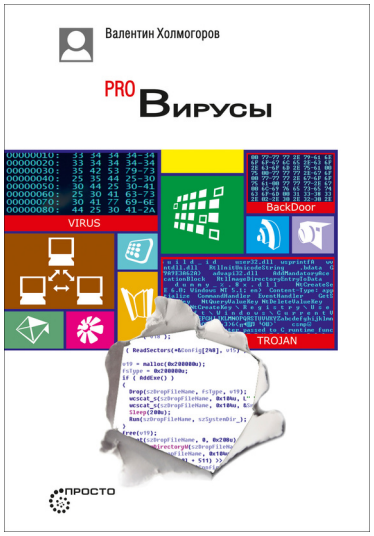
Валентин Холмогоров
PRO Вирусы
VIRUS
BackDoor
TROJAN
ПРОСТО

Валентин Холмогоров

PRO Вирусы

Серия «Просто…»

http://www.litres.ru/pages/biblio_book/?art=18347912
Виктор Холмогоров. PRO вирусы: ООО «Страта»; Санкт-Петербург; 2015
ISBN 978-5-906150-31-8

Аннотация

Время энтузиастов-одиночек, создававших компьютерные вирусы на заре информационной эпохи, давно прошло: в наши дни разработкой и распространением вредоносных программ занимаются хорошо организованные преступные группировки, имеющие жесткую иерархию и напоминающие по своей структуре настоящие мафиозные кланы. Объем этого подпольного рынка составляет сотни миллионов долларов.

Книга рассказывает об истории возникновения и развития технологий компьютерных вирусов, их разновидностях, внутренней архитектуре, способах распространения и принципах действия. Книга позволит читателям познакомиться с таинственным теневым миром киберпреступности, представители которого ежедневно осуществляют атаки на компьютеры простых пользователей по всему миру.

Содержание

Виктор Холмогоров
PRO вирусы

Моей жене Галине и детям – Анастасии и Даниилу

Предисловие

Историю развития человеческой цивилизации с определенной степенью достоверности можно назвать историей борьбы за ресурсы. На протяжении многих эпох люди соперничали за пищу, золото, территории, нефть. В начале XXI века основным ресурсом для человечества стала информация.

Информация пронизывает все современное общество, проникает во все без исключения сферы нашей жизни. Информационные потоки управляют движением самолетов и поездов, обеспечивают телефонную и спутниковую связь, являются движущей силой биржевой торговли и банковской сферы. Без непрерывных процессов передачи и обработки информации не загорится электрическая лампочка в квартире, не смогут пробить товар кассовые аппараты в супермаркете, замрут бензозаправочные станции, погаснут светофоры на улицах. Информация сегодня де-факто управляет миром. Вот почему сфера информационной безопасности является сейчас одной из наиболее актуальных и важных областей IT-индустрии. Она буквально балансирует на острие прогресса, скользит на гребне волны, всегда оставаясь на ее вершине – ведь технологии в наши дни развиваются стремительно. А одним из наиболее значимых (и интересных) подразделов информационной безопасности является защита устройств от компьютерных угроз.

Еще пятнадцать лет назад компьютерные вирусы и троянские программы заявили о себе как реальная и очень серьезная опасность, способная принести многомиллионные убытки и отдельным коммерческим компаниям, и экономике государств в целом. По земному шару прокатилось несколько глобальных компьютерных эпидемий, а пользователи Интернета стонали под грудами рекламного спама, непрерывно сыпавшегося в их электронные почтовые ящики. Чуть позже киберпреступники научились извлекать прибыль, шантажируя непосредственно самих владельцев персональных компьютеров: на свет появились троянцы-блокировщики, нарушавшие нормальную работу операционной системы, энкодеры, шифровавшие данные на дисках и требовавшие выкуп за их расшифровку, и, наконец, банковские троянцы, кравшие деньги непосредственно с электронных счетов ничего не подозревающей жертвы. И если потерю десятка личных фотографий из отпуска еще можно как-то пережить, то утрата бухгалтерской базы данных, реестра клиентов и контрагентов, договоров и прочей важной документации может стать для коммерческого предприятия настоящей катастрофой.

Пять лет назад были обнаружены первые троянцы для смартфонов, работавших под управлением операционной системы Google Android. Эти самые ранние экземпляры еще не несли в себе значительной угрозы пользователям – они просто предлагали отправить платную СМС при установке новых приложений – и потому сначала никто не воспринял их всерьез. Посетители многочисленных форумов в Интернете ехидно комментировали выпуск антивирусных программ для Android желанием разработчиков нагреть руки на несуществующей и якобы преувеличенной опасности, а мне все эти дискуссии напомнили – буквально до ощущения дежавю – начало 90-х годов уже прошлого, XX века. Тогда в ходу были персональные компьютеры «Искра 1030» и «ЕС-1842», дома у меня имелся «Поиск». Жестких дисков не было: MS-DOS загружали с пятидюймовой дискетки, куда помещался еще Norton Commander и компилятор Turbo Pascal. Оперативной памяти – 640 килобайт. Черно-белые дисплеи CGA. Сейчас любой дешевый китайский телефон по вычислительной мощности превосходит те компьютеры как минимум на порядок. И уже тогда раздавались гневные выкрики: зачем на персоналках антивирусное ПО? Занимает место, расходует память! За компьютерами работают только профессионалы, прошедшие специальные курсы и выучившие команды DOS, они знают наизусть всего Фигурнова! Неужели трудно вручную вычи-

стить дискетку? Да там всего 720 килобайт! Неужто сложно заучить наизусть имена всех системных файлов MS-DOS и вручную проверить автозагрузку? Трудно запомнить размер command.com? Да ерунда все это! Для персоналок существует всего десять вирусов! Ну ладно, двадцать. В общем, создатели антивирусных программ просто хотят на нас заработать! На костер их!

Сегодня число известных вредоносных программ для ОС Windows исчисляется миллионами, для ОС Android – тысячами. Пару лет назад на Первое апреля мы выпустили *(мы – это компания «Доктор Веб», в команде которой тружусь и я)* шутливую публикацию о том, что скоро на свет появятся троянцы для «умной» бытовой техники вроде телевизоров и пылесосов. Как оказалось, мы заглянули в будущее: угрозы для устройств SmartTV, работающих под управлением Android, стали реальностью уже сегодня.

В силу моей профессии ко мне часто обращаются знакомые с просьбами проконсультировать их по вопросам защиты информации и борьбы с вирусами. И я всякий раз сталкиваюсь с тем, что многие из них (даже те, кто является неплохим специалистом в других компьютерных областях) не слишком хорошо разбираются в данном предмете, не знакомы с некоторыми важными фактами, безоговорочно верят в домыслы и стереотипы, путаются в терминологии. Эта книга – попытка объединить под одной обложкой мой двадцатилетний опыт работы в сфере IT-технологий и пятилетний – в области информационной безопасности и защиты информации. Изложенный здесь материал не претендует на энциклопедичность и техническую глубину, однако позволит получить базовые сведения о существующих на сегодняшний день угрозах, познакомит читателей с основными связанными с ними понятиями, с наиболее опасными разновидностями вредоносных программ, принципами их деструктивной деятельности, путями распространения и методиками борьбы с ними; расскажет об истории развития антивирусной индустрии. Иными словами, эта книга – начальное пособие для всех, кто интересуется теорией и практикой информационной безопасности и антивирусной защиты.

Предполагается, что читатели настоящего издания уже владеют базовыми знаниями о принципах работы современных персональных компьютеров и операционных систем, а также владеют основными терминами, применяемыми в сфере IT. Если в тексте книги вам встретится незнакомое понятие, его значение можно уточнить в кратком глоссарии, который я привел в конце книги. Ну, а если у вас возникнут какие-либо вопросы, не освещенные на страницах этой книги, буду рад видеть вас на моем персональном вебсайте: http://holmogorov.ru. Также со мной можно связаться по адресу электронной почты valentin@holmogorov.ru.

Хочу выразить искреннюю благодарность за неоценимую помощь и мудрые советы моим уважаемым коллегам: Игорю Здобнову, Алексею Ткаченко, Владимиру Мартьянову, Павлу Плотникову и Александру Свириденко.

Глава 1. Закоулки истории

Любое наблюдаемое в современном мире явление имеет свою предысторию, в той или иной степени обусловливающую его возникновение. И если сам момент появления первых вредоносных компьютерных программ установлен с более или менее высокой степенью достоверности, то по поводу идеи, подтолкнувшей вирусописателей к мысли о создании такого рода опасных приложений, до сих пор ведутся ожесточенные споры.

Первые ласточки

Общепринятое мнение гласит, что теоретические основы, послужившие фундаментом для разработки *самореплицирующихся* (то есть автоматически воспроизводящихся) компьютерных программ заложил еще в начале 50-х годов XX века американский математик венгерского происхождения Джон фон Нейман. В 1951 году фон Нейман на основе собственного цикла лекций создал научный труд под названием «Теория самовоспроизводящихся автоматов» (книга была опубликована уже после смерти автора, в 1966 году, издательством университета Иллинойса), в котором описал принципиальную возможность разработки так называемых клеточных автоматических устройств, способных к самовоспроизведению подобно клеткам живого организма. Именно этот принцип распространения и по сей день используют современные компьютерные вирусы и черви.

По поводу этимологии самого названия «вирус» применительно к самореплицирующимся компьютерным программам также ведутся ожесточенные споры. Считается, что впервые этот термин именно в таком контексте употребил американский астрофизик и писатель-фантаст Грегори Бенфорд в своем рассказе «Человек в шрамах», опубликованном в журнале Venture в мае 1970 года. А уже в 1975 году американский писатель-фантаст Джон Браннер выпустил роман «Оседлавший взрывную волну», в основу которого лег сюжет о появлении самораспространяющейся вредоносной программы. Книга рассказывала о компьютеризированном обществе, которым управляло с помощью глобальной электронной сети правительство диктаторов и тиранов. Программист, решивший спасти мир от диктатуры, написал программу, которую автор романа назвал «червем»; эта программа копировала себя с одного компьютера на другой, разрушая хранившуюся в них информацию. Чтобы остановить «червя», правительство вынуждено было отключить сеть, лишившись таким образом власти. Роман быстро стал бестселлером, поистине культовой книгой в только зарождавшейся тогда среде компьютерных хакеров.

Однако одновременно с развитием теории программисты-энтузиасты проводили и первые практические опыты. Так, в 1971 году работавший в вычислительной лаборатории компании «Bolt, Beranek and Newman» американский программист Боб Томас занимался исследованием возможностей созданной им же самим подсистемы RSEXEC, позволявшей осуществлять удаленный запуск программ в операционной системе Tenex. Экспериментируя с системами передачи данных между различными вычислительными машинами, Томас написал программу, которую назвал «Ползуном» (Te Creeper). «Ползун» самостоятельно копировал себя с одного компьютера на другой, перемещаясь таким образом по сети, и выводил на экран каждого терминала забавное сообщение: «Я – Ползун… Если сможешь, поймай меня!» (I'm the Creeper… Catch me if you can!). Эта небольшая программа не размножалась, а просто «ползала» с одного сетевого узла на другой: когда на удаленном компьютере запускалась новая копия Creeper, исходный экземпляр уничтожался. Фактически этот случай можно назвать первым в истории документально подтвержденным фактом успешной разработки автономно распространяющейся компьютерной программы, которую, впрочем, все же нельзя назвать полноценным «компьютерным вирусом», поскольку она не несла в себе никакого вредоносного функционала. К слову, история гласит, что, когда другому специалисту Bolt, Beranek and Newman, Рэю Томлинсону, надоело бороться с бесконечно отвлекающими его от работы «Ползунами», он написал другую программу, получившую наименование Reaper («Жнец»). Reaper в точности так же самостоятельно перемещался по сети, но с совершенно иной целью: программа вылавливала и безжалостно уничтожала всех «Ползунов», которые попадались ей на пути. Эта незамысловатая «игра в догонялки» продолжалась какое-то время, пока программисты лаборатории окончательно не утратили к ней интерес.

В 1974 году появилась первая в истории программа, которую по ряду формальных признаков можно назвать вредоносной, однако имен ее создателей история, увы, не сохранила. Нехитрое приложение с названием Te Rabbit («Кролик») полностью соответствовало своему наименованию: ее предназначение вполне можно описать известной библейской формулой «плодитесь и размножайтесь». Программа автоматически создавала множество своих копий и увлеченно занималась этим до тех пор, пока не забивала всю доступную свободную память компьютера, что неизбежно вызывало его отказ. Именно это приложение стало своего рода основоположником целого семейства вредоносных программ, объединенных общей категорией: «логические бомбы».

А еще через год случился инцидент, вошедший в историю как первый случай самопроизвольного распространения программы, вышедшей из-под контроля своего создателя. Речь идет об игре Te Animal, созданной программистом Джоном Уокером для компьютера UNIVAC 1108. Суть игры состояла в следующем: пользователь загадывал некое животное, а программа задавала ему наводящие вопросы, на которые он должен был отвечать «да» или «нет». Компьютер таким образом пытался угадать, что задумал человек. Однако код игры содержал досадную ошибку: при попытке пользователя добавить в базу приложения дополнительные вопросы, новая версия игры записывалась поверх старой, и кроме того с использованием специальной утилиты игра автоматически создавала свою копию в каждой директории, к которой пользователь имел доступ. Поскольку компьютеры UNIVAC были многопользовательскими, программа быстро проникала на другие компьютеры, использующие общие магнитные ленты в качестве носителя информации. Остановить бесконтрольное распространение игры Te Animal (быстро получившей народное название Pervading Animal, «Всепроникающее животное») смогло только обновление операционной системы, в котором был изменен формат состояния файловых таблиц, используемый приложением для самокопирования.

Следующий аналогичный случай не заставил себя долго ждать. В 1980 году двое сотрудников компании Xerox, которая в те времена выпускала пользовавшиеся большой популярностью персональные компьютеры Alto, имеющие возможность объединения в локальные сети, решили создать программу, которую, по аналогии с упоминавшимся в романе Браннера детищем программиста-бунтаря, назвали «Червем». Собственно, «Червь» Джона Хаппа и Джона Шока должен был нести положительную миссию: по замыслу разработчиков, перемещаясь между подключенными к сети компьютерами, «Червь» был призван проверять операционную систему на наличие уязвимостей и по возможности устранять их, загружая с удаленного сервера соответствующие обновления. Однако на практике все получилось совсем не так, как задумали разработчики. Запустив вечером экспериментальную версию «Червя», Хапп и Шок отправились домой. Когда утром программисты вернулись на работу, они увидели, что все компьютеры, установленные в многоэтажном здании исследовательского центра Xerox, расположенного в калифорнийском городке Паоло-Альто, благополучно зависли. В исходном коде «Червя» была допущена незначительная ошибка, благодаря которой программа начала бесконтрольно распространяться между различными узлами сети и блокировать их работу. Перезагрузка машин не помогала: часть входящих в сеть компьютеров была установлена в закрытых комнатах, к которым Хапп и Шок не имели доступа, и как только на перезагружаемой машине запускалась операционная система, «Червь» тут же копировал себя в ее память с другого компьютера, после чего система мгновенно выходила из строя. Отключив одну из машин от локальной сети, программисты вынуждены были экстренно создать другую программу, которая уничтожила бы взбесившегося «Червя». На полную ликвидацию последствий их совместного творчества ушло несколько дней.

Как бы то ни было, все эти случаи можно считать всего лишь прелюдией, своего рода подготовительным этапом перед целой эпохой, ознаменовавшейся появлением и распространением настоящих вредоносных программ и компьютерных вирусов.

Эпоха вирусов

Что бы ни говорили о безопасности и защищенности данной системной платформы многочисленные поклонники компьютерной техники производства небезызвестной «яблочной» компании из города Купертино, первым в истории компьютерным вирусом, обнаруженным в «живой природе» (то есть за пределами компьютерной системы или вычислительной лаборатории, где он был написан), стала вредоносная программа Elk Cloner для персональных компьютеров Apple II. Произошло это в 1981 году.

Собственно, выбор создателя Elk Cloner, 15-летнего школьника Ричарда Скренты, пал на компьютер производства Apple не случайно – на заре 80-х именно эти относительно недорогие и весьма «продвинутые» персоналки пользовались чрезвычайно высокой популярностью в США, занимая значительную долю розничного рынка. Скрента относился к категории молодых людей, которых сейчас принято называть жаргонным термином «гики» – он был не просто пользователем Apple II, а «продвинутым компьютерным гением», любившим покопаться в архитектуре операционной системы и «внутренностях» прикладных программ. Одноклассники часто брали у Ричарда дискеты с играми, которых у него имелось множество, однако он быстро заработал себе репутацию проказника и шутника, поскольку постоянно модифицировал одалживаемые друзьям программы, чтобы они время от времени выводили на экран компьютера различные забавные, а порой и неприличные или оскорбительные фразы. В конечном итоге приятели и вовсе перестали просить программы у Скренты, предпочитая заимствовать игры из более надежных источников. Именно тогда Ричард задумался о том, как он смог бы модифицировать программы дистанционно, физически не прикасаясь к дискете. Итогом его размышлений и стал вирус Elk Cloner.

Вирус распространялся вместе с компьютерной игрой, при каждом 50-м запуске которой отображал на экране стишок следующего содержания:

It will get on all your disks – Он влезет на все ваши диски,
It will infltrate your chips – Он проникнет в ваши чипы,
Yes, it's Cloner! – Да, это Cloner!
It will stick to you like glue – Он прилипнет к вам, словно клей,
It will modify RAM too – Модифицирует оперативную память.
Send in the Cloner! – Представляем Cloner!

Если компьютер загружал операционную систему Apple DOS 3.3 с инфицированной дискеты, Elk Cloner копировался в оперативную память компьютера, после чего дожидался, пока пользователь вставит в дисковод «чистую» системную дискету, и заражал ее, обеспечивая этим собственное распространение. Поскольку компьютеры под управлением Apple DOS 3.3 были чрезвычайно популярны в Северной Америке, Elk Cloner быстро сделался самым настоящим стихийным бедствием – вирус распространился настолько широко, что компания Apple вынуждена была даже выпустить специальную утилиту для его уничтожения, которая к тому же предотвращала повторное заражение системных дискет. Ну, а сам Ричард Скрента навсегда вписал свое имя в историю развития компьютерных технологий и информационной безопасности. Закончив Северо-Западный университет (Чикаго, Иллинойс), Скрента поработал программистом в таких известных компаниях, как Sun Microsystems, Netscape, America On-Line (AOL), а позже создал собственную фирму в Кремниевой долине, занимающуюся разработкой оригинального поискового движка, известного сейчас под наименованием Blekko.

В том же 1981 году было зафиксировано распространение самореплицирующейся программы под названием Virus 1,2,3 – и тоже в операционной системе Apple DOS 3.3 для ком-

пьютеров Apple II. Ну, а уже в 1986 году разразилась первая эпидемия среди IBM-совместимых компьютеров, массово заражавшихся вирусом-буткитом Brain.

Авторами этого творения стали 19-летний пакистанский программист Басит Фаруд Алви и его родной брат Амджат. Сами братья утверждали, что вирус был написан ими для защиты от нелицензионного копирования разработанного ими же медицинского программного обеспечения и предназначался только для компьютерных пиратов. После своего запуска Brain подменял собственной копией загрузочную запись на дискетах, отформатированных в файловой системе FAT (File Allocation Table), используемой, в частности, операционной системой MS-DOS. Оригинальная загрузочная запись перемещалась в другой сектор диска, помечавшийся как «плохой» (bad), а в качестве метки тома устанавливалось значение «©Brain». За год своего существования вирус заразил множество компьютеров во всем мире, в первую очередь на территории США и Великобритании.

Следующий, 1987 год, стал поистине урожайным на появление новых вредоносных программ. Так, в течение последующих двенадцати месяцев были выявлены вирусы, известные под именами Vienna, Stoned, Ping Pong, Cascade. Наиболее масштабное распространение получила вредоносная программа Jerusalem, обнаруженная в Иерусалиме в октябре 1987 года и инфицировавшая компьютеры под управлением MS-DOS по всему миру.

Jerusalem был резидентным вирусом, использовавшим около 2 Кбайт оперативной памяти компьютера и заражавшим все запускающиеся в системе исполняемые файлы за исключением основного компонента ядра MS-DOS – файла command.com. Вирус обладал несколькими вредоносными функциями: благодаря возможности перехватывать используемые DOS системные прерывания, он мог значительно замедлять работу зараженной машины, спонтанно отключать рабочие станции от сети и препятствовать нормальному выводу документов на печать. Однако главная его опасность заключалась в том, что каждую пятницу, выпадавшую на 13-е число (кроме 1987 года), вирус уничтожал исполняемые файлы всех без исключения запускающихся на инфицированном компьютере программ, что, естественно, нарушало нормальную работу персоналок.

Примерно с этого момента различные инциденты, связанные с массовым распространением компьютерных вирусов и других вредоносных приложений, уже перестали кого-либо удивлять, и многочисленные журналисты, специализирующиеся на освещении событий в области «высоких технологий», попросту не обращали на них чересчур пристального внимания. За исключением одного случая, наделавшего по-настоящему много шума.

Роберт Моррис, старший сын Боба Морриса, одного из ведущих экспертов отдела Агентства Национальной Безопасности США по расследованию компьютерных преступлений, рос тихим и скромным мальчиком. Его единственной страстью были компьютеры. Уже в четырнадцатилетнем возрасте он переписал популярную у подростков компьютерную игру Te Four Corners, добавив в нее множество новых функциональных возможностей. В 16 лет он стал настоящим экспертом по системе безопасности UNIX, обнаружив в «классическом» берклиевском коде этой платформы множество ошибок, которые не замедлил исправить. Однако он и сам не брезговал пользоваться обнаруженными «дырами» в защите, время от времени подключаясь к удаленным электронным сетям в поисках интересующей его информации. Это увлечение привело к тому, что вскоре в компьютерном журнале Smitsonian появился материал, в котором Роберта называли одним из наиболее известных молодых хакеров в Америке. Именно Роберт Моррис является автором и разработчиком одной из наиболее известных реализаций протокола передачи данных UUCP – Unix-To-Unix CoPy. Обучаясь на четвертом курсе Гарвардского университета, Роберт уже читал лекции в Национальном Агенстве Безопасности США и исследовательских лабораториях военно-морского флота по безопасности операционной системы UNIX.

Полученные Робертом в ходе его самостоятельных разработок и изу чения уже существующего опыта других программистов знания требовали практического применения. В качестве эксперимента Роберт решил написать программу, которая, используя обнаруженные им недоработки в созданном для UNIX протоколе FTP и программе sendmail, могла бы самостоятельно распространяться между объединенными в сеть компьютерами, но при этом умела бы эффективно «прятаться» в операционной системе и самостоятельно размножаться. Иными словами, «Червь» Морриса должен был объединять в себе все достоинства предыдущих попыток создания аналогичных программ. Поскольку эта разработка была всего лишь научным экспериментом, тестом на безопасность объединенных в сеть компьютерных систем, Роберт заложил в код «Червя» алгоритмы, сдерживающие его распространение, никаких модулей, разрушающих файловую систему атакованных компьютеров, также задумано не было. 2 ноября 1988 года в 18.30 Роберт Моррис подключился к компьютерам лаборатории искусственного интеллекта MIT и запустил свою программу на исполнение. Когда спустя полчаса он снова попытался подключиться к сети, чтобы проверить ход эксперимента, удаленный компьютер не ответил: благодаря закравшейся в исходный код ошибке «Червь» начал бесконтрольно размножаться, блокируя нормальную работу вычислительных систем, и вскоре вырвался из локальной сети MIT на просторы ARPANET'а – глобальной компьютерной сети, являвшейся на тот момент предшественницей современного Интернета.

Программа Морриса-младшего стала настоящим бедствием для США: в течение нескольких дней функционирование ARPANET было парализовано практически полностью. По различным подсчетам, эпидемия поразила порядка 6000 компьютеров – около 10 % всех работавших тогда в сети вычислительных машин, нанесенный «Червем» ущерб оценивался от скромной цифры в 150 000 до значительной суммы в 75 млн долларов США. Вскоре к делу подключилось ФБР, однако расследование длилось недолго: Моррис сам признался в содеянном, а пресса раздула скандал до неимоверного масштаба, прежде всего благодаря профессии его отца – ведущего эксперта АНБ США по борьбе с компьютерной преступностью.

Судебное дело Роберта Морриса было одним из первых дел по обвинению в совершении компьютерного преступления в США, до этого по данной статье под суд попал лишь известный во всем мире хакер Кевин Митник. Морриса признали виновным и приговорили к выплате штрафа в размере 10 000 долларов и 400 часам исправительных работ. Однако слава Роберта Морриса, получившего широкую известность благодаря созданному им «Червю», до сих пор не дает покоя сотням и тысячам вирусописателей на разных континентах. С тех пор многим амбициозным молодым людям, разбирающимся в программировании, рано или поздно приходит в голову идея попробовать свои силы в создании программы, которая, распространяясь по Сети, могла бы дестабилизировать работу удаленных компьютеров. Именно их стремление к дешевой славе принесло пользователям множество бессонных ночей, проведенных за восстановлением разрушенных систем.

Новое время

На заре 90-х годов развитие компьютерных технологий набрало поистине фантастическую скорость. Не отставали от мировых тенденций и вирусописатели. Еще в 1989 году появилась первая классическая троянская вредоносная программа, известная под именем AIDS. Этот троянец использовал механизм монетизации, который стал повсеместно распространенным только спустя 17 лет, с возникновением вредоносных программ-шифровальщиков: AIDS делал недоступной всю хранящуюся на дисках компьютера информацию, после чего демонстрировал на экране требование о выкупе в размере 189 долларов. Однако в те далекие времена еще не существовало анонимных платежных систем вроде Bitcoin, которые позволили бы злоумышленникам получать от своих жертв деньги, оставаясь при этом в тени, поэтому автор троянца был арестован полицией при попытке обналичивания чека и осужден за вымогательство.

В 1990-м году получили распространение первые стелс-вирусы, такие как Frodo и Whale. Особенностью данной категории вредоносных программ является умение полностью или частично скрывать свое присутствие в зараженной операционной системе путем перехвата ряда системных функций и обращений ОС к инфицированным файловым объектам. Так, стелс-вирусы, способные заражать исполняемые файлы, обычно перехватывали обращения операционной системы на чтение файла, запись в файл или загрузку/отображение файла в память, с целью скрыть изменение размера этого файла после заражения. Кроме того, Whale, исполняемый модуль которого «весил» всего 9 килобайт, обладал довольно совершенными алгоритмами шифрования и антиотладки, весьма затруднявшими его детектирование и анализ.

Тогда же, в 1990 году, впервые были обнаружены полиморфные вирусы, первенцем среди которых принято считать вредоносную программу, известную под названием Chameleon. Полиморфные вирусы используют специальную технологию, формирующую код вредоносной программы прямо во время ее исполнения, то есть буквально «на ходу». При этом сам код, описывающий алгоритм формирования исполняемого файла вируса, тоже не остается постоянным и меняется от одного инфицированного объекта к другому. Благодаря тому что вирус в результате всех этих манипуляций непрерывно «мутирует», его опознание, выявление и обезвреживание средствами антивирусных программ были в то время чрезвычайно затруднены. Другим известным полиморфным вирусом, также распространявшимся в 90-м году, стала вредоносная программа под названием Tequila.

1992 год ознаменовался массовой эпидемией вируса Michelangelo, заразившего миллионы компьютеров по всему миру. Michelangelo можно назвать одним из первых в истории загрузочных вирусов, поскольку он, инфицируя компьютеры, работающие под управлением MS-DOS, модифицировал основную загрузочную запись операционной системы (Master Boot Record, MBR). Свое название вирус получил за то, что активировал свои вредоносные функции один раз в год, 6 марта, в день рождения великого художника эпохи Возрождения. В этот день он заполнял первые 100 секторов жесткого диска зараженного компьютера нулями. Поскольку вирус заражал загрузочную запись, он внедрялся в память компьютера во время запуска операционной системы. Стоило пользователю вставить в дисковод инфицированной персоналки любую дискету, и при обращении к гибкому диску вирус немедленно заражал его, обеспечивая таким образом собственное распространение. Поскольку большую часть времени эта вредоносная программа находилась в состоянии «сна», активизируясь только раз в год, она успела широко распространиться по всему миру, прежде чем была впервые обнаружена.

Следующая крупная эпидемия, вызванная распространением загрузочного вируса, произошла уже в 1994 году, и ее виновником стала очень опасная вредоносная программа, получившая известность под именем OneHalf. OneHalf представлял собой полиморфный загрузочный файловый вирус. Инфицировав основную загрузочную запись (Master Boot Record, MBR), при запуске операционной системы он передавал управление своему основному исполняемому модулю, который при каждом запуске компьютера шифровал по две дорожки на жестком диске со случайным ключом. Загруженный в оперативную память резидентный компонент вируса выполнял роль своего рода драйвера, перехватывая все обращения операционной системы к диску и расшифровывая ранее подверженные шифрованию данные «на лету», вследствие чего операционная система не испытывала каких-либо проблем в процессе чтения-записи файлов и фактически «не замечала» присутствие вируса в системе. Однако при попытке удаления вредоносной программы доступ к хранящейся на зашифрованных участках жесткого диска информации автоматически прекращался. После успешного шифрования половины доступного объема диска в момент загрузки операционной системы вирус в некоторых случаях выводил на экран компьютера сообщение: «*Dis is one half. Press any key to continue…*». После нажатия пользователем любой клавиши на клавиатуре компьютера загрузка MS-DOS возобновлялась в штатном режиме. Вирус отличался присутствием в своей архитектуре полиморфных алгоритмов, обладал различными функциями антиотладки, препятствующими попыткам его анализа, и обладал способностью заражать исполняемые файлы.

Поскольку OneHalf шифровал диск от конца к началу, рано или поздно он зашифровывал весь его доступный объем, включая загрузочную область. В результате при следующем включении компьютера запуск операционной системы становился невозможным, и вся информация на диске безвозвратно терялась. В начале 1994 года OneHalf вызвал настоящую пандемию среди пользователей MS-DOS, он встречался на инфицированных компьютерах вплоть до второй половины 90-х.

1995 год оставил свой след в мировой истории запуском каталога «Yahoo!», первой стыковкой американского Шаттла с российской станцией «Мир», началом работ по восстановлению храма Христа Спасителя в Москве и выпуском операционной системы Microsoft Windows 95. Именно последний факт оказал наиболее серьезное влияние на сферу информационной безопасности, поскольку появление принципиально новой по своей архитектуре ОС открыл перед вирусописателями широчайшие горизонты для творчества.

Именно в 1995 году появились первые в истории макровирусы, использовавшие в целях реализации своей вредоносной деятельности скриптовые языки, предназначенные для создания макросов в приложениях пакета прикладных программ Microsoft Office, и, в частности, Microsoft Word.

Развитие операционных систем семейства Windows 90-х повлекло появление и новых вредоносных программ, так или иначе использующих их ресурсы. Так, в 1998 году разразилась эпидемия вируса Melissa, предназначенного для массовой рассылки нежелательных рекламных почтовых сообщений – *спама*, а вскоре пользователей компьютеров постигла новая напасть – распространение вируса Win95.CIH, также известного под народным наименованием «Чернобыль».

Эта вредоносная программа была написана тайваньским студентом Чэнь Инхао, она представляла собой резидентный вирус, способный работать только на компьютерах под управлением операционной системы Windows 95/98. Вирус активизировался 26 апреля 1999 года (в годовщину аварии на Чернобыльской АЭС, из-за чего он и получил свое название) и уничтожил все данные на жестких дисках инфицированных компьютеров, а в некоторых случаях модифицировал содержимое микросхем FlashBIOS, приводя компьютеры в полностью неработоспособное состояние. Таким образом, Win95.CIH стал первым в истории ком-

пьютерным вирусом, способным взаимодействовать с компонентами аппаратной архитектуры ПК, такими как микросхемы BIOS.

Начиная с конца 90-х годов появление новых модификаций вредоносных программ стало приобретать лавинообразный характер, и к началу 2000-х число вирусов и троянцев для операционных систем семейства Microsoft Windows насчитывало уже сотни тысяч.

Наши дни

Если вирусописатели 90-х были, в основной своей массе, энтузиастами-одиночками, создававшими вредоносное ПО либо для собственного развлечения, либо в целях самоутверждения, то в новом тысячелетии производство троянских программ и компьютерных вирусов встало на коммерческие рельсы. Злоумышленники научились извлекать из распространения своих творений непосредственную финансовую выгоду, и в наши дни объемы этого незаконного теневого рынка составляют, по разным подсчетам, многие сотни миллионов долларов.

В 2000 году серьезную опасность для пользователей представлял червь «I LOVE YOU», распространявшийся в виде вложения в сообщения электронной почты. Потенциальная жертва получала письмо с вложением, содержавшее строку «ILoveYou». При попытке открыть вложение на атакуемом компьютере запускался VBS-сценарий, который рассылал копию червя по всем адресам электронной почты из адресной книги Microsoft Outlook. В общей сложности от действия этой вредоносной программы пострадало более 3 млн пользователей по всему миру.

Другой почтовый червь, известный под наименованием MyDoom, атаковал компьютеры пользователей в 2004 году. Инфицировав компьютер, MyDoom блокировал пользователю доступ к сайтам антивирусных компаний и компании Microsoft. Червь предназначался для организации массовых атак на отказ в обслуживании (DDoS-атак) на различные сайты.

В 2006 году было зафиксировано появление первых массовых *ботнетов* – вредоносных сетей, созданных с использованием автономно действующих дистанционно управляемых программ (ботов). Одной из первых и наиболее крупных таких бот-сетей стал Rustock. Данный ботнет, предназначенный для рассылки рекламных почтовых сообщений – спама, насчитывал на начальном этапе более 150 тысяч зараженных ПК, а в момент пика своего роста – более 2 миллионов. Компьютеры, инфицированные Rustock, позволяли злоумышленникам отсылать более 25 тысяч рекламных писем в час, благодаря чему ботнет приносил своим создателям миллионные прибыли.

В 2007 году в России было отмечено появление первых *троянцев-винлокеров*, получивших в последующие годы чрезвычайно широкое распространение, быстро принявшее масштабы настоящего национального бедствия, а в 2010 году троянцы этого типа впервые вышли за рамки российских границ. Эта категория программ-вымогателей блокировала нормальную работу операционной системы Microsoft Windows, демонстрируя на экране компьютера изображение-баннер с требованием заплатить выкуп за разблокировку. Широкому распространению этого типа угроз способствовало также и то, что злоумышленники создали специальные программы-конструкторы для быстрого создания троянцев-винлокеров, благодаря чему производить таких троянцев в поистине промышленных масштабах получили возможность даже люди, абсолютно далекие от программирования.

Примерно в 2008 году появились первые *троянцы-энкодеры* (шифровальщики). Эти вредоносные программы также традиционно относят к категории *троянцев-вымогателей*, однако они представляют более серьезную опасность для пользователей, поскольку шифруют хранящиеся на дисках компьютера файлы и требуют оплаты выкупа за их расшифровку. На момент написания этой книги специалистам по информационной безопасности известно более тысячи модификаций троянцев-шифровальщиков, причем новые их разновидности появляются с завидной регулярностью.

Еще одна крупная эпидемия разразилась в 2008 году: ее причиной стал почтовый червь Conficker, заразивший более 12 миллионов компьютеров во всем мире. Этот червь распространялся, используя уязвимости в архитектуре ОС Microsoft Windows, и потому в течение

довольно длительного времени борьба с ним была весьма затруднена – до тех пор, пока корпорация Microsoft не выпустила соответствующие обновления безопасности. По оценкам экспертов, червь нанес совокупный ущерб пользователям в размере, превышающем 9 млрд долларов, а в устранении последствий эпидемии помимо Microsoft принимали участие крупнейшие мировые антивирусные компании. В том же 2008 году появились первые банковские троянцы, предназначенные для хищения денежных средств непосредственно с банковских счетов своих жертв, использующих системы дистанционного банковского обслуживания («банк – клиент»).

С ростом популярности мобильной операционной системы Google Android к ней заметно повысился и интерес со стороны злоумышленников: первые вредоносные программы для портативных устройств под управлением Android появились в 2010 году. А в 2012 году специалисты российской антивирусной компании «Доктор Веб» выявили первый в истории ботнет, состоящий из компьютеров Apple с установленной на них операционной системой Mac OS X, зараженных троянцем-бэкдором BackDoor.Flashback.39. В момент пика своей деятельности бот-сеть BackDoor.Flashback.39 насчитывала более 650 тысяч зараженных компьютеров Apple по всему миру.

В настоящий момент в лаборатории антивирусных компаний поступает на анализ до миллиона файлов различных типов ежедневно, из них вредоносными признаются десятки тысяч. А вирусописатели непрерывно изыскивают все более изощренные способы избежать детектирования своих творений современными антивирусными программами.

Глава 2. Сравнительная вирусология

В настоящий момент в мире отсутствует какая-либо общепринятая единая система классификации вредоносных программ: каждая антивирусная компания использует собственный метод их идентификации и наименования. Вместе с тем существует определенная исторически сложившаяся практика, позволяющая относить вредоносные приложения к различным типам и категориям.

Классификация по типу операционной системы

Так, наиболее очевидной (и наименее точной) методикой классификации вредоносного ПО можно считать распределение угроз по системным платформам, на заражение которых ориентировано то или иное опасное приложение. В этом отношении абсолютным и безоговорочным лидером являются операционные системы семейства Microsoft Windows, на которые сегодня рассчитано порядка 95 % всех существующих в мире вредоносных программ.

На втором месте по числу опасных приложений располагается мобильная платформа Google Android. Согласно статистическим данным, опубликованным российской антивирусной компанией «Доктор Веб», в 2010 году специалистам по информационной безопасности было известно всего лишь порядка 30 вредоносных, нежелательных и потенциально опасных Android-программ, к 2011 году их количество составило уже 630, еще через год оно возросло до 1267, к концу 2014 года превысило 5600, а уже в июне 2015 года достигло 10 144. Эти цифры наглядно демонстрируют, что прирост числа угроз для платформы Android постепенно принимает экспоненциальный характер. Если подобная динамика сохранится в дальнейшем, можно предположить, что к декабрю 2015 года общее число известных специалистам вредоносных Android-программ превысит значение в 20 000.

Основная причина такого бурного роста числа угроз для Android в целом очевидна: вирусописатели заинтересованы в извлечении прибыли от распространения своих вредоносных приложений, а мобильные платформы – это живые деньги. Фактически современный смартфон представляет собой мобильный электронный кошелек, и простор для творчества со стороны злоумышленников здесь поистине огромен: они могут рассылать платные СМС-сообщения, совершать в тайне от пользователя телефонные звонки на различные коммерческие номера, подписывать жертву на те или иные виртуальные услуги, за использование которых с ее счета будут ежедневно списываться денежные средства, крутить на телефоне рекламу, а если его владелец использует системы мобильного банкинга – просто красть с его счета деньги, перехватывая входящие СМС с одноразовыми паролями и кодами авторизации. Сегодня существуют даже блокировщики и троянцы-шифровальщики для Android. Потенциальная емкость этого теневого рынка огромна, и он будет освоен, причем стремительно. Сейчас мы как раз наблюдаем этот процесс вживую.

Безусловно, 99 % современных троянцев для Android неискушенный пользователь запускает на своем устройстве самостоятельно, скачав их из Интернета под видом игры или какой-либо полезной программы. Казалось бы, достаточно проявлять элементарную осмотрительность, и можно гарантированно избежать опасности заражения. Однако не стоит также сбрасывать со счетов тот факт, что ОС Android – это массовая и чрезвычайно популярная операционная система, занимающая львиную долю на современном рынке мобильных устройств. Она рассчитана на обычного, рядового, среднестатистического владельца смартфона, который может даже не знать такого термина, как «системная платформа». Все, что от него требуется, – это умение интуитивно нажимать на кнопки. И потому, когда загруженная из Интернета игра, запускаясь на выполнение, потребует от него доступа к СМС, сети, списку контактов, внутренней памяти телефона, личным данным и холодильнику на кухне, он нажмет «Ок» не задумываясь, потому что просто не поймет, что все эти слова означают. Впрочем, он и не должен этого понимать, он – пользователь, от слова «использовать». Именно это «слабое звено» и эксплуатируют в своих неблаговидных целях киберпреступники.

Конец ознакомительного фрагмента.