

Стелс-вирусы

Стелс-вирусы теми или иными способами скрывают факт своего присутствия в системе. Известны стелс-вирусы всех типов - загрузочные вирусы, файловые DOS-вирусы и даже макро-вирусы.

Загрузочные вирусы

Загрузочные стелс-вирусы для скрытия своего кода используют два основных способа. Первый из них заключается в том, что вирус перехватывает команды чтения зараженного сектора (INT 13h) и подставляет вместо него незараженный оригинал. Этот способ делает вирус невидимым для любой DOS-программы, включая антивирусы, неспособные "лечить" оперативную память компьютера. Возможен перехват команд чтения секторов на уровне более низком, чем INT 13h.

Второй способ направлен против антивирусов, поддерживающих команды прямого чтения секторов через порты контроллера диска. Такие вирусы при запуске любой программы (включая антивирус) восстанавливают зараженные сектора, а после окончания ее работы снова заражают диск. Поскольку для этого вирусу приходится перехватывать запуск и окончание работы программ, то он должен перехватывать также DOS-прерывание INT 21h.

С некоторыми оговорками стелс-вирусами можно назвать вирусы, которые вносят минимальные изменения в заражаемый сектор (например, при заражении MBR правят только активный адрес загрузочного сектора - изменению подлежат только 3 байта), либо маскируются под код стандартного загрузчика.

Файловые вирусы

Большинство файловых стелс вирусов использует те же приемы, что приведены выше: они либо перехватывают DOS-вызовы обращения к файлам (INT 21h) либо временно лечат файл при его открытии и заражают при закрытии. Также как и для загрузочных вирусов, существуют файловые вирусы, использующие для своих стелс-функций перехват прерываний более низкого уровня - вызовы драйверов DOS, INT 25h и даже INT 13h.

Полноценные файловые стелс-вирусы, использующие первый способ скрытия своего кода, в большинстве своем достаточно громоздки, поскольку им приходится перехватывать большое количество DOS-функций работы с файлами: открытие/закрытие, чтение/запись, поиск, запуск, переименование и т.д., причем необходимо поддерживать оба варианта некоторых вызовов (FCB/ASCII), а после появления Windows95/NT им стало необходимо также обрабатывать третий вариант - функции работы с длинными именами файлов.

Некоторые вирусы используют часть функций полноценного стелс-вируса. Чаще всего они перехватывают функции DOS FindFirst и FindNext (INT 21h,

АН=11h, 12h, 4Eh, 4Fh) и "уменьшают" размер зараженных файлов. Такой вирус невозможно определить по изменению размеров файлов, если, конечно, он резидентно находится в памяти. Программы, которые не используют указанные функции DOS (например, "Нортоновские утилиты"), а напрямую используют содержимое секторов, хранящих каталог, показывают правильную длину зараженных файлов.

Макро-вирусы

Реализация стелс-алгоритмов в макро-вирусах является, наверное, наиболее простой задачей - достаточно всего лишь запретить вызов меню File/Templates или Tools/Macro. Достигается это либо удалением этих пунктов меню из списка, либо их подменой на макросы FileTemplates и ToolsMacro.

Частично стелс-вирусами можно назвать небольшую группу макро-вирусов, которые хранят свой основной код не в самом макросе, а в других областях документа - в его переменных или в Auto-text.

Резидентные вирусы

Под термином "резидентность" (DOS'овский термин TSR - Terminate and Stay Resident) понимается способность вирусов оставлять свои копии в системной памяти, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов). Таким образом, резидентные вирусы активны не только в момент работы зараженной программы, но и после того, как программа закончила свою работу. Резидентные копии таких вирусов остаются жизнеспособными вплоть до очередной перезагрузки, даже если на диске уничтожены все зараженные файлы. Часто от таких вирусов невозможно избавиться восстановлением всех копий файлов с дистрибутивных дисков или backup-копий. Резидентная копия вируса остается активной и заражает вновь создаваемые файлы. То же верно и для загрузочных вирусов - форматирование диска при наличии в памяти резидентного вируса не всегда вылечивает диск, поскольку многие резидентные вирусы заражают диск повторно после того, как он отформатирован.

Нерезидентные вирусы, напротив, активны довольно непродолжительное время - только в момент запуска зараженной программы. Для своего распространения они ищут на диске незараженные файлы и записываются в них. После того, как код вируса передает управление программе-носителю, влияние вируса на работу операционной системы сводится к нулю вплоть до очередного запуска какой-либо зараженной программы. Поэтому файлы, зараженные нерезидентными вирусами значительно проще удалить с диска и при этом не позволить вирусу заразить их повторно.