УДК 004.492

А. В. Никишин, М. А. Павлющик, Д. В. Зенкин
("Лаборатория Касперского")

Компьютерные вирусы: рискуют все. Антивирусные программы "Лаборатории Касперского"*

Рассматриваются макро-вирусы, их происхождение, реальная оценка их угрозы и ущерба, методы защиты от них: алгоритмические, программные и операционно-технологические, разработанные в "Лаборатории Касперского" на базе макро-языка VBA, соответствующего международным требованиям.

1. ЧТО ТАКОЕ МАКРО-ВИРУС И С ЧЕМ ЕГО ЕДЯТ?

Скоро исполняется пять лет как название "макро-вирус" прочно вошло в лексикон компьютерных пользователей всего мира. Несмотря на разработку надежных средств защиты против этой "заразы" и многочисленные обзоры методов борьбы с ней, это словосочетание до сих пор заставляет миллионы пользователей содрогаться и запускать на всякий случай антивирусные сканеры. Что же такое макро-вирусы? Чем они отличаются от других представителей компьютерной "фауны"? Насколько они опасны? Есть ли средства защиты против них? Полная или частичная неясность этих вопросов и сделала их предметом этой статьи.

Макро-вирусы являются разновидностью компьютерных вирусов, созданной при помощи специальных макроязыков, встроенных в популярные офисные приложения наподобие Word, Excel, Access, PowerPoint, Project, Corel Draw! и др. Макроязыки используются для написания специальных программ (макросов) для повышения эффективности работы в этих приложениях. Например, с помощью макроса Word можно автоматизировать процесс заполнения и рассылки факсов. Пользователю достаточно будет только ввести данные в поля формы и нажать на кнопку — все остальное макрос сделает сам. Таким образом, использование макросов позволяет максимально упростить и автоматизировать работу. Проблема заключается в том, что это можно сделать незаметно для пользователя. Более того, можно незаметно совершить гораздо более опасные действия: изменить содержание документа, стереть файл или директорию. Вредоносные макросы, обладающие способностью создавать свои копии и совершающие некоторые действия без ведома пользователя, и называются макро-вирусами.

Функциональные возможности этого типа вирусов ограничены возможностями макроязыков, с помощью которых они созданы. Именно с помощью этих языков они размножаются, распространяются, наносят вред зараженным компьютерам. Таким образом, чем более продвинутый макроязык, тем более хитрыми, изощренными и опасными могут быть макро-вирусы. Наиболее распространенный макроязык Visual Basic for Applications (VBA) предоставляет вирусам наиболее полный спектр возможностей. Причем, с каждой новой версией эти возможности стремительно расширяются. Таким образом, чем более совершенными будут офисные приложения, тем опаснее будет становиться работа в них.

2. КАК ЭТО ВСЕ НАЧИНАЛОСЬ?

Первый макро-вирус для MS Word "Concept" заявил о себе в августе 1995 г., когда все прогрессивное человечество праздновало торжественный запуск Windows 95 и очередной версии MS Office. В считанные дни вирус вызвал настоящую пандемию, заразив десятки тысяч компьютеров по всему миру и прочно заняв первое место в статистических отчетах различных научно-исследовательских организаций и компьютерных изданий. Важно отметить, что многие антивирусные компании оказались просто не готовы к такому повороту событий и им пришлось вносить значительные изменения в используемые антивирусные "движки" или вообще заново их создавать.

В июле 1996 г. в "диком виде" обнаружен первый макро-вирус для MS Excel — "Laroux", практически одновременно парализовавший работу двух нефтедобывающих компаний в разных концах земного шара — в ЮАР и на Аляске.

Март 1997 г. ознаменовался появлением макровируса "ShareFun", идея которого была позднее позаимствована недавно осужденным Дэвидом Смитом, автором нашумевшего в конце марта 1999 г. вируса Melissa. В ShareFun был впервые использован метод распространения через электронную почту, посредством рассылки зараженных сообщений почтовой программой MS Mail.

В марте 1998 г. жертвой компьютерных вирусов ("AccessiV") пало еще одно офисное приложение — система обработки баз данных MS Access. А в самом конце того же года макро-вирус "Attach" "сразил" программу создания презентаций MS PowePoint.

В 1999 г. макро-вирусы продолжили свой "качественный" рост и распространили свое влияние

* В статье использованы фрагменты книги Е. Касперского "Компьютерные вирусы и как с ними бороться".— М., 1996.

на файлы графического редактора Corel Draw! (обнаруженный в мае вирус "Gala") и документы планировщика MS Project (вирус "Corner", открытый в конце октября).

Вместе с тем, все в большем количестве стали появляться так называемые многоплатформенные макро-вирусы, т. е. вирусы, способные внедряться сразу в несколько офисных приложений. Классическим примером тому может служить "Triplicate" — первый известный макро-вирус, одновременно заражающий документы Word, Excel и PowerPoint. Кроме того, они берут на вооружение все новые уловки для усложнения процедуры их обнаружения и удаления. В первую очередь это — Stealth-технологии (уловка, делающая вирус невидимым в зараженном документе) и полиморфизм (модификация (шифрование) исходного кода вируса при сохранении его функциональности).

3. ПОЧЕМУ ИМЕННО МАКРО-ВИРУСЫ?

За последние несколько лет макро-вирусы прочно занимают первые места в списках наиболее распространенных вирусов. По данным Международной ассоциации компьютерной безопасности (www.icsa.net), доля представителей этого класса компьютерной "фауны" в общем числе "диких" вирусов составляет 2/3. Согласно статистике "Лаборатории Касперского", это число меньше (около 55%), однако оно все равно наглядно демонстрирует преобладание макро-вирусов.

Такая высокая распространенность макровирусов имеет разумное объяснение.

Во-первых, это высокое распространение объектов их поражения, т. е. офисных приложений. Сегодня практически нет таких людей, которые бы не использовали в своей повседневной работе текстовый процессор, электронные таблицы, систему обработки базы данных или мастер презентаций.

Во-вторых, — очень низкий уровень встроенной антивирусной защиты этих приложений. Несмотря на все уверения Microsoft об изменении ситуации в новом MS Office 2000, наш многолетний профессиональный опыт позволяет утверждать обратное: офисные приложения остались столь же уязвимыми для вирусов, как и их предшественники.

В-третьих, простота создания макро-вирусов. Для того чтобы написать вирус, например, для MX Word, достаточно изучить азы языка программирования VBA. Несмотря на то, что он является самым простым и доступным среди всех остальных языков, он предоставляет вирусописателям все необходимые рычаги для того, чтобы уничтожить важную информацию и надолго вывести компьютер из строя.

Наконец, *в-четвертых*, наиболее популярные офисные приложения (в первую очередь из пакета MS Office), как правило, интегрированы с почтовыми программами (например, MS Outlook). Это обстоятельство определяет доступ макро-вирусов к электронной почте — наиболее удобному и быстрому способу распространения. Таким образом, они имеют неограниченные возможности для молниеносного поражения миллионов компьютеров по всему миру.

4. ЧТО ДЕЛАТЬ?

Макро-вирусы представляют реальную угрозу компьютерным пользователям. Мало того, по нашим прогнозам, одновременно с совершенствованием макроязыков и обнаружением новых "дыр" в системах безопасности офисных приложений, макровирусы будут становиться все более неуловимыми и опасными, а скорость их распространения достигнет небывалых величин.

Несмотря на столь мрачные прогнозы, необходимо помнить главное условие борьбы с компьютерными вирусами — не паниковать. Круглосуточно на страже компьютерной безопасности находятся тысячи высококлассных антивирусных специалистов по всему миру. Поверьте нам, их профессионализм многократно превосходит совокупный потенциал всего хакерского движения. За многие годы существования антивирусная индустрия изобрела много способов противодействия компьютерным вирусам. Однако в чем преимущества и недостатки того или иного способа защиты? Насколько они эффективны именно по отношению к макровирусам?

На сегодняшний день выделяется пять основных подходов к обеспечению антивирусной безопасности.

Во-первых, это классический сканер — пионер антивирусного движения, впервые появившийся на свет практически одновременно с самими компьютерными вирусами. Принцип его работы заключается в поиске в файлах, памяти, и загрузочных секторах вирусных сигнатур, т. е. уникального программного кода вируса. Здесь возникает первая проблема, потому что малейшие модификации вируса могут сделать его невидимым для сканера. К примеру, существует несколько десятков вариантов вируса Melissa, и почти для каждого из них антивирусным кампаниям приходилось выпускать отдельное обновление антивирусной базы. Последнее обстоятельство означает вторую проблему: время между появлением вируса и выходом соответствующего обновления пользователь оставался практически незащищенным от атак новых вирусов. Позднее, эксперты придумали и внедрили в сканеры оригинальный способ обнаружения неизвестных вирусов — эвристический анализатор, т. е. анализ кода программы на предмет возможного присутствия в нем компьютерного вируса. Однако данный метод характеризуется высоким уровнем ложных срабатываний (false alarm), недостаточной надежностью и невозможностью вылечить обнаруженные вирусы. Наконец, третья проблема: антивирусный сканер проверяет файлы, только когда пользователь "попросит" его это сделать, т. е. запустит сканер. Это требует от пользователя постоянного внимания и концентрации. Очень часто он забывает проверить сомнительный файл, загруженный, например, из Интернета и, в результате, своими руками заражает компьютер. Сканер способен определить факт заражения постфактум, т. е. уже после того, как в системе появится вирус.

Для устранения такой возможности был разработан *второй вид* антивирусных программ — антивирусные мониторы. По своей сути они являются разновидностью сканеров, которые постоянно находятся в памяти компьютера и осуществляют фоновую проверку файлов, загрузочных секторов и памяти в масштабе реального времени. Для включения антивирусной защиты, пользователю достаточно загрузить монитор при загрузке операционной системы. Все запускаемые файлы будут автоматически проверяться на вирусы.

Третья разновидность антивирусов — ревизоры изменений (integrity checkers). Их принцип рабо-

ты основан на снятии оригинальных "отпечатков" (CRC-сумм) с файлов и системных секторов. Эти "отпечатки" сохраняются в базе данных. При следующем запуске ревизор сверяет "отпечатки" с их оригиналами и сообщает пользователю о произошедших изменениях. У этого типа антивирусных программ тоже есть свои недостатки. Во-первых, ревизоры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. Во-вторых, они не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из резервной копии или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Этим пользуются некоторые вирусы, которые используют эту "слабость" ревизоров и заражают только вновь создаваемые файлы, оставаясь, таким образом, невидимыми для них. В-третьих, ревизоры требуют регулярного запуска — чем чаще это будет происходить, тем надежнее будет контроль за вирусной активностью.

Необходимо также упомянуть такую разновидность антивирусных программ, как иммунизаторы. Они делятся на два вида: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.

Первые обычно записываются в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на изменение. Недостаток у таких иммунизаторов всего один, но он принципиален: абсолютная неспособность обнаружить заражение stealth-вирусами (вирусами-невидимками), которые хитро скрывали свое присутствие в зараженном файле.

Второй тип иммунизаторов защищает систему от поражения каким-либо определенным вирусом. Файлы модифицируются таким образом, что вирус принимает их за уже зараженные. Например, чтобы предотвратить заражение COM-файла вирусом Jerusalem, достаточно дописать в его конец строку MsDos. Для защиты от резидентного вируса в память компьютера заносится программа, имитирующая копию вируса. При запуске вирус натыкается на нее и считает, что система уже заражена.

Второй тип иммунизации не может быть признан универсальным, поскольку нельзя иммунизировать файлы от всех известных вирусов: у каждого из них свои приемы определения зараженности файлов. Однако, несмотря на это, подобные иммунизаторы в качестве полумеры могут вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет определяться антивирусными сканерами.

Из-за описанных выше недостатков иммунизаторы не получили большого распространения и в настоящее время практически не используются.

Все перечисленные выше типы антивирусов не решают главной проблемы — защиты от неизвестных вирусов. Таким образом, компьютерные системы оказываются беззащитны перед ними до тех пор, пока антивирусные вендоры не разработают противоядия. Иногда на это требуется до нескольких недель. Все это время компании по всему миру имеют реальную "возможность" потерять важнейшие данные, от которых зависит их будущее.

Однозначно ответить на вопрос "что же делать с неизвестными вирусами?" нам предстоит лишь в грядущем тысячелетии. Однако уже сейчас можно сделать прогноз относительно наиболее перспективных путей развития антивирусного программного обеспечения. На наш взгляд, таким направлением станут так называемые поведенческие блокираторы (behaviour blocker/sandbox). Именно они имеют реальную возможность со 100%-й гарантией противостоять атакам новых вирусов.

Что такое поведенческий блокатор? Это резидентная программа, которая перехватывает различные события и в случае "подозрительных" действий (действий, которые может производить вирус или другая вредоносная программа), запрещает это действие или запрашивает разрешение у пользователя. Иными словами, блокиратор совершает не поиск сигнатуры, т. е. кода вируса, а отслеживает и предотвращает его действие. Идея блокираторов не нова. Они появились давно, однако эти антивирусные программы не получили широкого распространения из-за сложности настройки, требующей от пользователей глубоких знаний в области компьютерных технологий.

Давайте рассмотрим подробнее достоинства и недостатки поведенческих блокираторов. Теоретически блокиратор может предотвратить распространение любого как известного, так и неизвестного (написанного после блокиратора) вируса, предупреждая пользователя до того, как вирус заразит другие файлы или нанесет какой-либо вред компьютеру. Но вирусоподобные действия может производить и сама операционная система или полезные утилиты. Поведенческий блокиратор (здесь имеется в виду "классический" блокиратор, который используется для борьбы с файловыми вирусами) не может самостоятельно определить, кто же выполняет подозрительное действие — вирус, операционная система или какая-либо утилита и вынужден спрашивать подтверждения у пользователя. Т. е. в конечном счете решение зачастую принимает пользователь, который должен обладать достаточными знаниями и опытом, чтобы дать правильный ответ. В противном случае ОС или утилита не сможет произвести требуемое действие, либо вирус проникнет в систему. Именно по этой причине блокираторы и не стали популярными: их достоинства зачастую становились их недостатками, они казались слишком навязчивыми своими запросами и пользователи просто удаляли эти программы. К сожалению, ситуацию сможет исправить лишь изобретение искусственного интеллекта, который сможет самостоятельно разобраться в причинах того или иного подозрительного действия.

Возвращаясь к макро-вирусам, необходимо заметить, что здесь ситуация совсем иная. Если рассматривать программы, написанные на наиболее распространенном макроязыке VBA, то тут можно с очень большой долей вероятности отличить вредоносные действия от полезных. В конце 1999 г. "Лаборатория Касперского" разработала уникальную систему защиты от макро-вирусов пакета MS Office (версий 97 и 2000), основанную на новых подходах к принципам поведенческого блокиратора — AVP Office Guard. Благодаря проведенному анализу макро-вирусов в процессе моделирования их поведения, были определены наиболее часто встречающиеся последовательности их действий. Это позволило внедрить в программу новую, высокоинтеллектуальную систему фильтрации действий макросов и с высокой долей достоверности безошибочно выявлять те из них, которые представляют собой реальную опасность. Именно благодаря