЕСТНЫЕ КОМПЬЮТЕРНЫЕ ВИРУСЫ

Количество современных компьютерных вирусов, бродящих по Интернет-сайтам, жёстким дискам и флешкам, так велико, что не вписывается ни в какие рамки. Зачем они отравляют наши компьютеры и наши жизни? Для какой цели их создавали? Одни вирусы крадут ваши логины и пароли, другие блокируют доступ к системе, третьи превращают ваш компьютер в спам-бота... Их объединяет одно - они созданы для того, чтобы приносить доход своим творцам. Вирусы, крадущие ваши данные для входа на различные сайты, отправляют их хозяину, который с прибылью продаёт их на чёрном рынке. Вирусы, блокирующие компьютер, требуют от вас отправки SMS на короткий номер. И, наконец, вирусы, превращающие вашу машину в спам-зомби, заставляют её отправлять сотни рекламных писем, за которые организатору ботнета также солидно платят.

Тем необычнее и тем привлекательнее для нас старые добрые вирусы прошлого, которые были созданы не ради наживы, а просто так, похулиганить. Показать пользователю издевательскую надпись или неприличную картинку, нарисованную псевдографикой, удалить с его компьютера все картинки... Авторы компьютерных вирусов 80-х и 90-х мечтали не заработать с помощью своих вредоносных творений миллионы, а всего лишь услышать в толпе про созданные ими вирусы или прочитать в газетах о том, какой же они принесли вред мировым компаниям. Сегодня это кажется нам странным, но тогда компьютерный мир был в основном свободен от бизнеса и финансов - это было время компьютерных гениев и компьютерных хулиганов.

Постепенно деньги становились важнее собственного "я", и вирусы начали писаться либо ради собственной наживы, либо на заказ. "Хулиганские" вирусы ещё существовали некоторое время, однако это хулиганство было совершенно другого рода. Уже не круто поиздеваться над одним пользователем, гораздо круче организовать ботнет и устроить DDoS-атаку на сервер крупной компании или правительственной структуры... Впрочем, вскоре исчезли и они. Давайте вспомним самые известные из этих вирусов, не принесших своим создателям ничего, кроме мировой известности и уголовных проблем, связанных с разработкой вредоносного ПО.
Компьютерные вирусы были всегда - говорят, что первые вредоносные программы были даже на больших ЭВМ размером с квартиру. Однако первым вирусом, заставившим о себе говорить даже некомпьютерщиков, был вирус Brain, созданный в далёком 1986 году. О том, что создание вируса было чистой воды хулиганством, говорит даже тот факт, что его авторы, пакистанские братья Басит Фарук Алви и Амджад Фарук Алви, "зашили" в тело вируса телефонный номер своей фирмы по ремонту компьютеров. Деструктивное проявление Brain было тоже довольно оригинальным: инфицируя загрузочный сектор бывших в то время в обращении пятидюймовых дискет на 360 килобайт, он постепенно и незаметно заполнял до отказа всё содержимое дискеты. В 1980-х, когда жёсткими дисками оснащались далеко не каждые компьютеры, а на дискетах был важен каждый килобайт, Brain принёс действительно много бед. Его было крайне сложно удалить, так как он, будучи первым в истории stealth-вирусом, прятался в загрузочном секторе, который в то время не проверялся антивирусами. Позднее эту технологию применили ещё несколько вирусов, правда, вскоре разработчики антивирусов наделили свои программы возможностью проверять загрузочный сектор, а производители BIOS включили опцию, предотвращающую загрузку вредоносного кода с дискет, и эти вирусы прекратили своё существование.

Вирус Brain распространялся по компьютерам мира с помощью дискет, так же, как сейчас вирусы типа AutoRun распространяются с помощью флешек. А вот вирус Morris, появившийся в 1988 году, был первым червём, использующим для своего распространенияВсемирную сеть. Интересно, что создатель вируса, Роберт Таплан Моррис, вовсе не задумывался о том, чтобы сделать вредоносную программу; по замыслу, Morris должен был всего лишь определить размер тогдашнего Интернета, поселяясь на всех компьютерах, включённых в эту сеть. Причём стоит обратить внимание на тот факт, что Роберт включил в свою программу систему защиты от

удаления, дабы пользователи и администраторы не удалили Morris и один компьютер не был засчитан дважды. Однако благая идея обернулась ночным кошмаром, и Morris, подобно мутанту из комиксов, из исследовательского инструмента превратился в серьёзную опасность. Компьютеры заражались Morris'ом, заражали им других, сами многократно перезаражались... Вышедший из-под контроля эксперимент нанёс значительный урон тогда ещё немногочисленной, но уже тогда всемирной компьютерной сети.

Но всё же самым известным из вирусов прошлого был "Чернобыль" - Win95.CIH. Созданный тайваньским выпускником университета Ченом Инь Хау в 1997 году, он и до сих пор остаётся одним из самых опасных и вредоносных вирусов. Действие "Чернобыля" напоминало действие бомбы с таймером. До наступления 26 апреля, годовщины катастрофы на Чернобыльской электростанции и дня рождения автора, вирус выдавал себя лишь постепенным увеличением занятого пространства на диске (за что и получил ещё одно название - Spacefiller) да инфицированием всех исполняемых файлов на компьютере. Ну а когда наступал "час X", "Чернобыль" отрывался по полной: удалял всё содержимое жёсткого диска, а на некоторых компьютерах даже портил BIOS, превращая компьютер в груду бесполезного хлама. Так глубоко, пожалуй, не "гадил" ни один вирус планеты. Всего около пятисот тысяч компьютеров пострадали от зловредных действий Win95.CIH. Слава богу, в 2000 году Чена всё же арестовали власти Тайваня, и он не успел создать что-нибудь ещё разрушительнее.

Ну и, конечно же, наш список был бы неполным, если бы мы не упомянули о двух вирусах, распространившихся по всему миру в конце 90-х - начале 2000-х посредством электронной почты: Melissa и ILOVEYOU. Первый представлял собой макровирус, "зашитый" в Word'овский файл и отправленный тысячам пользователей Интернета в качестве вложения. Этот вирус рассылал свои копии первым пятидесяти адресатам в списке контактов Outlook, а также изрядно портил текстовые файлы пользователя инфицированного компьютера, изменяя произвольные блоки текста на цитаты из "Симпсонов". Вирус ILOVEYOUраспространялся примерно таким же методом: запуская добавленный к письму скрипт, замаскированный под txt-файл с признанием в любви от молодой девушки, пользователь автоматически заражал свой компьютер. ILOVEYOU распространялся не только посредством e-mail, но и с помощью носителей информации, что принесло ему куда большую распространённость, чем Melissa. Вирусом ILOVEYOU были заражены как компьютеры домашних пользователей, так и рабочие компьютеры, и даже компьютеры сотрудников Пентагона. Примечательно, что основной ущерб от вируса ILOVEYOU был причинён во время процедуры его удаления, поскольку для этого были отключены многие компьютерные сети и даже целые почтовые серверы.

Итак, мы рассказали вам о пяти самых знаменитых компьютерных вирусах прошлого. Мы не рассказали о многих других, не менее легендарных, вирусах, начиная от ветхозаветных Cascade и Dir II и заканчивая нашумевшими в своё время Code Red и, конечно же, Blaster. Однако на описание всех вирусов, заслуживающих внимания, не хватило бы и целой книги, так что мы оставляем это увлекательное занятие за вами, дорогой читатель.

9 САМЫЕ ИЗВЕСТНЫЕ ХАКЕРЫ В ИСТОРИИ

Что больше всего раздражает обыкновенных пользователей, которым компьютеры нужны как для работы, так и для развлечений? Пожалуй я не открою Америку, сказав, что самое большое раздражение, а порой даже то, что вызывает злость у «юзеров», этокомпьютерные вирусы, троянские программы, спам и всё остальное, что связано со сбоем работы компьютера не по вине пользователя. Естественно, люди пытаются найти защиту для своих компьютеров, устанавливая различные антивирусы и прочие программы, которые следят

за безопасностью компьютера. В большинстве случаев, грамотные действия при работе с антивирусом, гарантирую безопасность вашего компьютера. Однако речь не про это, а речь про то, что если эти все вирусы попадают на наши компьютеры, то значит, их кто-то создаёт. Кто эти люди, и зачем им это?

Вопрос конечно неоднозначный. Людей, которые создают вирусы и прочее вредоносное ПО, называют хакерами, а занимаются они этим по всяким причинам, иногда для развлечения, иногда из личных интересов, но всё-таки чаще всего, из-за желания наживы. Однако к счастью, хакеры, это не только те люди, которые приносят вред нашим компьютерам. Существует и другая разновидность хакеров, которая как раз то наоборот, помогает различным компаниям бороться с вирусами, либо они тестируют различные программы на безопасность. Иногда такие хакеры не работают в организациях, а работают лишь сами на себя, тем самым создавая своё дело, однако где бы они не работали, главное их условие, это не нарушать закон, а лишь искать лазейки в законе для своих действий. В общем, условно говоря, существует два вида хакеров, одни которые «приносят вред», называют «Чёрными шапками», а те хакеры которые помогают компаниям в разработке продуктов, называют «Белыми шапками».

Что ж, давайте сделаем небольшой обзор самых известных хакеров на планете, распределив их на две группы: «Белые шапки» и «Чёрные шапки».

9.1 Белые шапки

Номер один в этом списке, является Стивен Возняк. Этот один из отцов Apple, наравне со Стивом Джобсом. Некоторые называют этого человека Воз, либо Стивен из Apple, однако мы будем его называть, как и полагается. Ещё в студенческом возрасте, Стивен уже тогда начал заниматься хакерством, а именно начал создавать блю-боксы, благодаря которым можно было с обыкновенного стационарного телефона, звонить по межгороду совершенно бесплатно. Продажа таких блю-боксов – первый бизнес Возняка и Джобса. После Стивен Возняк бросил учёбу и вместе с Джобсом, решил создать полноценный компьютер в едином корпусе. Это был действительно первый настоящий успех этих двух парней, которые сейчас известны на весь мир. На сегодняшний день, Стивен Возняк не работает в Apple, а стал заниматься благотворительностью, помогая детям осваивать современные технологии.

Следующей «белой шапкой», является Тим Бернерс-Ли. Что он сделал? Он создал сеть, которая сейчас называется World Wide Web. Другими словами, Тим создал интернет. Однако прежде чем создать всемирную паутину, Тим Бернерс-Ли, еще, будучи студентом,взломал шифрованные коды своего университета. После того случая, ему напрочь запретили подходить ко всем компьютерам, которые находились в Оксфордском университете.

Третьим в нашем списке является Линус Торвальдс. Это человек, который создал самую известную бесплатную операционную систему Linux. Как заявляет сам Линус, он получает удовольствие от того, что разрабатывает самую лучшую ОС в мире. Впервые он начал разрабатывать свою систему на компьютере Sinclair QL. Он самостоятельно модифицировал его, разработав под модифицированную установку несколько игр и текстовый редактор. После он набрал команду таких же программистов-любителей, как и он, и они совместными усилиями создали операционную систему Linux. На сегодняшний день, Линус Товальдс является одним из руководителей так называемого братства Линукс. Кроме того, он является почётным преподавателем в области компьютерных технологий, во многих европейских университетах.

Ещё одним представителей «белых шапок», является Ричард Столлман. Сам Столлман любит, когда его называют «RMS», а прославился этот RMS тем, что является одним из отцов бесплатного программного обеспечения. По заявлениям самого Столлмана, будущее

компьютерной индустрии за бесплатным программным обеспечением, а всё платное ПО, рано или поздно уйдёт в небытие, так как не сможет конкурировать с бесплатным, но ничем не хуже, софтом. Вся карьера этого человека и связана лишь с продвижением бесплатного софта, поэтому он является почётным сотрудником, в некоторых авторитетных организациях, которые занимаются разработками подобного рода.

Наконец замыкает нашу пятёрку «белых воротничков» хакер по имени Тсутому Шимомура. Данный хакер получил славу «белого воротничка», наверно, сам того не подозревая, а дело было вот как: однажды его взломал известный хакер Кевин Митник. Этот факт настолько разозлил Шимомуру, что он задался идеей во, чтобы то не стало, найти его, а также он стал сотрудничать с ФБР для помощи поимки других хакеров. Однако, не смотря на то, что он помогал ФБР в области киберпреступлений, он и сам был не без грешка и достаточно часто взламывал мобильные телефоны для прослушки. В конце концов, когда Митник был задержан, Шимумора написал книгу о своей жизни, по мотивам которой, даже был снят фильм.

9.2 Чёрные шапки

Ну а сейчас мы рассмотрим наиболее известных «чёрных шапок», или другими словами тех, хакеров, которых ненавидит почти всё население земли.

Чёрной шапкой номер один, без сомнений можно назвать Кевина Митника. Федеральное Бюро Расследований, до сих пор считает его самым известным хакером в мире. По мотивам его киберпреступлений, было снято аж два фильма. А начинал Митник с достаточно безобидного взлома транспортной системы Лос-Анжелесса с целью получения бесплатного проезда в общественно транспорте. Дальше - больше, затем он начал взламывать целые телефонные сети, крал важные данные с чужих компьютеров, ему даже удалось проникнуть в Американскую систему военной безопасности. Конец его хакерской деятельности пришёл тогда, когда он взломал компьютер Тсутому Шимомура, о котором писалось выше. Наконец, после почти 6 лет тюремной камеры, он стал «полезным гражданином» и сейчас занимается тем, что помогает разрабатывать защитное ПО.

Ещё одна «черная шапка», это Адриан Ламо. Известен он тем, что взламывал сети известнейших компаний, в том числе таких гигантов, например Microsoft, Yahoo и многих других. В принципе, этого человека можно было бы отнести и к белым шапкам, потому как он занимался тем, чем и они, но проблема лишь в том, что белые шапки, никогда не нарушали закон, в, то время как Ламо, этим не удосуживался. Почти всегда, он выходил в сеть из разных мест: кафе, библиотек, и других массовых мест скопления людей, в результате чего, он получил прозвище «Бездомный хакер». Несколько лет назад, этот человек всё-таки был пойман, но получил относительно лёгкое наказание: полгода домашнего ареста. На сегодняшний день, Адриан Ламо завершил свою хакерскую деятельность и стал работать журналистом.

Третья «чёрная шапка» - это Джонтан Джеймс. Трудно поверить, но первый тюремный срок за хакерство, он получил ещё в шестнадцатилетнем возрасте. Джонатан Джеймс – это человек, который смог взломать одно из подразделений Министерства Обороны Соединённых Штатов, а также проникнул в защищённую сеть НАСА и выкрал оттуда совершенно секретного ПО, стоимость которого оценивалась в несколько миллионов! На сегодняшний день, Джонатан Джеймс – это молодой компьютерный гений, который планирует открыть собственную компанию, занимающуюся защитой секретной информации.

Четвёртым в списке «чёрных шапок», является Роберт Моррис. Это первый человек в мире, который разыскивался по конвенции Компьютерного мошенничества. Именно Моррис создал первый компьютерный червь, который распространялся по интернету. Из-за его действий,

пришло в неисправность более 6000 компьютеров. На сегодняшний день, Роберт Моррис – это штатный работник в одной из компьютерных лабораторий, которая занимается совершенствованием компьютерных технологий.

Пятым хакером в рейтинге «чёрных шапок», является Кевин Поулсен. Этот хакер прославился тем, что взламывал закрытые телефонные сети. Однако наивысшим его достижением, является взлом базы данных ФБР, в результате чего, у него появился доступ к секретной информации. Для ФБР было делом чести найти этого киберпреступника. После его поимки, его осудили на 5 лет тюрьмы общего режима. На сегодняшний день, он работает главным редактором в крупной американской газете.

10 ИСТОРИЯ МОБИЛЬНЫХ ВИРУСОВ

Вирусы для мобильных телефонов, смартфонов и планшетных компьютеров - не миф, а жестокая быль сегодняшнего дня. Отрицать проблему массового распространения мобильных вирусов так же глупо и нелепо, как отрицать проблему массового распространения вирусов для компьютеров. Антивирусы для смартфонов входят в число самых продаваемых мобильных приложений, а сеть кишит рекомендациями по защите от мобильных вирусов - одним словом, всё как на "больших" компьютерах. А ведь первый мобильный вирус был создан не для того, чтобы навредить кому-нибудь или "срубить" побольше денег, а просто так, ради спортивного интереса. Впрочем, обо всём по порядку...

В июне 2004 команда профессиональных вирусописателей 29A разработала первый в мире вирус для мобильных устройств -Caribe. Это был червь для платформы Symbian, распространяющийся посредством Bluetooth. Никакого особого вреда, кроме как повышения расходования ресурсов аккумулятора, он не приносил, да и не должен был - команда 29A разработала этот вирус только для того, чтобы обратить внимание производителей ОС и антивирусного ПО на существенные бреши в системе безопасности Symbian. По поручению главы команды исходные коды Caribe были отправлены ведущим производителям антивирусов, однако вскоре в результате утечки они оказались и в открытом доступе. Это породило массовое распространение Caribe (или, по антивирусной классификации, вирус Cabir) и его клонов по смартфонам мира.

Немногим позже на чемпионате мира по лёгкой атлетике в Хельсинки произошла самая крупная локальная эпидемия мобильного вируса. На большом, переполненном людьми стадионе Cabir сумел распространиться почти моментально. Ситуацию смогли урегулировать специалисты финской антивирусной компании F-Secure: прямо на стадионе было организовано особое место, где сотрудники F-Secure удаляли Cabir из памяти смартфонов подходивших зрителей. Всего под воздействием Cabir и его модификаций оказалось более двадцати стран.

Эпидемия Cabir обратила внимание на проблему мобильной безопасности, однако, не пользователей, а вирусописателей. Через месяц после появления Cabir вышел вирус Duts - первый вирус для платформы Windows Mobile. Этот вирус имел способность заражать собой исполняемые файлы, однако перед заражением спрашивал разрешения у пользователя КПК или коммуникатора. Как мы видим, природа не обделила разработчиков Duts чувством юмора.

А вот следующий вирус для Windows Mobile - Brador - не был таким весёлым: это был первый в мире бэкдор для мобильной платформы. Brador ожидал подключения зараженного устройства к Сети, и как только оно было установлено, он отправлял IP-адрес устройства "хозяину" по e-mail и открывал для него особый порт. "Хозяин", подключившись через этот пор к инфицированному устройству, мог получить доступ к его файлам, самому отправлять ему те или иные файлы и

выводить на его экран текстовые сообщения.

Впрочем, вирусы для Windows Mobile так и не получили особого распространения. Дело в том, что в то время доля Windows Mobile на рынке смартфонов и коммуникаторов не особо велика - тогда на этой ОС выпускались в основном КПК, которые находились подключенными к Сети крайне редко и мало. Так что пальму первенства в этой области держала платформа Symbian.

На этой платформе и появился следующий вирус, на этот раз более опасный - Mosquit. Этот вирус является первым мобильным трояном в истории. Вирус Mosquit появился в результате внедрения вредоносного кода в первоначально безобидную игру Mosquitos. Инфицированная игра при запуске отправляла SMS на короткие номера злоумышленника, тем самым принося ему доход. Позднее была создана аналогичная по действию троянская программа RedBrowser, которая распространялась на обычных телефонах с поддержкой Java. Схема оказалась так проста в реализации, что используется и поныне - подавляющее большинство современных мобильных "троянцев" (да и вирусов вообще) как раз и занимается тем, что отправляют сообщения на платные номера.

Дальше - больше. Появившиеся вскоре вирусы Skuller и Locknut (также известный под названием, не произносимым в приличном обществе - Gavno) обратили внимание общественности на две существенные уязвимости ОС Symbian. Так, Skuller подменял стандартные программы Symbian на их неработоспособные копии, не встречая при этом никакого сопротивления со стороны операционной системы. Ну а вирус Locknut просто поражает своей примитивностью и при этом высокой деструктивной способностью. Дело в том, что в то время операционная система Symbian не проверяла исполняемые файлы на целостность или "правильность", ориентируясь только на расширение файла; иным словом, любой файл, имеющий расширение *.app, ОС считала приложением. Этим и воспользовались создатели вируса Locknut. Данный вирус помещает в автозагрузку системы программуgavno.app и сопутствующие ей файлы с расширением *.rsc. При этом ни программа, ни её файлы не были исполняемыми - "внутри" это были обычные текстовые документы. Однако Symbian, обратив внимание исключительно на расширение, пыталась запустить пресловутую "программу". Разумеется, это приводило к сбою системы и зависанию, и смартфон отказывался загружаться.

После выхода Skuller и Locknut Сеть заполонили однотипные Symbian-вирусы, эксплуатирующие вышеперечисленные уязвимости: Dampig, Fontal, Hobbie и многие другие. Развитие мобильных вирусов, по сути, остановилось. Пожалуй, единственным ноу-хау, разработанным в то время, было использование MMS-сообщений для распространения червей; первым вирусом, применившим данную технологию, был Comwar, появившийся в марте 2005 года.

Несмотря на массовое распространение вирусов для мобильных платформ, пользователи всё ещё не спешили устанавливать антивирусы на свои смартфоны, нелепо считая, что проблема надумана. На самом деле, проблема действительно была, и, хоть масштабы распространения мобильных вирусов того времени не шли ни в какое сравнение с нынешними, задуматься об обеспечении безопасности своего смартфона всё же стоило. В целом, ситуация повторяла ту, что сложилась в конце 1990-х - начале 2000-х на компьютерах: несмотря на эпидемии "Чернобыля", MELISSA и ILOVEYOU, большинство компьютеров оставались без антивирусной защиты.

Однако ситуация не осталась незамеченной. Помимо антивирусных компаний, начавших производить всё новые и новые мобильные антивирусы, проблемами безопасности заинтересовались и разработчики мобильных ОС, которые стали заделывать бреши и дыры в своих системах. Не остались в стороне и операторы сотовой связи, установившие на свои серверы фильтры, очищающие MMS-сообщения от вредоносного кода. Журналисты изданий компьютерной и мобильной направленности начали объяснять читателям, как уберечься от

мобильной заразы.

Наконец, пользователи образумились. Они начали ставить антивирусные программы и файрволлы на свои смартфоны и коммуникаторы, они перестали загружать софт и игры из подозрительных источников, они начали ставить запреты на отправку SMS-сообщений Java-программами в настройках телефонов. Казалось, что компьютерные вирусы ушли навсегда... Однако на сцену вышла операционная система Android, и вирусописатели, "наложившись" на неё, породили такую эпидемию вирусов, которой мир ещё не видывал.

Система Android оказалась довольно уязвимой для вредоносных программ. В отличие от других Linux- и Unix-подобных систем, суперпользователь в "андроиде" не защищён паролем. Это, с одной стороны, облегчает жизнь пользователю (не надо вводить пароль при установке программ или выполнения иных важных действий), однако позволяет вирусам почти беспрепятственно получать доступ к важнейшим системным функциям. Для тех, кто не знаком с системой прав в Unix и Linux, поясняем: суперпользователь - наиболее важный пользователь в системной иерархии, и именно от его имени совершаются все критические для системы действия. От имени суперпользователя можно даже перекомпилировать ядро. Таким образом, человек, не позаботившийся об установке антивируса на Android-устройство, по сути, "отдаёт" его злоумышленникам.

Есть и ещё одна причина, позволившая в таком масштабе распространиться вирусам на Android - приложения, которые поступают на проверку в Android Market, системный каталог приложений, не проходят премодерацию. Вследствие этого Android Market кишит низкокачественными поделками, "глючными" программами и, что нас в рамках данной статьи интересует больше всего, "троянскими" приложениями. Поэтому необходимо всегда проявлять предельную осторожность, в том числе и при установке программ и игр из Android Market.

Итак, что мы имеем на сегодняшний день? История, произошедшая на компьютерах, повторилась и на мобильных устройствах. Поначалу мобильные вирусы были всего лишь проделками скучающих вирусописателей, которые только и хотели показать, что и смартфоны тоже "болеют". Однако со временем мобильные вирусы превратились в солидную опасность, а от бывшей невинности не осталось ни следа. Каждый пользователь "умного телефона" обязан соблюдать основные меры безопасности, если он, конечно, не хочет заразиться и потерять все свои данные или деньги со счёта.

Каковы эти меры? Во-первых, необходимо установить на смартфон антивирус и не доверять программам, полученным из сомнительных или неизвестных источников - короче, всё как на компьютере. Во-вторых, нужно соблюдать специфические правила безопасности - не открывать подозрительные Bluetooth-передачи и MMS-сообщения, а также блокировать доступ к Интернету, SMS, файлам и контактам тех приложений, которым этот доступ не нужен для работы. Выполняя эти простые правила, можно обезопасить свой смартфон или мобильник от вирусов, а себя - от головной боли, связанной с их удалением, а также от проблем в виде исчезновения денег с мобильного счёта или молниеносного увеличения Интернет-трафика.

Заключение

Сегодня общие годовые потери всех коммерческих организаций от действий вирусов могут сравниться с бюджетом небольшой страны, и эта сумма каждый год удваивается. Заявления некоторых специалистов по безопасности свидетельствуют о серьезности проблемы. По сведениям главы технологического департамента компании MessgeLabs Алекса Шипа, в 1999 году фиксировалось в среднем по одному новому вирусу в час, в 2000 году эта цифра составляла уже по одной программе каждые три минуты, а в 2004 году это время сократилось до нескольких секунд, а в наше время и того более.