Министерство образования XXX

Государственное бюджетное профессиональное образовательное учреждение

XXX «Колледж «XXX»

09.02.07

ОТЧЕТ

По лабораторным работам

МДК 04.02 Обеспечение качества функционирования компьютерных систем

ККОО.ПМ.XXX.000

Студент XXX

Преподаватель XXX

Дата защиты_____ Оценка_____

2022

Лабораторная работа №5.2

Изучение работы макровируса

Цель работы: изучить работу макровируса

Ход работы

С момента появления персональных компьютеров начала свой отсчет и история компьютерных вирусов. Любой вирус внедряет свой код в тело программы, благодаря чему он будет выполняться при каждом ее запуске. Большинство вирусов распространяется с помощью дисков и через сеть. В настоящее время имеется около тысячи видов вирусов. Учитывая тот факт, что каждый из них существует в нескольких модификациях, нужно увеличить это число в 5-10 раз. Существуют так называемые макровирусы, которые распространяются с помощью файлов шаблонов.

Макровирусы – это программы, написанные на так называемых макроязыках, встроенных в некоторые системы обработки данных (текстовые и графические редакторы, электронные таблицы и т. д.). Для своего размножения такие вирусы используют возможности макроязыков, они переносятся от одного зараженного файла к другому.

Наибольшее распространение получили макровирусы для Microsoft Word, Excel. Макровирусы получают управление при открытии или закрытии зараженного файла, перехватывают стандартные файловые функции и затем заражают файлы, к которым каким-либо образом идет обращение. Большинство макровирусов являются резидентными вирусами: они активны не только в момент открытия или закрытия файла, но до тех пор, пока активен сам текстовый или табличный редактор (а некоторые после выключения компьютера).

Первый макровирус был создан в 1999 год - вирус Melissa для MS Word, сочетавшего в себе также и функциональность интернет-червя. Сразу же после заражения системы он считывал адресную книгу почтовой программы MS Outlook и рассылал свои копии по первым 50 найденным

адресам.

В России первый макровирус появился в апреле 1997 года-вирус Laroux для Microsoft Excel, а создан в июне 1997 года- первый самошифрующийся вирус для Windows95.

Принцип «работы» макровирусов.

Работа макровируса происходит по следующему принципу: работая с документами, Microsoft Word выполняет разнообразные команды, отдающиеся на макроязыке. Первым делом программа проникает в главный шаблон, через который открываются все файлы этого формата. При этом вирус копирует свой код в макросы, которые обеспечивают доступ к главным параметрам. Выходя из приложения, происходит автоматическое сохранение в «.dot». Далее он попадает в стандартные макросы, перехватывая отправляемые другим файлам команды, инфицируя и их.

Основной механизм заражения.

Основной механизм заражения такой: когда мы открываем зараженный документ Word, макровирус копирует свой код в область глобальных макросов документа. А при выходе из Word глобальные макросы (включая макросы вируса) автоматически записываются в dot-файл глобальных макросов (шаблон Normal.dot).

Затем вирус переопределяет стандартные макросы (например, FileOpen, FileSave, FileSaveAs, FilePrint) и с их помощью перехватывает команды работы с файлами. При вызове этих команд заражается файл, к которому идет обращение.

Как обнаружить макровирусы.

Характерными признаками присутствия макровирусов являются:

1) невозможность сохранения зараженного документа Word в другой формат (по команде «Сохранить как…»);

2) невозможность записи документа в другой каталог или на другой диск командой «Сохранить как…»;

3) невозможность сохранения внесенных изменений в документ

(команда «Сохранить»);

4) недоступность вкладки «Уровень безопасности» (меню «Сервис» — «Макрос» — «Безопасность…»);

5) т.к. многие вирусы написаны с ошибками (или некорректно работают в различных версиях пакета Microsoft Office), то возможно появление соответствующих системных сообщений с кодом ошибки;

6) другие «странности» в поведении документов Word;

7) зачастую макровирусы можно обнаружить визуально. Дело в том, что большинство вирусописателей отличаются тщеславием: в свойствах файла Word (окно Свойства вызывается по щелчку правой кнопки мыши — выбрать из контекстного меню Свойства) на вкладке Сводка заполняют поля ввода (Название, Тема, Автор, Категория, Ключевые слова и Комментарий). Эту информацию (как правило, в макровирусах она пишется смесью латиницы с кириллицей и включает — в числе прочего — некоторые бессмысленные слова, типа муниципализмо и т. д.) можно увидеть при наведении указателя мыши на значок файла Word — она появляется во всплывающей подсказке и внизу слева в папке, в окошке «Подробно» (если включено Использование типичных задач для папок).

Как обезвредить макровирус. Опишите алгоритм, позволяющий в большинстве случаев обнаружить и обезвредить макровирус в MS Word.

Обнаружив подозрительный файл или документ, первым делом просканируйте его антивирусом. При обнаружении угрозы антивирусы попробуют вылечить его, а в случае неудачи полностью закроют к нему доступ.

В случае если был заражен весь компьютер, следует воспользоваться аварийным загрузочным диском, который содержит антивирус с последней базой данных. Он проведет сканирование винчестера и обезвредит все найденные им угрозы.

Если защититься таким образом не получается и аварийного диска нет, то следует попробовать метод «ручного» лечения:

Открываем «Этот компьютер», в верхнем меню заходим в «Параметры — Изменить параметры папок и поиска».

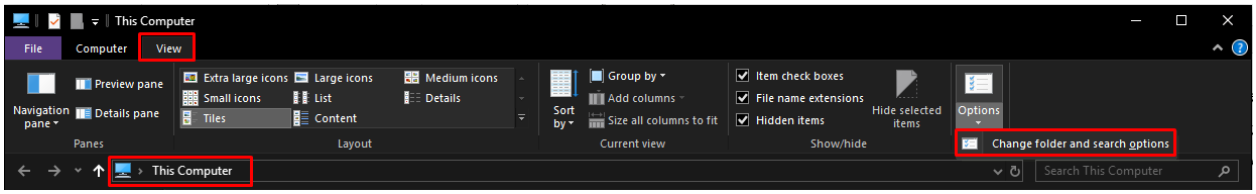

Рисунок 1 Этот компьютер

Перемещаемся во вкладку «Вид». Убираем галочку напротив пункта «Скрывать расширение для всех зарегистрированных типов».

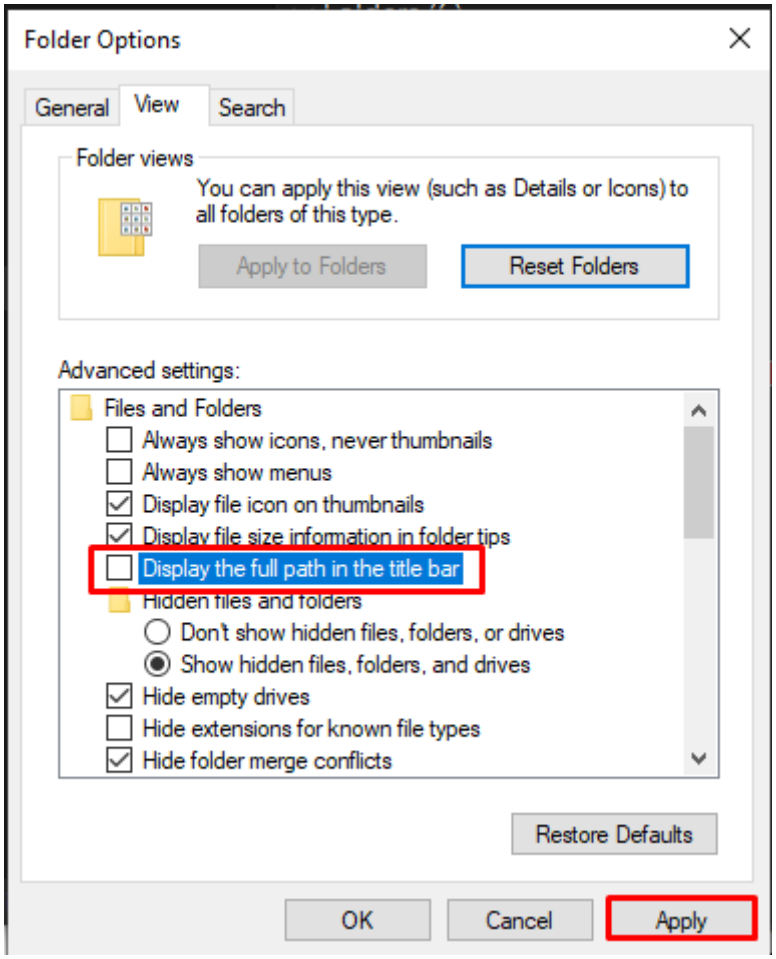

Рисунок 2 Меню «Вид»

Находим зловред. Изменяем его расширение с «.doc» на «.rtf». Благодаря формату «rtf» можно сохранить всю необходимую информацию, при этом надстройка VBA будет очищена от вредоносного кода.

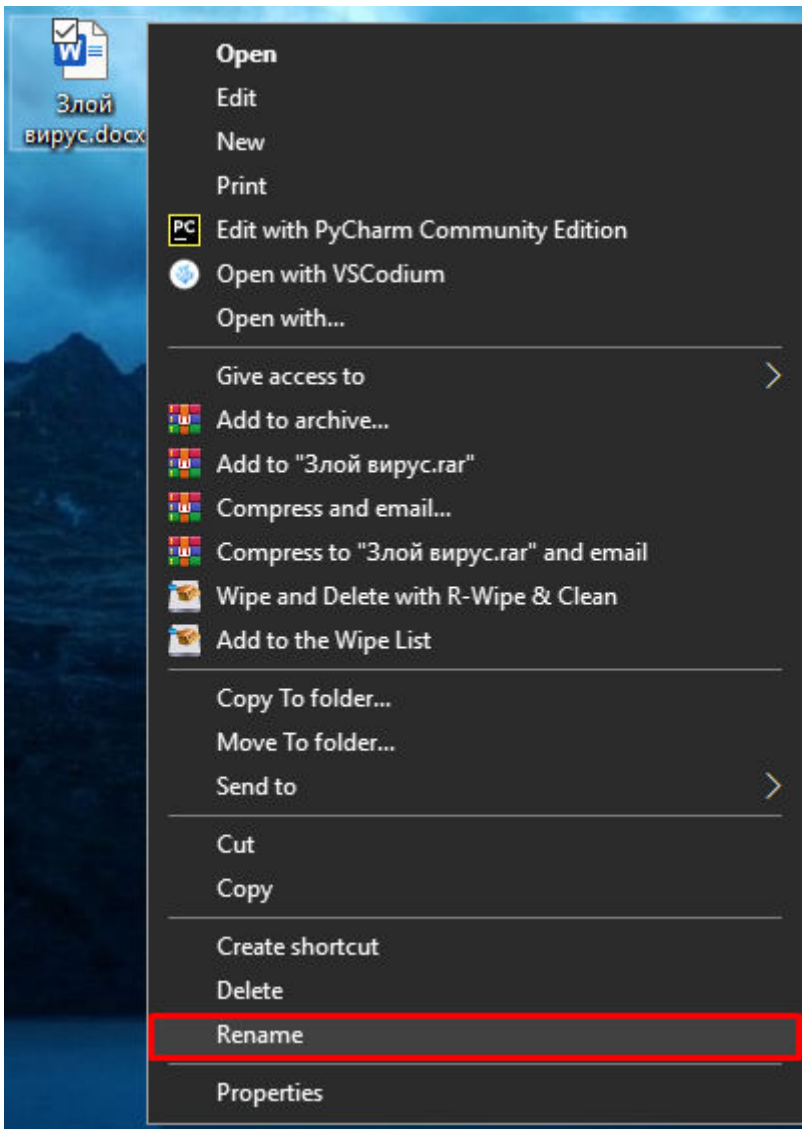

Рисунок 3 Кнопка «Переименовать»

Далее вы увидите сообщение системы о смене имени. Нажимаем «ДА».

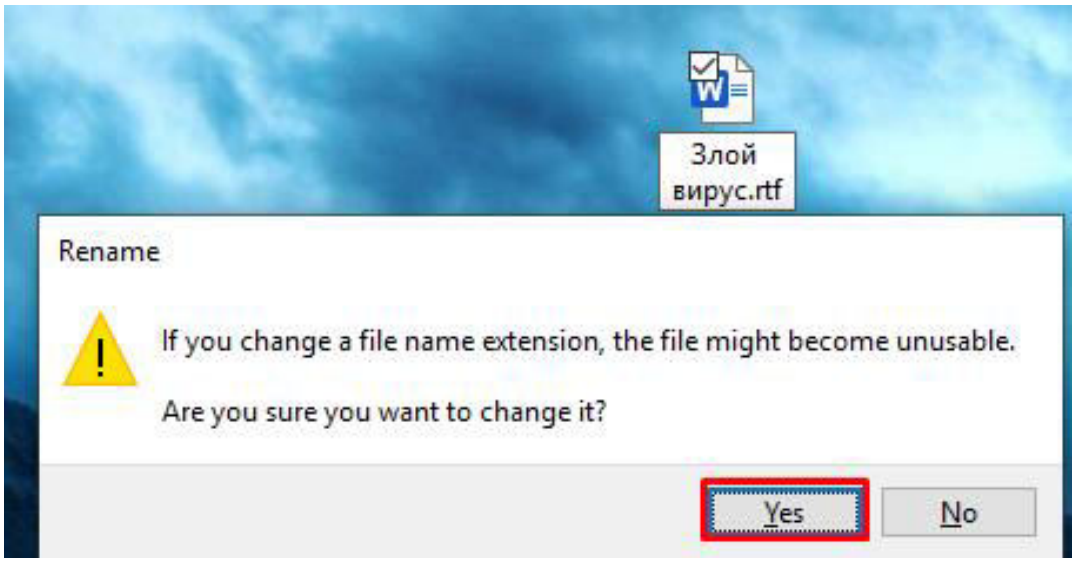

Рисунок 4 Согласие на изменение расширения файла

Изменяем расширение документа обратно. Восстанавливаем первоначальные параметры.

Таким образом, вы удалите макровирус с зараженного документа, однако это ни в коем случае не значит, что он не остался в системе. Именно поэтому рекомендую при первой возможности просканировать ПК антивирусом.

Защита от макровирусов.

- Необходимо иметь хороший антивирус и следить за его регулярными обновлениями.
- Если у вас старый компьютер или ноутбук, и вы не хотите еще больше нагружать и без того медленную систему, тогда обратите внимание на легкие защитники. Работают быстро даже на слабых машинах.
- Перед копированием с носителей или скачиванием программ из интернета тщательно проверяйте их, чтобы они не были заражены вредоносным ПО.
- Если у вас установлен плохой защитник или его вообще нет, то проводите сохранение в формате «.rtf».
- Храните важные данные сразу в нескольких местах на (ПК, флешке, любом файлообменнике или в облаке).

Контрольные вопросы

1. Назовите основные способы защиты от макровирусов.
   - Необходимо иметь хороший антивирус и следить за его регулярными обновлениями.
   - Храните важные данные сразу в нескольких местах на (ПК, флешке, любом файлообменнике или в облаке).
2. Опишите алгоритм, позволяющий обезвредить макровирус.

Обнаружив подозрительный файл или документ, первым делом просканируйте его антивирусом. При обнаружении угрозы антивирусы попробуют вылечить его, а в случае неудачи полностью закроют к нему

доступ.

В случае если был заражен весь компьютер, следует воспользоваться аварийным загрузочным диском, который содержит антивирус с последней базой данных. Он проведет сканирование винчестера и обезвредит все найденные им угрозы.

Если защититься таким образом не получается и аварийного диска нет, то следует попробовать метод «ручного» лечения:

Открываем «Этот компьютер», в верхнем меню заходим в «Параметры — Изменить параметры папок и поиска».

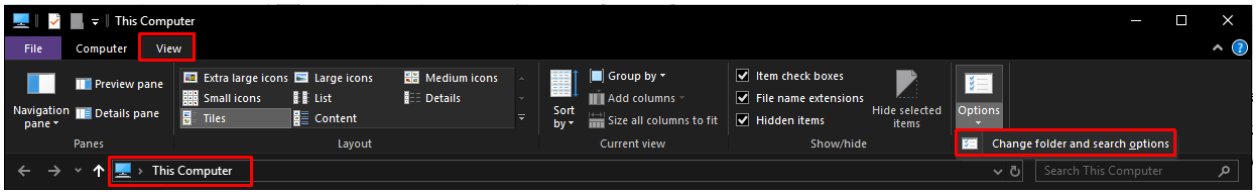

Рисунок 5 Этот компьютер

Перемещаемся во вкладку «Вид». Убираем галочку напротив пункта «Скрывать расширение для всех зарегистрированных типов».

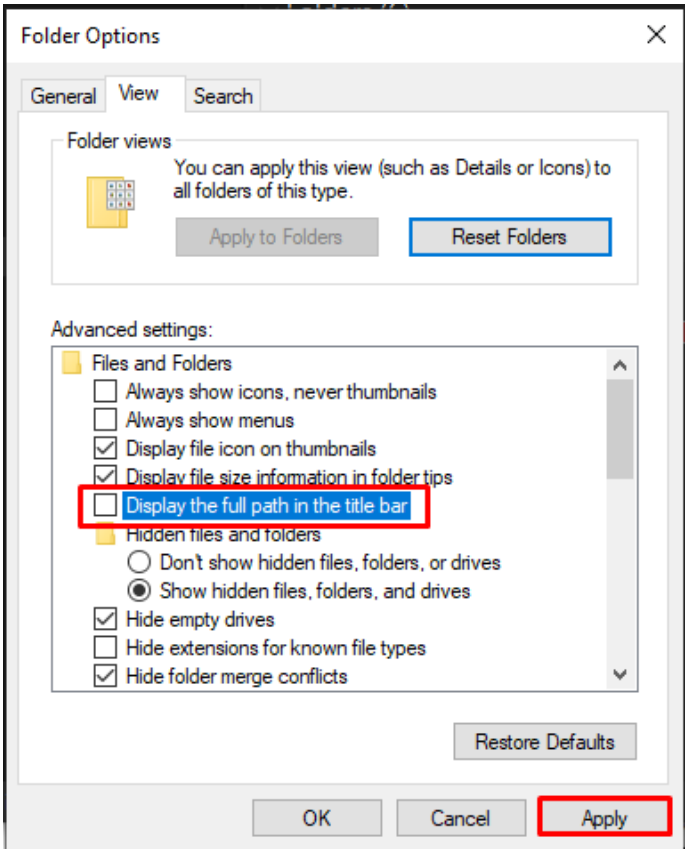

Рисунок 6 Меню «Вид»

Находим зловред. Изменяем его расширение с «.doc» на «.rtf». Благодаря формату «rtf» можно сохранить всю необходимую информацию, при этом надстройка VBA будет очищена от вредоносного кода.

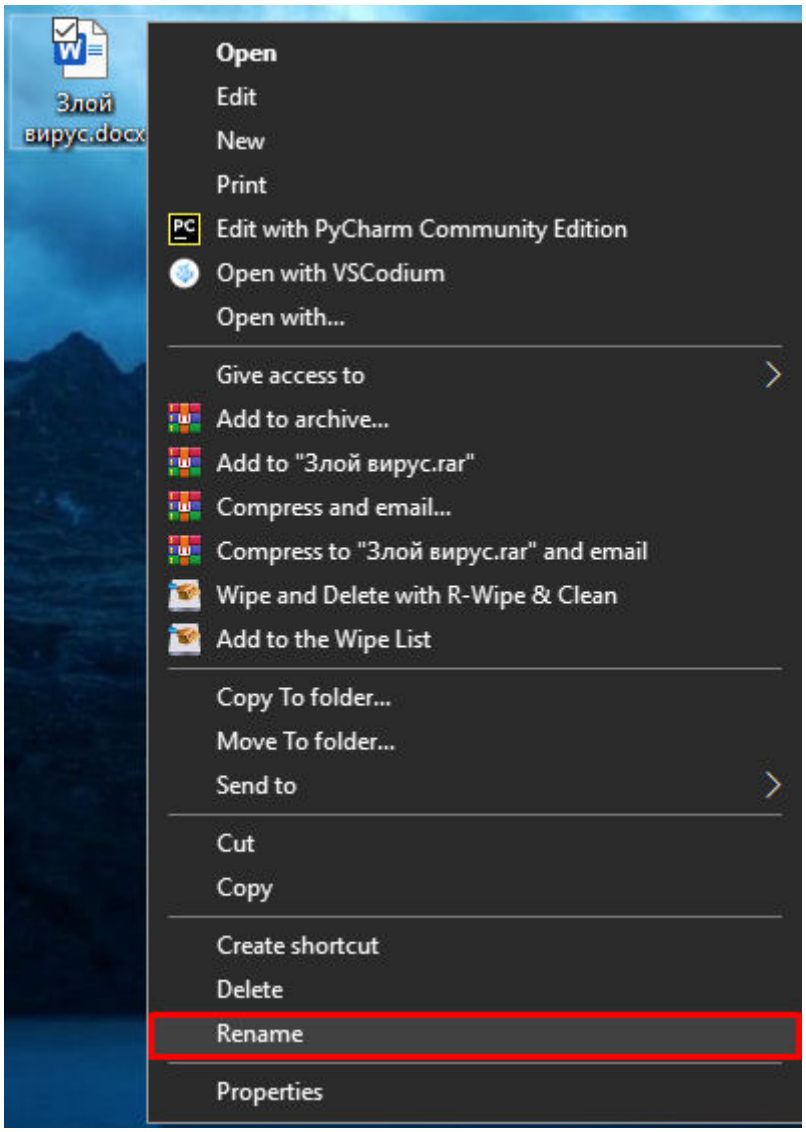

Рисунок 7 Кнопка «Переименовать»

Далее вы увидите сообщение системы о смене имени. Нажимаем «Да».

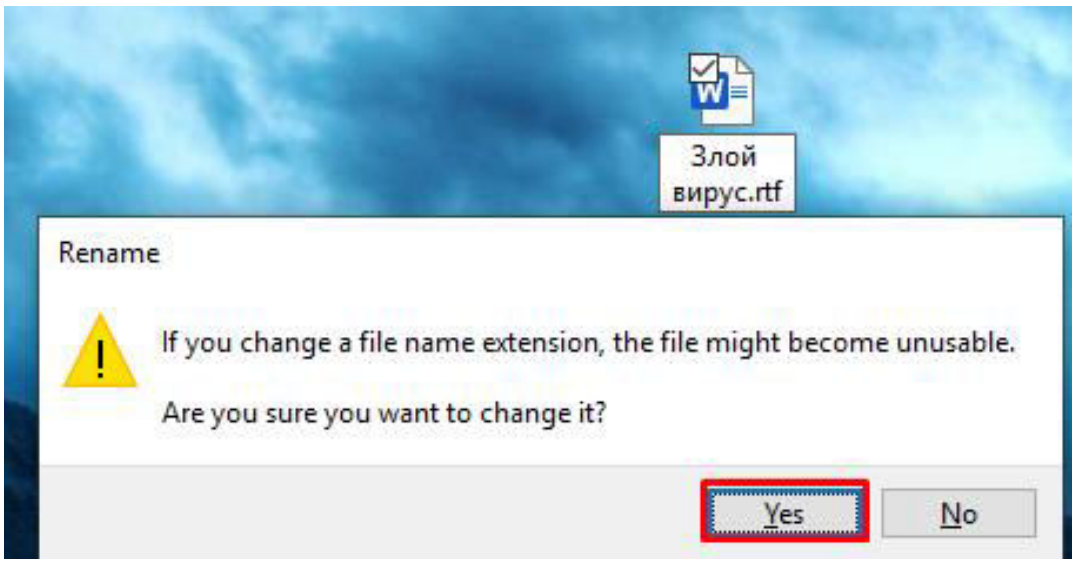

Рисунок 8 Согласие на изменения расширения файла

Изменяем расширение документа обратно. Восстанавливаем первоначальные параметры.

Таким образом, вы удалите макровирус с зараженного документа, однако это ни в коем случае не значит, что он не остался в системе. Именно поэтому рекомендую при первой возможности просканировать ПК антивирусом.

3. Как происходит заражение компьютера макровирусом?

Макровирусы заражают файлы документов Word и электронных таблиц Excel. Макровирусы являются фактически макрокомандами (макросами), которые встраиваются в документ.

После загрузки зараженного документа в приложение макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы.

4. Что такое макрос?

Макрос - набор инструкций, которые сообщают программе (такой как Word или Excel), какие действия следует выполнить, чтобы достичь определенной цели.