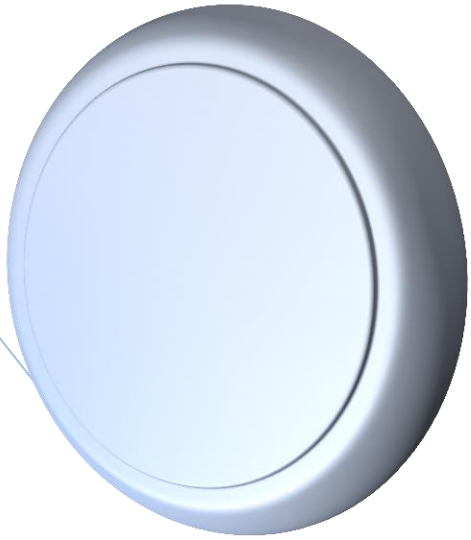


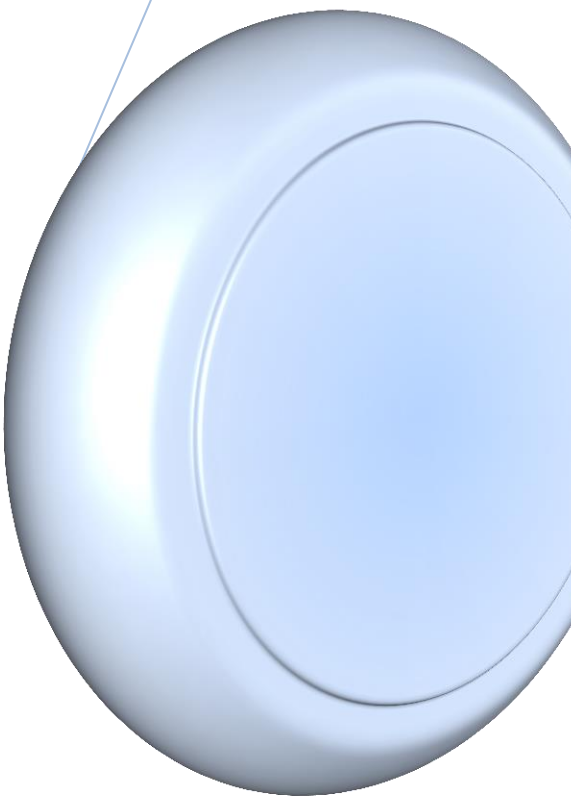
Глоссарий

Вирусы и антивирусные программы

Выполнил студент ВГСПУ факультета МИФ
группы МИБ-122

Горбунов Алексей

05.07.2013



Анти—антивирусный вирус (Anti-antivirus Virus, Retrovirus) — компьютерная вирусная программа, объектом нападения которой являются антивирусные программы.

Антивирусный вирус (Anti-virus Virus) — компьютерная вирусная программа, объектом нападения которой являются другие компьютерные вирусы.

Антивирусная программа (Anti-virus program) — программа поиска, диагностики, профилактики и лечения файлов, зараженных компьютерным вирусом. В процессе поиска и диагностики определяются зараженные файлы и тип вируса. Профилактика позволяет предотвращать заражение. Лечение подразумевает удаление вируса и восстановление поврежденных файлов.

Антивирусный сканер (Anti-virus scanner) — программа, способная обнаруживать программный код вирусов (сигнатуру) в зараженных ими файлах при помощи базы данных о вирусах, известных такой антивирусной программе или исходя из априорных предпосылок об устройстве такого кода. Сканеры периодически, например, по запросу пользователя, проверяют определенные объекты (диски, каталоги или файлы, а также оперативную память и загрузочные секторы) на наличие программного кода.

Апплет (Applet) — Класс языка Java, встроенный в виде исполняемого модуля в документ, созданный на языке HTML. Апплет загружается с сервера на компьютер пользователя как прикрепленный файл. Апплеты применяют, например, при организации на Web-страницах интерактивного диалога с пользователем.

Архивный файл (Archive file) — файл, являющийся результатом сжатия архиватора.

BIOS-кит (BIOS-kit) — вредоносная программа, способная заражать BIOS компьютера7

Ботнет (Botnet) — сеть компьютеров, зараженных троянцами-ботами. Ботнет используется для рассылки спама или проведения сетевых атак, например подбора паролей или DoS-атак.

Буткиты (Boot viruses) — вредоносные программы, которые заражают загрузочные записи (Boot record) дискет, разделов жестких дисков, а также модифицируют главный загрузочный сектор MBR (Master Boot Record)

Вирус (Virus) — программа, инфицирующая файловые объекты и способная к самовоспроизведению.

Вирусная программа-червь (Worm-virus) — паразитическая программа, обладающая механизмом саморазмножения, но не заражающая другие исполняемые файлы. Проникая в систему, распространяет свои копии на другие компьютеры, объединенные в ту же сеть, что и инфицированный ПК.

Демон (Daemon) — программа, используемая для выполнения служебной функции без запроса со стороны пользователя и даже без его ведома.

DNS-заражение (DNS poisoning) — атака на кеш DNS-сервера. В результате в кеше появляется ложная запись о соответствии DNS-имени хоста, которому жертва доверяет, и IP-адреса, указанного атакующим. Является подвидом спуфинга. Атака может поражать как клиентский хост, так и хост сервера, что может привести к массовому перенаправлению пользователей на ложный адрес.

Дозвонщики (Dialers) — программы, используемые злоумышленниками для накручивания оплаты за телефон жертве или для незаметного подключения пользователя через модем к дорогостоящим платным телефонным службам.

DoS-атаки (DoS-attacks) — популярный среди злоумышленников вид сетевых атак, граничащий с терроризмом. Заключается в отправке запросов с компьютеров на атакуемый сервер с целью выведения его из строя. При достижении определенного количества запросов (ограниченного аппаратными возможностями сервера) сервер перестает справляться с нагрузкой, что приводит к отказу в обслуживании. Данной атаке часто предшествует спуфинг. DoS-атаки стали широко используемым средством запугивания и шантажа конкурентов.

"Дроппер" (Dropper) — файл-носитель, устанавливающий вирус в систему. Техника иногда используемая вирусописателями для "прикрытия" вирусов от антивирусных программ.

Ключ реестра (Registry key) — запись в реестре, уникальный идентификатор, присваиваемый определенной части информации, хранящейся в реестре.

Компьютерные вирусы (Computer viruses) — это программы или фрагменты программного кода, которые, попав на компьютер, могут вопреки воле пользователя выполнять различные операции на этом компьютере — создавать или удалять объекты, модифицировать файлы данных или программные файлы, осуществлять действия по собственному распространению по локальным вычислительным сетям или по сети Интернет. Модификация программных файлов, файлов данных или загрузочных секторов дисков таким образом, что последние сами становятся носителями вирусного кода и в свою очередь могут осуществлять вышеперечисленные операции, называется заражением (инфицированием) и является важнейшей функцией компьютерных вирусов. В зависимости от типов заражаемых объектов выделяются различные типы вирусов.

Макрокомандные вирусы (Macroviruses) — вредоносные программы, которые заражают файлы, созданные приложениями Microsoft Office и другими программами, допускающими наличие макрокоманд

Ревизор (Revisor) — программа, периодически проверяющая изменения в потенциально заражаемых файлах, сверяя части системы с эталонными. Ревизор сначала сохраняет контрольные суммы контролируемых файлов и секторов, а в последствии проверяет соответствие эталонных и текущих значений контрольных сумм. Срабатывает в момент несовпадения (в следствие проникновения вируса). Позволяет выявить вирусную активность после заражения и в ряде случаев восстановить состояние файлов до заражения. Ревизор не в состоянии определить, в результате чего изменилась программа — ее поразил вирус или просто перетранслировали.

Реестр (Registry) — иерархическая база данных, в которой операционная система централизованным образом хранит всю системную информацию, в частности, конфигурацию вычислительной системы, значения различных параметров, сведения об установленных программах и т.д. Изменения в реестре производятся пользователем в окне редактирования реестра.

Системный файл (System file) — файл, содержащий один из модулей операционной системы или набор данных, которые она использует.

Скрипт, сценарий (Script) — программа, особый вид программного кода, как правило, написанная на интерпретируемом (не компилируемом) языке и содержащая команды-инструкции.

Скрипт—вирусы (Script virus) — вирусы, написанные на языках Visual Basic, Java Script, Jscript и других. Программы на языках Visual Basic и Java Script могут располагаться как в отдельных файлах, так и встраиваться в HTML-документ и в таком виде интерпретироваться браузером с удаленного сервера или локального диска.

Скрытый файл (Hidden file) — файл, имя которого согласно политике безопасности не отражается в списке файлов каталога. Для этого он снабжается специальным знаком.

Спуфинг (Spoofing) — сетевая атака, заключающаяся в получении доступа в сеть обманным путем посредством имитации соединения. Используется для обхода систем управления доступом на основе IP-адресов, а также для маскировки ложных сайтов под их легальных двойников или просто под законные бизнес-проекты. Блокируется брандмауэром.

Стелс вирусы (Stealth virus) — вирусные программы, предпринимающие специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в зараженных объектах.

Так называемая стелс-технология может включать в себя:

- затруднение обнаружения вируса в оперативной памяти
- затруднение трассировки и дезассемблирования вируса
- маскировку процесса заражения
- затруднение обнаружения вируса в зараженной программе и загрузочном секторе.

Троянцы (Trojans) — вредоносные программы, осуществляющие несанкционированные пользователем действия на его компьютере. Эти действия необязательно будут разрушительными, но они всегда направлены во вред пользователю.

Название этого типа атак происходит от известной легенды о деревянной статуе коня, использованной греками для проникновения в Трою.

Примеры: Trojan.Botnetlog, Trojan.DownLoad, Trojan.Stuxnet.

Файловые вирусы (File viruses) — вирусы, заражающие двоичные файлы (в основном исполняемые файлы и динамические библиотеки). Такие вирусы внедряются в файлы операционной системы, активируются при запуске пораженной программы и затем распространяются