СОГБПОУ<Верхнеднепровский Технологический Техникум>

Компьютерные вирусы

ВЫПОЛНИЛ: УЧАЩИЙСЯ ГРУППЫ 27-С
КОЗЫРЕВ Э.Р.

2016г

Компьютерный вирус

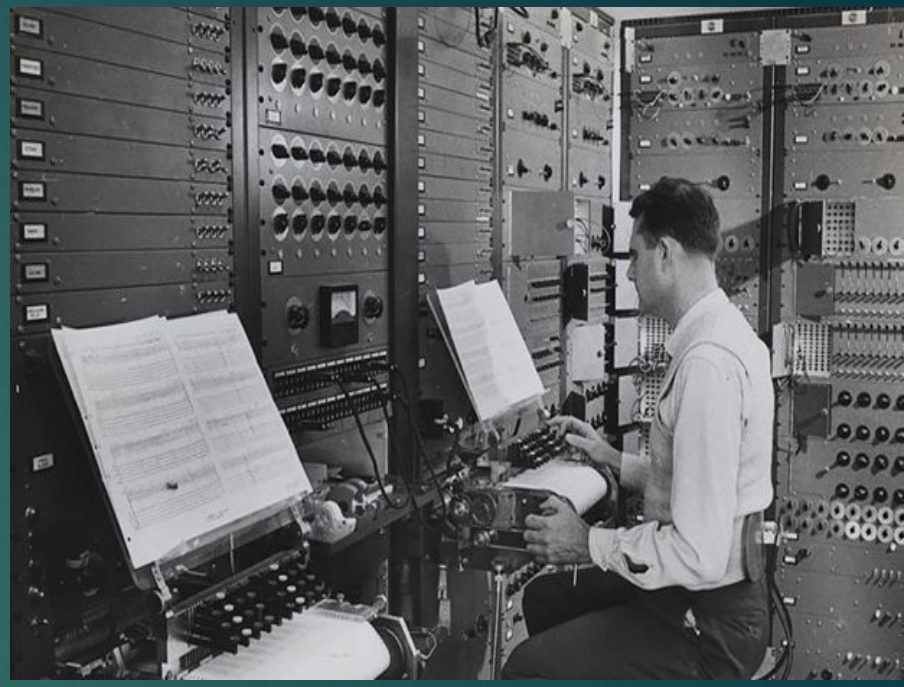
вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи

Как правило, целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы

В обиходе «вирусами» называют всё вредоносное ПО, хотя на самом деле это лишь один его вид.

История

- Основы теории самовоспроизводящихся механизмов заложил американец Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ



Первыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году. Зимой 1984 года появились первые антивирусные утилиты — CHK4BOMB и BOMBSQAD авторства Энди Хопкинса (англ. Andy Hopkins). В начале 1985 года Ги Вонг (англ. Gee Wong) написал программу DPROTECT — первый резидентный антивирус

История названия

Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения. По-видимому, впервые слово «вирус» по отношению к программе было употреблено Грегори Бенфордом (Gregory Benford) в фантастическом рассказе «Человек в шрамах», опубликованном в журнале Venture в мае 1970 года

Термин «компьютерный вирус» впоследствии не раз «открывался» и переоткрывался. Так, переменная в подпрограмме PERVADE (1975), от значения которой зависело, будет ли программа ANIMAL распространяться по диску, называлась VIRUS. Также, вирусом назвал свои программы Джо Деллинджер и, вероятно, это и было то, что впервые было правильно обозначено как вирус

Классификация вирусов по способу маскировки

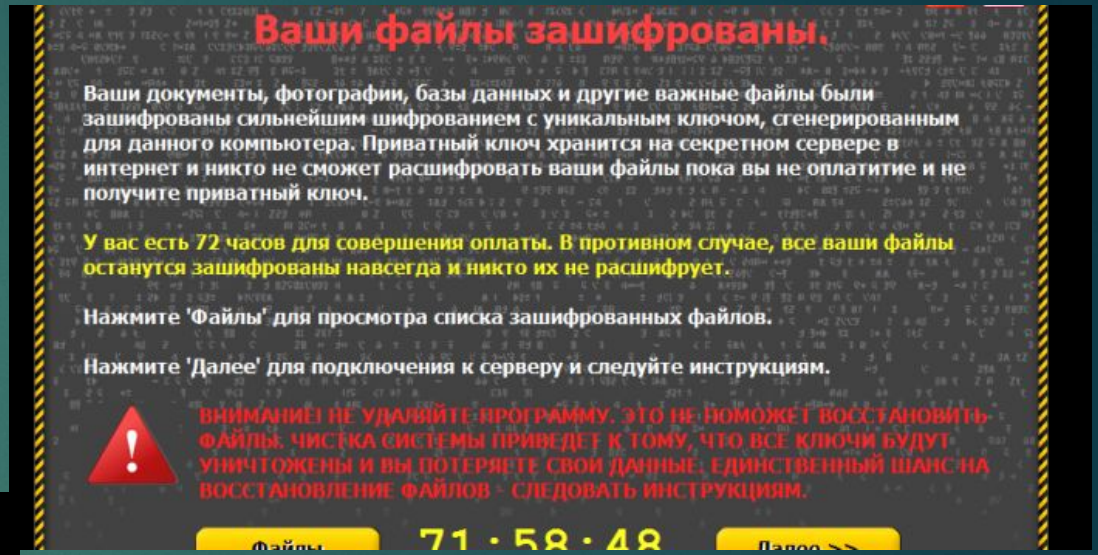
При создании копий для маскировки могут применяться следующие технологии:

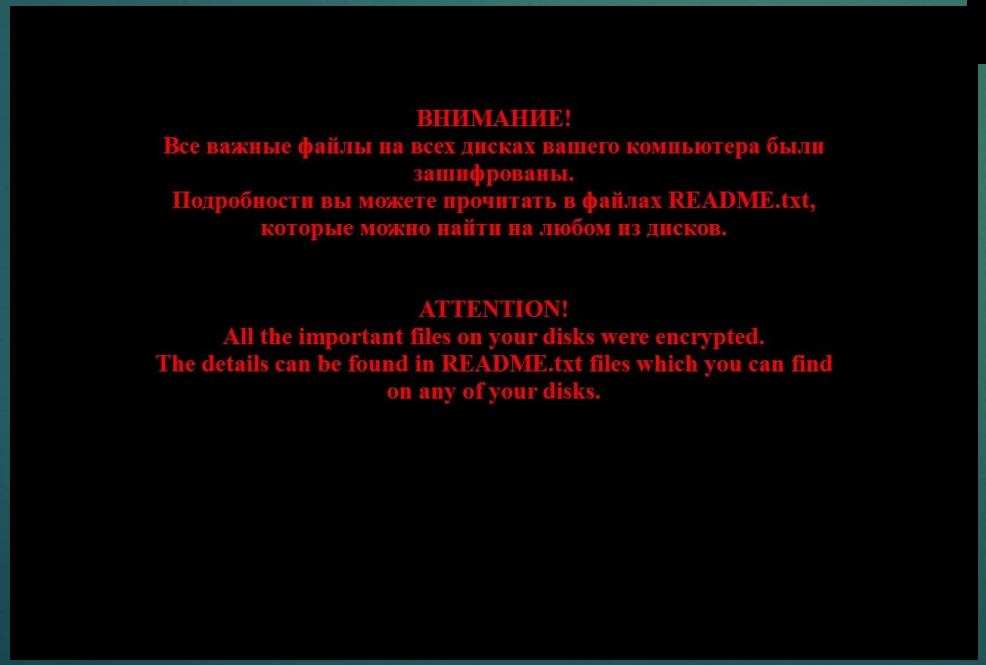
Шифрование — вирус состоит из двух функциональных кусков: собственно вирус и шифратор. Каждая копия вируса состоит из шифратора, случайного ключа и собственно вируса, зашифрованного этим ключом

Метаморфизм — создание различных копий вируса путем замены блоков команд на эквивалентные, перестановки местами кусков кода, вставки между значащими кусками кода «мусорных» команд, которые практически ничего не делают

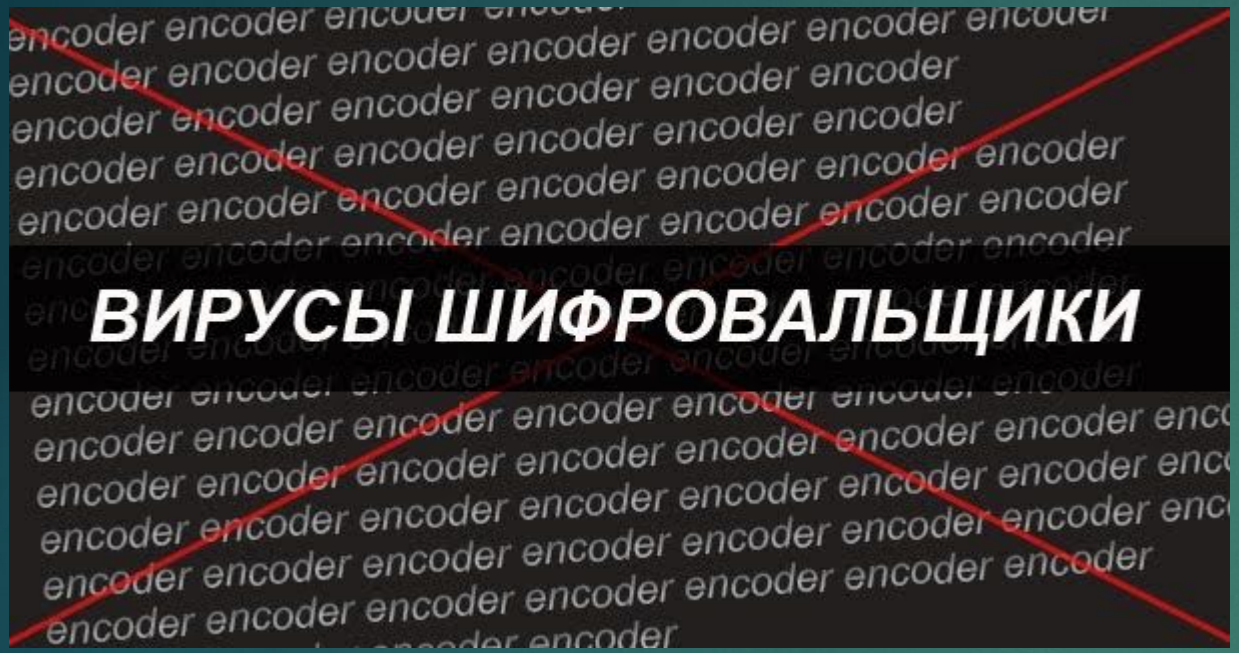
Шифрованный вирус

- Это вирус, использующий простое шифрование со случайным ключом и неизменный шифратор. Такие вирусы легко обнаруживаются по сигнатуре шифратора





Вирус-шифровальщик

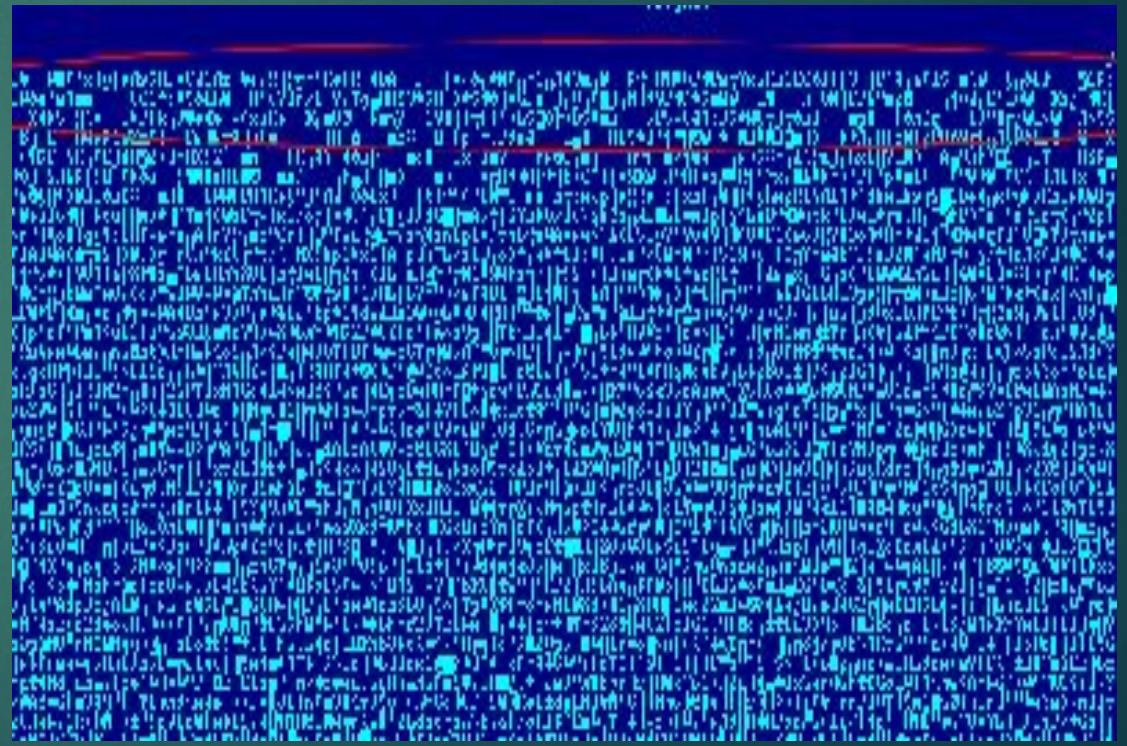


- В большинстве случаев вирус-шифровальщик приходит по электронной почте в виде вложения от незнакомого пользователю человека, а возможно, и от имени известного банка или действующей крупной организации. Письма приходят с заголовком вида: «Акт сверки…», «Ваша задолженность перед банком…», «Проверка регистрационных данных», «Резюме», «Блокировка расчетного счета» и прочее

В письме содержится вложение с документами, якобы подтверждающими факт, указанный в заголовке или теле письма. При открытии этого вложения происходит моментальный запуск вируса-шифровальщика, который незаметно и мгновенно зашифрует все документы. Пользователь обнаружит заражение, увидев, что все файлы, имевшие до этого знакомые значки, станут отображаться иконками неизвестного типа. За расшифровку преступником будут затребованы деньги. Но, зачастую, даже заплатив злоумышленнику, шансы восстановить данные ничтожно малы

Полиморфный вирус

- Вирус, использующий метаморфный шифратор для шифрования основного тела вируса со случайным ключом. При этом часть информации, используемой для получения новых копий шифратора также может быть зашифрована. Например, вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм



Классификация вирусов по среде обитания

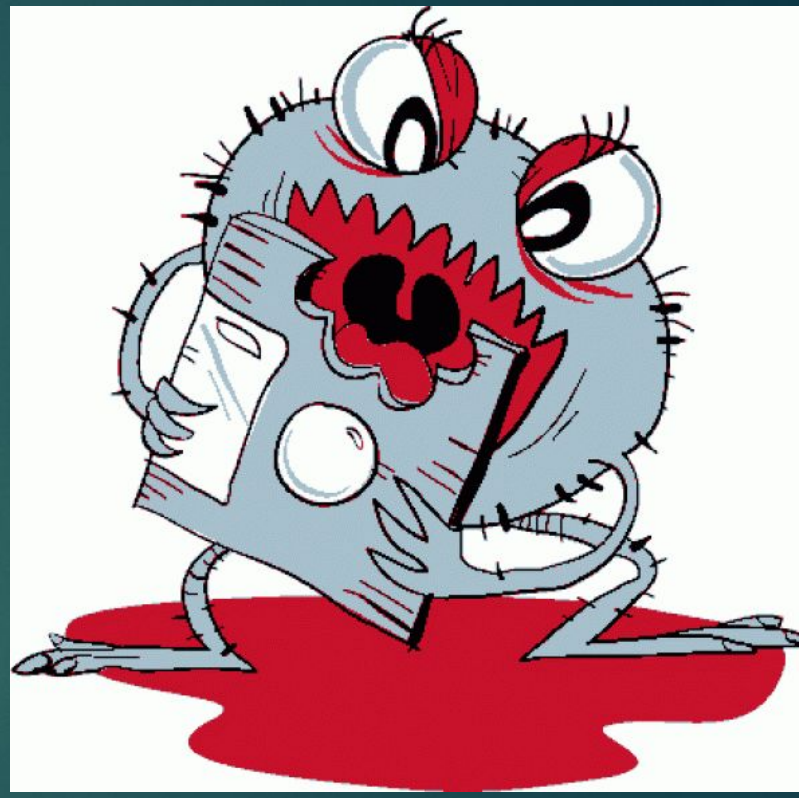
- Под «средой обитания» понимаются системные области компьютера, операционные системы или приложения, в компоненты (файлы) которых внедряется код вируса. По среде обитания вирусы можно разделить на:
- загрузочные;
- файловые
- макро-вирусы;
- скрипт-вирусы.

Файловые вирусы

Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС. Они:

- различными способами внедряются в исполняемые файлы (наиболее распространенный тип вирусов);
- создают файлы-двойники (компаньон-вирусы);
- создают свои копии в различных каталогах;
- используют особенности организации файловой системы (link-вирусы).

Все, что подключено к Интернету – нуждается в антивирусной защите: 82% обнаруженных вирусов «прятались» в файлах с расширением PHP, HTML и EXE.

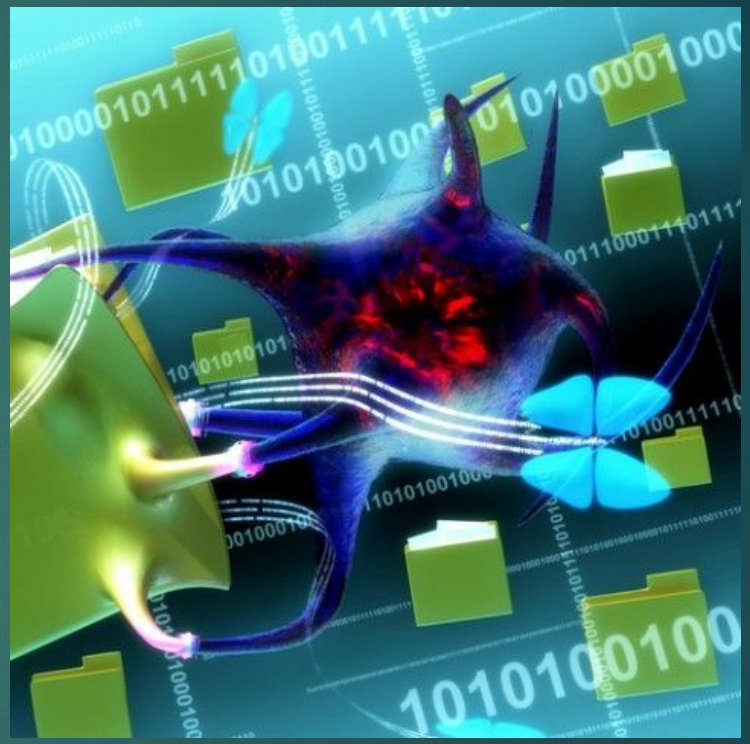


Загрузочные вирусы

- Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор. Данный тип вирусов был достаточно распространён в 1990-х, но практически исчез с переходом на 32-битные операционные системы и отказом от использования дискет как основного способа обмена информацией. Теоретически возможно появление загрузочных вирусов, заражающих CD-диски и USB-флешек, но на текущий момент такие вирусы не обнаружены

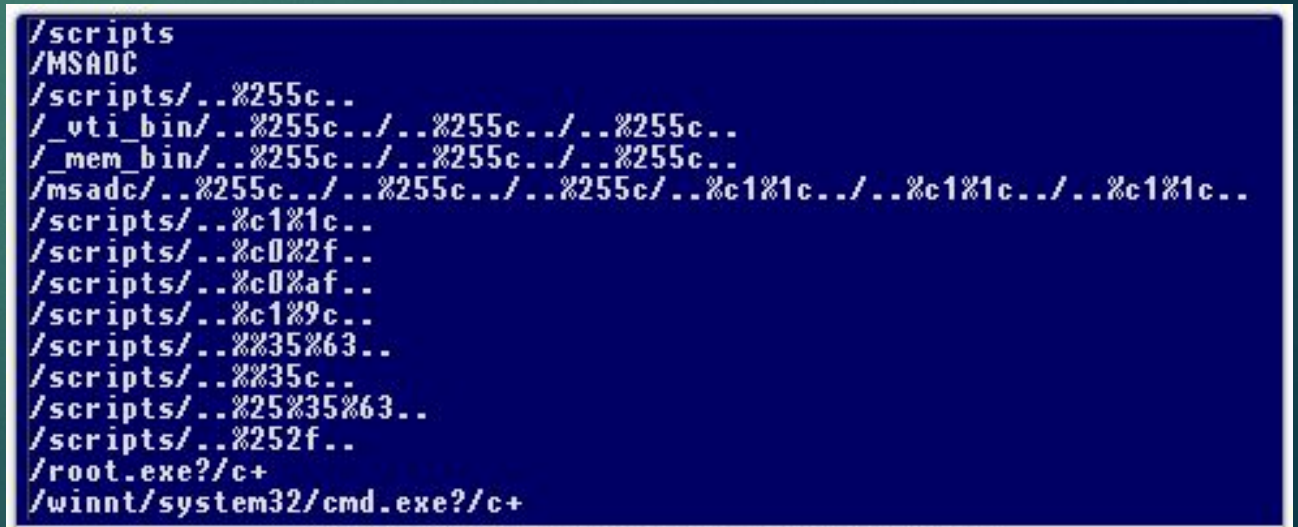
Макро-вирусы

Многие табличные и графические редакторы, системы проектирования, текстовые процессоры имеют свои макро-языки для автоматизации выполнения повторяющихся действий. Эти макро-языки часто имеют сложную структуру и развитый набор команд. Макро-вирусы являются программами на макро-языках, встроенных в такие системы обработки данных. Для своего размножения вирусы этого класса используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие



Скрипт-вирусы

Скрипт-вирусы, также как и макро-вирусы, являются подгруппой файловых вирусов. Данные вирусы, написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т.д.). Они либо заражают другие скрипт-программы (командные и служебные файлы MS Windows или Linux), либо являются частями многокомпонентных вирусов. Также, данные вирусы могут заражать файлы других форматов (например, HTML), если в них возможно выполнение скриптов



Directory traversal exploit strings in W32/Nimda-A

Заключение

Пожалуй, самым страшным кошмаром любого пользователя сети Интернет являются компьютерные вирусы, которые постоянно совершенствуются. Вирусы попадают на компьютеры часто, причем иногда не сразу понятно, что же произошло с системой. Хочется сразу заметить, что слишком уж бояться вирусов не стоит, особенно если компьютер приобретен совсем недавно, и много информации на жестком диске еще не накопилось. Вирус компьютер не взорвет. Ныне известен только один вирус (Win95.CIH), который способен испортить "железо" компьютера. Другие же могут лишь уничтожить информацию, не более того