Компьютерные вирусы
и
Антивирусные программы

МБУДО ЦТО и ДТТ г. Белгорода
преподаватель профессии Оператор
электронно-вычислительных и
вычислительных машин
Гусарова Т.Ю.

Компьютерные вирусы

Признаки

Разделение

Антивирусные программы

Типы

Что такое вирус?

Компьютерный вирус – это специально написанная компьютерная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии, внедрять их в файлы с целью порчи файлов и каталогов, создания помех в работе

Признаки проявления вирусов:

- Неправильная работа нормально работающих программ
- Медленная работа ПК
- Частые зависания и сбои в работе ПК
- Изменение размеров файлов
- Исчезновение файлов и каталогов
- Неожиданное увеличение количество файлов на диске
- Уменьшение размеров свободной оперативной памяти
- Вывод на экран неожиданных сообщений и изображений
- Подача непредусмотренных звуковых сигналов
- Невозможность загрузки ОС

Вирусы подразделяются на классы по следующим признакам:

- По среде обитания
- По способу заражения
- По степени воздействия

А также на:

- Троянские
- Вирусы-черви
- Паразитические
- Вирусы-невидимки или стелсы

По среде обитания:

Файловые

Файловые вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы.

Макровирусы

Макровирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

Загрузочные

Загрузочные вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на boot-сектор.

Сетевые

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

По способу заражения:

- резидентные (загружаемые в память ПК)
- нерезидентные (не заряжающие память ПК, остаются активными ограниченное время)

По степени воздействия:

- безвредные
- неопасные
- опасные
- очень опасные

Троянские

- самые опасные
- маскируются под полезную программу
- разрушают загрузочный сектор
- файловую систему дисков

Невидимки или стелсы:

- перехватывают обращения операционной системы к пораженным файлам и подставляют вместо своего тела незараженные участки

Черви

- распространяются по сети
- вычисляют адреса сетевых компьютеров и высылают по ним свои копии

Паразитические:

- изменяют содержимое файлов и секторов диска
- легко находятся и лечатся

Антивирусная программа

Антивирусная программа- это программа, позволяющая обнаруживать и удалять вирусы

Типы антивирусных программ:

- Программы – фильтры или «сторожа»
- Программы – ревизоры
- Фаги или программы – доктора или программы – вакцины
- Программы – детекторы

Программы – детекторы:

- только обнаруживают
- редки

Фаги или программы – доктора или программы – вакцины:

- обнаруживают и лечат
- Aidstes – Лозинский Д.
- Norton AntiVirus и Doctor Wed - Данилов И.

Программы – ревизоры:

- самые надежные
- запоминает исходное состояние программ тогда, когда ПК не заражен вирусом, затем периодически сравнивает текущее состояние с исходным и если обнаружены изменения, то на экране появляется надпись
- небольшие
- контролирует операции ПК, после обнаружения подозрительных действий при работе ПК, характерных для вируса подает сообщение и пользователь сам решает выполнять или нет действие
- обнаруживает на ранней стадии
- лечит

Интересно

- В 2004 году школьник из Германии написал и запустил вирус Sasser. Он заблокировал спутниковую связь французских новостных агентств и отменил несколько рейсов компании Delta. Этот роскошный подарок милый ребенок преподнес себе на 18-летие.
- Первый в истории интернет-червь появился в 1988 году. Червь Morris заразил тысячи компьютеров и практически остановил работу интернета на целый день.
- Самый разрекламированный вирус – это, безусловно, CIH («Чих», или «Чернобыль»). Он пришел из Тайваня в июне 1998-го. «Чернобыль» заражал файлы и размножался через оперативную память. Он мог перезаписать микросхемы BIOS и вывести компьютеры из строя.
- Самым заманчивым является червь Sober версии V. Суля бесплатные билеты на мировой футбольный кубок 2006 года в Германии, ему удалось достигнуть значительного уровня заражений. К счастью, пользователи стали осторожнее, и создателю не удалось начать новую эпидемию.
- Самые конъюнктурные вирусы – это «Анна Курникова» и «Бен Ладен». Они появились на волнах популярности соответствующих персонажей, наделали много шуму, но не были такими уж страшно опасными.

- Титул самого грубого без сомнения получает Cisum.A. Этот червь, отключая антивирусные защитные системы на зараженных компьютерах, оставляет пользователю сообщение: «Ты идиот». Оно не только появляется в небольшом окне на экране, но также раздается из колонок компьютера каждые пять секунд.
- Самый бесчувственный – это червь Zar.A. Он использовал тему пожертвований пострадавшим в результате Азиатского цунами, чтобы заставить пользователей открыть файл, содержащего вредоносный код.
- Самый быстро распространяющийся вирус – это знаменитая «Мелисса». 26 марта 1999 года им заразились 100 тысяч компьютеров по всему миру, что составляло на тот момент 20% деловых компьютеров в мире. Melissa распространялся по электронной почте настолько быстро, что многие крупные корпорации, включая Intel и Microsoft, были вынуждены заблокировать внутреннюю почту.
- Самый знаменитый вирус – это, конечно, ILOVEYOU (Loveletter и The Love Bug) 3 мая 2000 года вирус обнаружился в Гонконге. Он распространялся по почте с темой письма «Я тебя люблю» и вложением файла с «двойным» расширением .txt.vbs. Найденные в компьютере логины и пароли аккуратный вирус высылал своему создателю.
- Самый опасный вирус – Whiter.F, «благородный» код, удаляющий все содержимое жёсткого диска. Любопытный аспект этого кода в том, что перед удалением он заменяет все файлы пользователя на текстовые со следующим сообщением: You did a piracy, you deserve it (ты занимался пиратством и заслужил это).
- Самый милый компьютерный вирус был даже не совсем вирусом, а просто милой игрушкой, мотающей нервы владельцу компьютера. Вирус требовал: «Дай чучу!» – и отключал компьютер, пока пользователь не набирал эту «чучу» на клавиатуре.

СПАСИБО ЗА ВНИМАНИЕ