КВ ВирусБюллетень

СТОП: ВИРУС!

Загрузочные (бутовые) вирусы (немного теории)

Глава пятая. ПРОЯВЛЕНИЯ ВИРУСОВ

Когда в популярных компьютерных изданиях разговор заходит о проявлениях компьютерных вирусов, пожалуй, именно эта особенность вирусов вызывает живейший интерес у читателей. Можно даже говорить о неком околовирусно-компьютерном фольклоре, истории из которого не раз публикуются и пересказываются устно.

Проявления загрузочных вирусов (впрочем, как и всех компьютерных) принято формально делить на АУДИОВИЗУАЛЬНЫЕ и ДЕСТРУКТИВНЫЕ. Естественно, они могут сочетаться, но это происходит нечасто. Здесь можно вспомнить гипотезу Обухова: «Чем изощреннее аудиоэффекты и(или) видеоэффекты компьютерного вируса, тем меньшая вероятность его деструктивных действий».

5.1. Условия срабатывания

Для того, чтобы скрыть присутствие вируса на компьютере и тем самым обеспечить увеличение продолжительности периода размножения, авторы вирусов «откладывают» на определенный срок момент проявления деструктивной компоненты или аудио/видеоэффектов. Здесь можно выделить лишь самые общие условия срабатывания:

– Подсчет числа перезагрузок с инфицированного жесткого диска. На усмотрение авторов вирусов, счетчик может вестись в прямом (увеличение значения) или обратном (уменьшение значения) направлении. Статистически «любимыми» значениями счетчика у вирусописателей являются числа 16, 32, 256, 512.

– Количество инфицированных дискет за один сеанс (от перезагрузки до перезагрузки) работы компьютера. Обычно это 16 дискет.

– Количество обращений к диску. Резидентный обработчик вируса подсчитывает количество вызовов дискового прерывания (например, 13h-го). Чем «активнее» при работе с диском ведет себя пользователь и его прикладные программы, тем больше у него шансов на себе испытать деструктивные действия вирусов.

– Анализ состояния системного таймера. Вариантов огромное количество – проверять значения либо часов, минут, секунд, либо каких-то логических операций (NOT, AND ...) со значением таймера.

– Анализ системной даты. Проверяется либо точная дата, либо «больше/меньше» определенного года, месяца, дня, дня недели.

Вышеперечисленные условия срабатывания ни в коем случае не претендуют на полноту описания, а должны рассматриваться лишь как список самых общих.

Для некоторых наиболее известных вирусов существуют красивые легенды, которые пытаются объяснить условия срабатывания. Например, вирус 'March6' (который носит еще неформальное название Mickaelangelo)' 6-го марта каждого года разрушает информацию на жестком диске, с которого был загружен. При упоминании этого вируса для объяснения выбранной автором вируса даты (6-е марта) используют 2 гипотезы:

– 6-го марта считается днем рождения Микеланджело;

– 6-го марта произошли события — битва в Хелмском ущелье и взятие Изенгарда, которые подробно описаны во 2-й книге трилогии лорда Дж.Р.Р.Толкиена «Властелин колец».

5.2. Деструктивные проявления

Первые загрузочные вирусы, «изготовленные» за рубежом, были большей частью безвредными. Происходила «обкатка» вирусных алгоритмов, наработка опыта. И только затем в свои вирусы авторы стали добавлять определенные «пакости», способные натолкнуть пользователей на мысль, что с их компьютером не все в порядке. Поначалу лишь некоторые содержали в себе деструктивные действия, и по миру поползли леденящие рассказы о компьютерных «людоедах», разрушающих и «съедающих» информацию. Справедливости ради надо сказать, что даже легендарный 'Disk Killer', «убивая» диски, хотился о возможности восстановления информации.

В общем случае, деструктивные действия загрузочных вирусов можно условно разделить на ВЗРЫВНЫЕ и РАСПРЕДЕЛЕННЫЕ. При взрывном характере действия вирус после наступления условия срабатывания сразу разрушает информацию, содержащуюся либо на всем диске, либо в основных системных областях (Master Boot Record, Boot Sector, File Allocation Table, Root Directory). Вирус, действие которого носит распределенный характер, вносит мелкие изменения в информацию, находящуюся на диске. Обнаружить (а тем более исправить) такие изменения в текстах или файлах баз данных представляется делом весьма трудоемким. По устоявшемуся заблуждению, рядовые пользователи считают вирусы с распределенными деструктивными действиями практически безобидными. А специалисты, занимающиеся вопросами антивирусной защиты, относят такие вирусы в группу «Очень опасные».

Наиболее часто встречаются следующие виды разрушения информации загрузочными вирусами:

— Форматирование носителя информации. Вирус форматирует либо диск целиком, либо основные системные области.

— Разрушение (затирание) информации на диске.

— Искажение записываемой информации. В буфере, содержащем прочитанные с диска данные, вирус по определенному алгоритму искажает либо меняет местами участки информации и записывает измененные данные на диск.

— Подмена дисковой операции. Обычно применяется к операции «Запись». Когда пользователь записывает на диск необходимую информацию, вирус некоторое количество операций «Запись» заменяет, например, на дисковую операцию «Чтение» или «Верификация». Таким образом, только часть необходимой информации будет «пятнами» записана на диск.

— Обнуление базовых адресов портов ввода-вывода. Приводит к неработоспособности (до следующей перезагрузки) устройств, присоединенных к портам с выбранными вирусом адресами. Обычно это принтерный порт и коммуникационные порты.

— Замена секторов либо дорожек местами. На инфицированных дискетах вирус меняет местами, например, нулевую и последнюю дорожки дискеты. На компьютере, жесткий диск которого инфицирован, активный резидентный вирус будет тщательно скрывать подмену, и информация с дискеты будет прочитана корректно. На других неинфицированных компьютерах дискета не будет читаться вовсе либо данные будут прочитаны неверно.

Те загрузочные вирусы, которые в себе содержат алгоритмы ЖЕСТОКОГО разрушения информации, обычно в литературе носят название вирусов-«вандалов».

5.3. Аудиовизуальные проявления

Оглядываясь на историю развития загрузочных вирусов, можно натолкнуться на одну закономерность: число вирусов, которые для своего проявления используют только звуковые и визуальные эффекты, неуклонно падает; зато число вирусов, содержащих алгоритмы разрушения информации пользователей, неуклонно растет.

А какими красочными были визуальные картинки в первых загрузочных вирусах! Весело прыгающий по экрану шарик вируса 'Ping-Pong', красочная картинка поздравления с днем рождения у вируса 'Happy Birthday Joshy' и пр.

Среди современных вирусов все реже и реже встречаются экземпляры с утонченными видеоэффектами. В описаниях появившихся вирусов все чаще упоминаются: вывод пугающих пользователя сообщений, сопровождаемый звуками; проигрывание очень известных и сочиненных собственными руками мелодий; вывод на принтер отдельных слов, предложений или фраз. Как правило, все это создается наспех, с большим количеством ошибок и далеко не всегда работает.

В следующем номере читайте: ИСТОРИЯ.

По ВСЕМ вопросам, связанным с антивирусной защитой и восстановлением поврежденной информации, Вы можете связаться с авторами программы:

Пейджинг: тел. 276-95-10, 222-14-54 для абонента 20587
FidoNet: 2:450/26.20@fidonet либо 2:450/26.21@fidonet
E-mail: gr@nsys.minsk.by либо vk@nsys.minsk.by

Подозрительные файлы и дампы загрузчиков Вы можете поместить на BBS 'Bercli' в область 'VIRUS' (тел. станции 223-31-54, время работы — круглосуточно).

Компьютерные слоВести

№1x1, IV год от основания "КВ"

ГАЗЕТЕНКА ДЛЯ НЕСПЕЦИАЛИСТОВ И БЕЗДЕЛЬНИКОВ

ЭКОЛОГИЯ ФИДО

Увидел я в какой-то эхе: «Приходил ко мне какой-то юзер, пофрякал...» И возник у меня по этому поводу ряд ассоциаций — как, к примеру, мог бы представить себе Фидо человек, не знающий, что это такое.

Фидошник — существо, внешне похожее на гибрид слона с поросенком. У него есть короткий и толстый хобот-фрякало (фрекало). Когда он приходит на BBS или на узел, находит там такую большую лужу густой жидкости, в которой плавают куски покрупнее и помельче, опускает туда хобот и начинает фрякать, издавая хлюпающе-хрюкающие звуки и при этом млея от удовольствия. Фидошники делятся на несколько подвидов.

Юзеры розового цвета, у них тонкая нежная кожа и глаза большие, глупые и добрые.

Поинт похож на юзера, только шкура погрубее и не такая розовая, а в глазах доброты меньше.

У нод и сисопов шкура толстая, покрытая жесткой щетиной и шрамами от прошлых битв, вся грязно-бурая — никакой розовости нет и в помине, у основания хобота имеются клыки.

Есть еще страшный хищный подвид, получающийся в результате мутации остальных — модераторы. Их роговая броня покрыта костяными шипами, глазки маленькие, злобные, сверкают красным, а копыта имеют форму крестовой отвертки, поэтому там, где пробежит модератор, остаются «+»-образные следы. Эти копыта — основное оружие хищника, ни один фидошник не выдерживает больше трех ударов. Впрочем, некоторых модераторы убивают одним ударом 5-дюймовых клыков или трехгранного хвоста. Охотничий ареал модератора называется эхой. Модераторы тщательно охраняют свою территорию: модератор, забредший в чужую эху, может быть убит ее хозяином так же, как другие фидошники.

Модераторы бывают двух видов: одни небольшие и проворные, охотятся ежедневно, но редко добывают больше одной жертвы за раз; другие — массивные и неуклюжие, — наевшись, подолгу спят, зато, проснувшись, проносятся с визгом и грохотом по всей эхе, давя все на своем пути.

Немаловажную роль в экологии Фидо играют модемы — большие бескрылые кровососущие паразиты с длинным хоботком. Новейшие исследования показали, что это не паразиты, а симбионты; некоторые ученые даже полагают, что без них невозможен процесс фряканья...

По материалам "КомпьюТерра"

ЕСЛИ MICROSOFT НАЧНЕТ СТРОИТЬ МАШИНЫ...

1. В любой момент времени Модель Года в стадии доработки и будет доступна только через год.

2. Каждый раз, когда они рисуют новую разметку на дорогах, вы должны покупать новую машину.

3. Если ваша машина беспричинно умирает, просто сделайте рестарт. Не помогло — сделайте рестарт. Если проблема осталась — сделайте рестарт... рестарт... рестарт...

4. В машину помещается один человек, но если это машина'95 или машинаNT, вам нужно всего лишь докупить сидения.

5. Самое лучшее развлечение — upgrade. "Секунду... Вот теперь порядок! Следующий upgrade — завтра и очень дешево!"

6. Sun Motorsystems создают машины на солнечных батареях, вдвое надежнее, в 5 раз быстрее, но которые ездят только на 5% дорог.

7. Все датчики на передней панели будут заменяться на один по имени «General Car Fault».

8. Люди будут восхищены "новшествами" в машинах Microsoft, абсолютно забывая, что они были доступны в других системах веками.

9. Все срочно переходят на МикроСофт Бензин™.

10. Новые сидения примут форму любой задницы.

11. Intel создаст 128-цилиндровый двигатель, но автомобиль'95 будет использовать только 32 из них. Самый последний релиз автомобиляNT — аж целых 64, что будет настойчиво рекламироваться. Тем временем в двигателе MIPS из Silicon Lamborgini будет давно стоять 256 цилиндров, но это — для избранных.

13. Доходы компании достигнут космических цифр — ведь им первым придет в голову встроить пепельницы во все детали корпуса.

КВ CD-мания

Вышла в свет новая, как говорится в книгах, "переработанная и дополненная" версия Microsoft Music Central '96.

• В отличие от вышерассмотренной энциклопедии, информации более чем достаточно.

Подробнейшие статьи обо всех стилях и направлениях в музыке, от рэпа, до классики. Дискографии, отрывки из видеоклипов, записи песен и просто информация об огромном количестве групп и певцов.

Предметный указатель, то есть вы, может быстро найти интересующего вас исполнителя по его имени или по названию песни. Кроме того, есть возможность включить только видеофрагменты или информационные статьи или записи мелодий.

Довольно много видеоотрывков, причем, это не видеоклип, где исполнитель только открывает рот под фонограмму, это "живой" отрывок из концертной записи, что довольно приятно, особенно истинным меломанам.

Описывать данную энциклопедию более подробно не имеет смысла, это надо видеть.

В общем, диск получился довольно неплохой. С чем я вас и поздравляю.

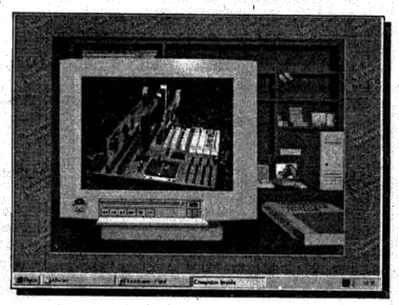
Многие дорого бы дали, чтобы на столе у них лежал универсальный справочник по компьютерной технике. Ну, если не по всей, то хотя бы основные моменты. К примеру, из чего состоит и как работает самый обыкновенный персональный компьютер. Да еще чтобы по-русски, и желательно с картинками.

Такой справочник есть. Это — энциклопедия по компьютеру на компакт-диске. Если у вас дома стоит компьютер, то, уверяю вас, этот компакт здорово поможет разобраться в сложном устройстве вашего электронного друга, объяснит принципы работы, предостережет от нежелательных действий. К тому же все сделано в виде видеороликов, с отличным звуковым сопровождением и огромным количеством качественных фотографий. Да еще вдобавок вы сможете узнать историю компьютерной техники и протестировать собственный компьютер.

Работать с энциклопедией очень просто.

Достаточно щелкнуть на изображении одного из устройств компьютера, и вам сразу же будет предоставлена подробнейшая информация о его (устройства) предназначении и принципе действия.

Если вы хотите узнать более подробно о «внутренностях» компьютера, щелкните мышкой на изображении системного блока, он развернется и... все устройства как на ладони. Выбирайте любое и смотрите видеоролик.



Если вас интересуют еще более подробные данные, загляните в справочное пособие. Там вы найдете все, что угодно, при этом отлично проиллюстрированное.

Вдобавок к этой программе на диске вы найдете огромное количество тестовых программ, разнообразных утилит, операционных систем и несколько интересных образовательных игр.

Приобрести эти, а также многие другие энциклопедии можно в фирме "Видеопечать" позвонив по одному из следующих телефонов — 265-23-67, 265-33-34, 265-34-23.

Иван КОВАЛЕВ