

Макро-вирусы

Макро-вирусы (macro viruses) являются программами на языках (макро-языках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макро-вирусы для Microsoft Word, Excel и Office97. Существуют также макро-вирусы, заражающие документы Ami Pro и базы данных Microsoft Access.

Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макро-языка с возможностями:

привязки программы на макро-языке к конкретному файлу;

копирования макро-программ из одного файла в другой;

возможность получения управления макро-программой без вмешательства пользователя (автоматические или стандартные макросы).

Данным условиям удовлетворяют редакторы Microsoft Word, Office97 и AmiPro, а также электронная таблица Excel и база данных Microsoft Access.

Эти системы содержат в себе макро-языки: Word - Word Basic, Excel, Office97 (включая Word97, Excel97 и Access) - Visual Basic for Applications.

При этом:

макро-программы привязаны к конкретному файлу (AmiPro) или находятся внутри файла (Word, Excel, Office97);

макро-язык позволяет копировать файлы (AmiPro) или перемещать макро-программы в служебные файлы системы и редактируемые файлы (Word, Excel, Office97);

при работе с файлом при определенных условиях (открытие, закрытие и т.д.) вызываются макро-программы (если таковые есть), которые определены специальным образом (AmiPro) или имеют стандартные имена (Word, Excel, Office97).

Данная особенность макро-языков предназначена для автоматической обработки данных в больших организациях или в глобальных сетях и позволяет организовать так называемый "автоматизированный документооборот". С другой стороны, возможности макро-языков таких систем позволяют вирусу переносить свой код в другие файлы, и таким образом заражать их.

На сегодняшний день известны четыре системы, для которых существуют вирусы - Microsoft Word, Excel, Office97 и AmiPro. В этих системах вирусы получают управление при открытии или закрытии зараженного файла, перехватывают стандартные файловые функции и затем заражают файлы, к которым каким-либо образом идет обращение. По аналогии с MS-DOS можно сказать, что большинство макро-вирусов являются резидентными: они активны не только в момент открытия/закрытия файла, но до тех пор, пока активен сам редактор.

Общие сведения

Физическое расположение вируса внутри файла зависит от его формата, который в случае продуктов Microsoft чрезвычайно сложен - каждый файл-документ Word, Office97 или таблица Excel представляют собой последовательность блоков данных (каждый из которых также имеет свой формат), объединенных между собой при помощи большого количества служебных данных. Этот формат носит название OLE2 - Object Linking and Embedding. Структура файлов Word, Excel и Office97 (OLE2) напоминает усложненную файловую систему дисков DOS: "корневой каталог" файла-документа или таблицы указывает на основные подкаталоги различных блоков данных, несколько таблиц FAT содержат информацию о расположении блоков данных в документе и т.д.

Более того, система Office Binder, поддерживающая стандарты Word и Excel позволяет создавать файлы, одновременно содержащие один или несколько документов в формате Word и одну или несколько таблиц в формате Excel. При этом Word-вирусы способны поражать Word-документы, а Excel-вирусы - Excel-таблицы, и все это возможно в пределах одного дискового файла. То же справедливо и для Office97.

Следует отметить, что Word версий 6 и 7 позволяет шифровать присутствующие в документе макросы. Таким образом, некоторые Word-вирусы присутствуют в зараженных документах в зашифрованном (Execute only) виде.

Большинство известных вирусов для Word несовместимы с национальными (в том числе с русской) версиями Word, или наоборот - рассчитаны только на локализованные версии Word и не работают под английской версией. Однако вирус в документе все равно остается активным и может заражать другие компьютеры с установленной на них соответствующей версией Word.

Вирусы для Word могут заражать компьютеры любого класса, а не только IBM-PC. Заражение возможно в том случае, если на данном компьютере установлен текстовый редактор, полностью совместимый с Microsoft Word версии 6 или 7 (например, MS Word for Macintosh). То же справедливо для Excel и Office97.

Следует также отметить, что сложность форматов документов Word, таблиц Excel и особенно Office97 имеет следующую особенность: в файлах-документах и таблицах присутствуют "лишние" блоки данных, т.е. данные, которые никак не связаны с редактируемым текстом или таблицами, либо являются случайно оказавшимися там копиями прочих данных файла. Причиной возникновения таких блоков данных является кластерная организация данных в OLE2-документах и таблицах - даже если введен всего один символ текста, то под него выделяется один или даже несколько кластеров данных. При сохранении документов и таблиц в кластерах, не заполненных "полезными" данными, остается "мусор", который попадает в файл вместе с прочими данными. Количество "мусора" в файлах может быть уменьшено отменой пункта настройки Word/Excel "Allow Fast Save", однако

это лишь уменьшает общее количество "мусора", но не убирает его полностью.

Следствием этого является тот факт, что при редактировании документа его размер изменяется вне зависимости от производимых с ним действий - при добавлении нового текста размер файла может уменьшиться, а при удалении части текста - увеличиться. То же и с макро-вирусами: при заражении файла его размер может уменьшиться, увеличиться или остаться неизменным.

Следует также отметить тот факт, что некоторые версии OLE2.DLL содержат небольшой недочет, в результате которого при работе с документами Word, Excel и особенно Office97 в блоки "мусора" могут попасть случайные данные с диска, включая конфиденциальные (удаленные файлы, каталоги и т.д.). В эти блоки могут попасть также команды вируса. В результате после лечения зараженных документов активный код вируса удаляется из файла, но в блоках "мусора" могут остаться часть его команд. Такие следы присутствия вируса иногда видимы при помощи текстовых редакторов и даже могут вызвать реакцию некоторых антивирусных программ. Однако эти остатки вируса совершенно безвредны: Word и Excel не обращают на них никакого внимания.

Принципы работы

При работе с документом Word версий 6 и 7 выполняет различные действия: открывает документ, сохраняет, печатает, закрывает и т.д. При этом Word ищет и выполняет соответствующие "встроенные макросы" - при сохранении файла по команде File/Save вызывается макрос FileSave, при сохранении по команде File/SaveAs - FileSaveAs, при печати документов - FilePrint и т.д., если, конечно, таковые макросы определены.

Существует также несколько "авто-макросов", автоматически вызываемые при различных условиях. Например, при открытии документа Word проверяет его на наличие макроса AutoOpen. Если такой макрос присутствует, то Word выполняет его. При закрытии документа Word выполняет макрос AutoClose, при запуске Word вызывается макрос AutoExec, при завершении работы - AutoExit, при создании нового документа - AutoNew.

Похожие механизмы (но с другими именами макросов и функций) используются и в Excel/Office97, в которых роль авто- и встроенных макросов выполняют авто- и встроенные функции, присутствующие в каком-либо макросе или макросах, причем в одном макросе могут присутствовать несколько встроенных и авто-функций.

Автоматически (т.е. без участия пользователя) выполняются также макросы/функции, ассоциированные с какой-либо клавишей либо моментом времени или датой, т.е. Word/Excel вызывают макрос/функцию при нажатии на какую-либо конкретную клавишу (или комбинацию клавиш) либо при достижении какого-либо момента времени. В Office97 возможности по перехвату событий несколько расширены, но принцип используется тот же.

Макро-вирусы, поражающие файлы Word, Excel или Office97 как правило пользуются одним из трех перечисленных выше приемов - в вирусе либо присутствует авто-макрос (авто-функция), либо переопределен один из стандартных системных макросов (ассоциированный с каким-либо пунктом меню), либо макрос вируса вызывается автоматически при нажатии на какую-либо клавишу или комбинацию клавиш. Существуют также полу-вирусы, которые не используют всех этих приемов и размножаются, только когда пользователь самостоятельно запускает их на выполнение.

Таким образом, если документ заражен, при открытии документа Word вызывает зараженный автоматический макрос AutoOpen (или AutoClose при закрытии документа) и, таким образом, запускает код вируса, если это не запрещено системной переменной DisableAutoMacros. Если вирус содержит макросы со стандартными именами, они получают управление при вызове соответствующего пункта меню (File/Open, File/Close, File/SaveAs). Если же переопределен какой-либо символ клавиатуры, то вирус активизируется только после нажатия на соответствующую клавишу.

Большинство макро-вирусов содержат все свои функции в виде стандартных макросов Word/Excel/Office97. Существуют, однако, вирусы, использующие приемы скрытия своего кода и хранящие свой код в виде не-макросов. Известно три подобных приема, все они используют возможность макросов создавать, редактировать и исполнять другие макросы. Как правило подобные вирусы имеют небольшой (иногда - полиморфный) макрос-загрузчик вируса, который вызывает встроенный редактор макросов, создает новый макрос, заполняет его основным кодом вируса, выполняет и затем, как правило, уничтожает (чтобы скрыть следы присутствия вируса). Основной код таких вирусов присутствует либо в самом макросе вируса в виде текстовых строк (иногда - зашифрованных), либо хранится в области переменных документа или в области Auto-text.

Алгоритм работы Word макро-вирусов

Большинство известных Word-вирусов (версий 6, 7 и Word97) при запуске переносят свой код (макросы) в область глобальных макросов документа ("общие" макросы), для этого они используют команды копирования макросов MacroCopy, Organizer.Copy либо при помощи редактора макросов - вирус вызывает его, создает новый макрос, вставляет в него свой код, который и сохраняет в документе.

При выходе из Word глобальные макросы (включая макросы вируса) автоматически записываются в DOT-файл глобальных макросов (обычно таким файлом является NORMAL.DOT). Таким образом, при следующем запуске редактора MS-Word вирус активизируется в тот момент, когда WinWord грузит глобальные макросы, т.е. сразу.

Затем вирус переопределяет (или уже содержит в себе) один или несколько стандартных макросов (например, FileOpen, FileSave, FileSaveAs, FilePrint) и перехватывает таким образом команды работы с файлами. При вызове этих команд вирус заражает файл, к которому идет обращение. Для этого вирус конвертирует файл в формат Template (что делает невозможной дальнейшие

изменения формата файла, т.е. конвертирование в какой-либо не-Template формат) и записывает в файл свои макросы, включая Auto-макрос.

Таким образом, если вирус перехватывает макрос FileSaveAs, то заражается каждый DOC-файл, сохраняемый через перехваченный вирусом макрос. Если перехвачен макрос FileOpen, то вирус записывается в файл при его считывании с диска.

Второй способ внедрения вируса в систему используется значительно реже - он базируется на так называемых "Add-in" файлах, т.е. файлах, являющихся служебными дополнениями к Word. В этом случае NORMAL.DOT не изменяется, а Word при запуске загружает макросы вируса из файла (или файлов), определенного как "Add-in". Этот способ практически полностью повторяет заражение глобальных макросов за тем исключением, что макросы вируса хранятся не в NORMAL.DOT, а в каком-либо другом файле.

Возможно также внедрения вируса в файлы, расположенные в каталоге STARTUP, - Word автоматически подгружает файлы-темплейты из этого каталога, но такие вирусы пока не встречались.

Рассмотренные выше способы внедрения в систему представляют собой некоторый аналог резидентных DOS-вирусов. Аналогом нерезидентности являются макро-вирусы, которые не переносят свой код в область системных макросов - для заражения других файлов-документов они либо ищут их при помощи встроенных в Word функций работы с файлами, либо обращаются к списку последних редактированных файлов (Recently used file list). Затем такие вирусы открывают документ, заражают его и закрывают.

Алгоритм работы Excel макро-вирусов

Методы размножения Excel-вирусов (включая Excel97) в целом аналогичны методам Word-вирусов. Различия заключаются в командах копирования макросов (например, Sheets.Copy) и в отсутствии NORMAL.DOT - его функцию (в вирусном смысле) выполняют файлы в STARTUP-каталоге Excel.

Следует отметить, что существует два возможных варианта расположения кода макро-вирусов в таблицах Excel. Подавляющее большинство таких вирусов записывают свой код в формате VBA (Visual Basic for Applications), однако существуют вирусы, хранящие свой код в старом формате Excel версии 4.0. Такие вирусы по своей сути ничем не отличаются от VBA-вирусов, за исключением отличий в формате расположения кодов вируса в таблицах Excel.

Несмотря на то, что в новых версиях Excel (начиная с версии 5) используются более совершенные технологии, возможность исполнения макросов старых версий Excel была оставлена для поддержания совместимости. По этой причине все макросы, написанные в формате Excel 4, вполне работоспособны во всех последующих версиях, несмотря на то, что Microsoft не рекомендует использовать их и не включает необходимую документацию в комплект поставки Excel.