Департамент образования и науки города Москвы

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ОБРАЗОВАТЕЛЬНЫЙ КОМПЛЕКС

по специальности 10.02.01 организация и технология защиты информации

ПРОВЕСТИ АНАЛИЗ КОМПЬЮТЕРНЫХ ВИРУСОВ, МЕТОДОВ ОБНАРУЖЕНИЯ, УДАЛЕНИЯ СПОСОБОВ ПРОФИЛАКТИКИ КОМПЬЮТЕРНЫХ ВИРУСОВ.

Студент группы ОТИ-416: Иванов К.
А.

ПРОВЕСТИ АНАЛИЗ КОМПЬЮТЕРНЫХ ВИРУСОВ, МЕТОДОВ ОБНАРУЖЕНИЯ, УДАЛЕНИЯ СПОСОБОВ ПРОФИЛАКТИКИ КОМПЬЮТЕРНЫХ ВИРУСОВ.

Компьютерный вирус – это специально написанная программа, обязательным свойством которого является возможность создавать свои дубликаты и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты.

КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Файловые вирусы

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

Загрузочные вирусы

Записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор

Макро-вирусы

Заражают файлы-документы и электронные таблицы нескольких популярных редакторов

Сетевые вирусы

Используют для своего распространения протоколы или команды компьютерных сетей и электронной почты

ОСОБЕННОСТИ АЛГОРИТМА РАБОТЫ ВИРУСОВ

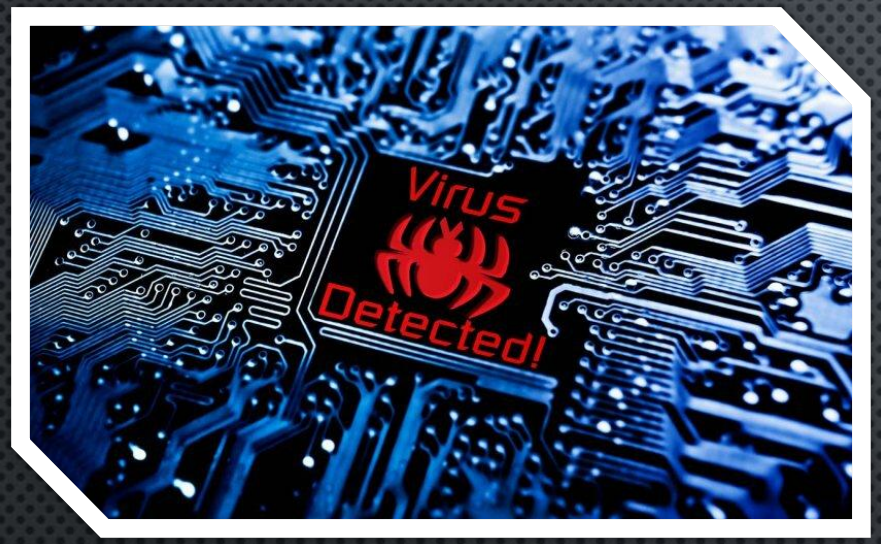
Резидентность

Резидентный вирус при проникновении в компьютер оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы.

Использование стелс-алгоритмов

Использование *стелс – алгоритмов* позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов.

ОСОБЕННОСТИ АЛГОРИТМА РАБОТЫ ВИРУСОВ



Самошифрование и полиморфичность

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик-вирусы – это достаточно трудно обнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода

Использование нестандартных приемов

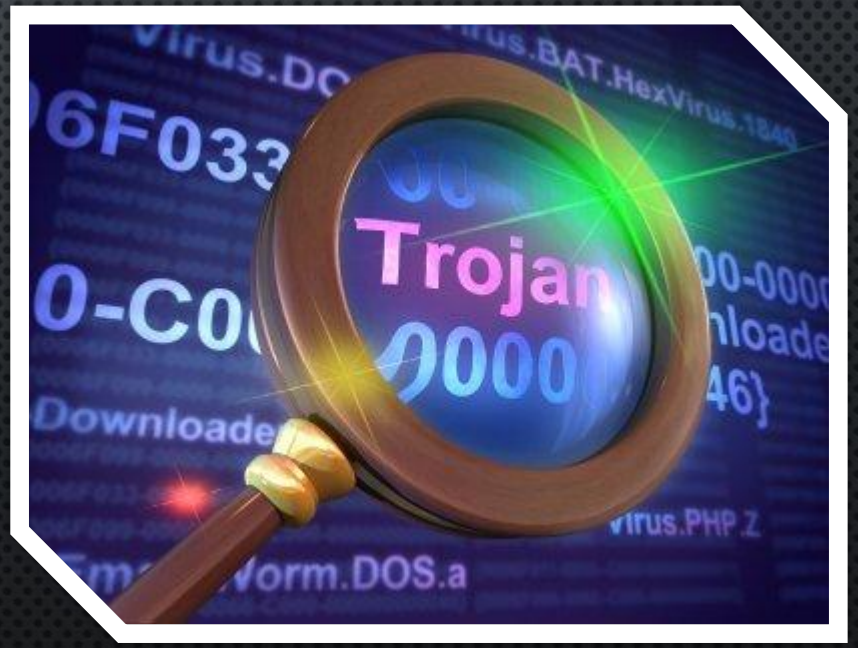
Различные нестандартные приемы часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре ОС, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса и т.д.

МЕТОДЫ ОБНАРУЖЕНИЯ И УДАЛЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Антивирусы-фильтры – это резидентные программы, которые оповещают пользователя о всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его, а также о других подозрительных действиях. При этом выводится запрос о разрешении или запрещении данного действия. Принцип работы этих программ основан на перехвате соответствующих векторов прерываний

МЕТОДЫ ОБНАРУЖЕНИЯ И УДАЛЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Программы-детекторы – программы, объединяющие в себе детектор и доктор. Наиболее известные представители этого класса - Aidstest, Doctor Web, Microsoft AntiVims, антивирус Касперского и др. Антивирусы-детекторы рассчитаны на конкретные вирусы и основаны на сравнении последовательности кодов содержащихся в теле вируса с кодами проверяемых программ. Такие программы нужно регулярно обновлять, так как они быстро устаревают и не могут обнаруживать новые виды вирусов.



МЕТОДЫ ОБНАРУЖЕНИЯ И УДАЛЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Антивирусы – вакцинаторы – записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной.