# Компьютерные вирусы

**Компьютерный вирус** - это вредоносная программа, написанная специально для получения доступа к компьютеру без разрешения его владельца. Такие программы в основном пишутся для кражи или уничтожения компьютерных данных. Большинство систем заражаются вирусами из-за ошибок в программах, уязвимости операционных систем и плохой защиты. По данным AV-Test, независимой организации, занимающейся анализом и оценкой антивирусного и защитного программного обеспечения, каждый день обнаруживается около 560 000 новых вредоносных программ. Существуют различные типы компьютерных вирусов, которые можно разделить на категории в зависимости от их происхождения, возможностей распространения, места хранения, файлов, которые они заражают, и разрушительной природы. Давайте углубимся и посмотрим, как эти вирусы работают на самом деле.

# Когда был создан самый первый компьютерный вирус?

Первый в истории компьютерный вирус (под названием Creeper) был написан Бобом Томасом из компании BBN Technologies в 1971 году. Creeper был экспериментальной самовоспроизводящейся программой, которая не имела никакого злого умысла. Она лишь отображала простое сообщение: "Я - Крипер. Поймай меня, если сможешь!".

# Кто создал первый вирус для ПК?

В 1986 году Амджад Фарук Алви и Басит Фарук Алви написали вирус для загрузочного сектора под названием "Brain", чтобы предотвратить несанкционированное копирование созданного ими программного обеспечения. 'Brain' считается первым компьютерным вирусом для IBM PC и совместимых компьютеров. Первым вирусом, специально нацеленным на Microsoft Windows, был WinVir. Он был обнаружен в 1992 году. Вирус не содержал никаких вызовов Windows API. Вместо этого он использовал API DOS.

# Какая самая дорогая кибератака всех времен?

Самой разрушительной вредоносной программой на сегодняшний день является MyDoom. Впервые обнаруженный в январе 2004 года, он стал самым быстро распространяющимся почтовым червем в истории. Он создавал сетевые дыры, через которые злоумышленники получали доступ к зараженным машинам.

В 2004 году почти четвертая часть всех электронных писем была заражена MyDoom. Ущерб от этого вируса составил более 38 миллиардов.

# Вирус загрузочного сектора

**Примеры:** Form, Disk Killer, Stone virus, Polyboot.B
**Может поражать:** Любой файл после попадания в основную память

Вирус Boot Sector заражает главную загрузочную запись (MBR) устройства хранения данных. Любой носитель, независимо от того, является он загрузочным или нет, может вызвать этот вирус. Эти вирусы внедряют свой код в таблицу разделов жесткого диска. После перезагрузки компьютера он попадает в основную память.

# Вирус загрузочного сектора

Среди распространенных проблем, которые могут возникнуть после заражения, - проблемы с загрузкой, нестабильная работа системы и невозможность найти жесткий диск. Поскольку вирус загрузочного сектора может шифровать загрузочный сектор, его может быть трудно удалить. В большинстве случаев пользователи даже не подозревают о заражении вирусом, пока не просканируют систему с помощью антивирусной программы. Однако этот тип вируса стал редким после сокращения использования дискет. Современные операционные системы поставляются со встроенной защитой загрузочного сектора, которая затрудняет поиск MBR.

# Вирус загрузочного сектора

**Защита**: Убедитесь, что используемый диск защищен от записи. Не запускайте и не перезагружайте компьютер с подключенными неизвестными внешними дисками.

# Вирус прямого действия

**Пример:** VCL.428, создан Лабораторией по конструированию вирусов.
**Может воздействовать на:** Все файлы с расширением .exe и .com

Вирус прямого действия быстро проникает в оперативную память, заражает все программы/файлы/папки, определенные в пути Autoexec.bat, а затем удаляет себя. Он также может уничтожить данные, находящиеся на жестком диске или USB, подключенном к компьютеру.

# Вирус прямого действия

Обычно они распространяются при выполнении файла, в котором они содержатся. Пока вы не запустите или не откроете файл, он не распространится на другие части вашего устройства или сети.

Хотя эти вирусы находятся в корневом каталоге жесткого диска, они способны менять местоположение при каждом выполнении. Во многих случаях они не удаляют системные файлы, но снижают общую производительность системы.

# Вирус прямого действия

**Защита:** Используйте антивирусный сканер. Вирус прямого действия легко обнаружить, а все зараженные файлы можно полностью восстановить.

# Вирус перезаписи

**Примеры:** Grog.377, Grog.202/456, Way, Loveletter.
**Может поражать:** Любой файл

Вирусы перезаписи очень опасны. Они поражают широкий спектр операционных систем, включая Windows, DOS, Macintosh и Linux. Они просто удаляют данные (частично или полностью) и заменяют оригинальный код своим собственным.

# Вирус перезаписи

Они заменяют содержимое файла, не изменяя его размер. И как только файл заражен, его невозможно восстановить, и в итоге вы потеряете все данные. Более того, вирусы этого типа могут не только сделать приложения неработоспособными, но и зашифровать и украсть ваши данные при выполнении. Несмотря на свою эффективность, злоумышленники больше не используют вирусы перезаписи.
Они предпочитают заманивать пользователей настоящими троянскими конями и распространять вредоносный код по электронной почте.

# Вирус перезаписи

**Защита:** Единственный способ избавиться от этого вируса - удалить все зараженные файлы, поэтому лучше постоянно обновлять свою антивирусную программу, особенно если вы используете Windows.

# Скрипт-вирусы

**Примеры:** DDoS, JS.fornight
**Может повлиять на:** Любая веб-страница путем внедрения скрытого кода в заголовок, нижний колонтитул или файл корневого доступа.

Вирус веб-скриптов нарушает безопасность веб-браузера, позволяя злоумышленникам внедрять сценарии на стороне клиента в веб-страницу. Он распространяется гораздо быстрее, чем другие обычные вирусы.

# Скрипт-вирусы

Когда он нарушает безопасность веб-браузера, он внедряет вредоносный код для изменения некоторых настроек и захвата браузера. Как правило, он распространяется с помощью зараженной рекламы, всплывающей на веб-страницах. Вирусы веб-скриптов в основном нацелены на сайты социальных сетей. Некоторые из них достаточно мощны, чтобы рассылать спам по электронной почте и инициировать опасные атаки, такие как DDoS-атаки, чтобы сделать сервер неотзывчивым или до предела медленным.

**Их можно разделить на две группы:**

- Постоянные вирусы веб-скриптов: могут выдавать себя за пользователя и наносить большой ущерб.
- Непостоянный вирус веб-скриптинга: атакует пользователя незаметно. Он работает в фоновом режиме и остается навсегда скрытым для пользователя.

# Скрипт-вирусы

**Защита:** Используйте средства удаления вредоносных программ в Windows, отключите скрипты, используйте защиту cookie или установите программное обеспечение для защиты веб-браузера в режиме реального времени.

# Каталоговый вирус

**Пример:** Dir-2
**Может поражать:** Всю программу в каталоге.

Каталоговый вирус (также известный как Кластерный вирус) заражает файл, изменяя информацию о каталоге DOS. Он изменяет DOS таким образом, что она указывает на код вируса, а не на исходную программу.

# Каталоговый вирус

Более конкретно, этот вирус внедряет вредоносный код в кластер и помечает его как выделенный в FAT. Затем он сохраняет первый кластер и использует его для нацеливания на другие кластеры, связанные с файлом, который он хочет заразить следующим. Когда вы запускаете программу, DOS загружает и выполняет код вируса до запуска собственно программного кода. Другими словами, вы неосознанно запускаете вирусную программу, в то время как оригинальная программа предварительно перемещена вирусом. После заражения становится очень трудно найти оригинальный файл.

# Каталоговый вирус

**Защита:** Установите антивирус, чтобы переместить ошибочно перемещенные файлы.

# Полиморфный вирус

**Примеры:** Whale, Simile, SMEG engine, UPolyX.
**Может поражать:** Любой файл

Полиморфные вирусы кодируют себя, используя разные ключи шифрования каждый раз, когда заражают программу или создают свою копию. Из-за различных ключей шифрования антивирусным программам становится очень трудно их обнаружить.

# Полиморфный вирус

Этот тип вируса зависит от мутационных механизмов для изменения своих процедур расшифровки каждый раз, когда он заражает устройство. Он использует сложные мутационные механизмы, которые генерируют миллиарды процедур дешифрования, что еще больше затрудняет его обнаружение. Другими словами, это самошифрующийся вирус, созданный для того, чтобы избежать обнаружения сканерами. Первый известный полиморфный вирус (под названием "1260") был создан Марком Вашбёрном в 1990 году. При выполнении он заражает файлы .com в текущем каталоге или каталоге PATH.

# Полиморфный вирус

**Защита:** Установите современные антивирусные инструменты, оснащенные новейшими технологиями безопасности (такими как алгоритмы машинного обучения и аналитика на основе поведения) для обнаружения угроз.

# Резидентный вирус памяти

**Примеры:** Randex, Meve, CMJ
**Может влиять на:** Текущие файлы на компьютере, а также файлы, которые копируются или переименовываются.

Резидентный вирус живет в первичной памяти (RAM) и активируется при включении компьютера. Он поражает все файлы, запущенные в данный момент на рабочем столе.

# Резидентный вирус памяти

Поскольку вирус загружает свой модуль репликации в основную память, он может заражать файлы, не будучи запущенным. Он автоматически активируется всякий раз, когда операционная система загружается или выполняет определенные функции.

**Существует два типа вирусов, живущих в памяти:**

- Быстрые инфекторы специально созданы для того, чтобы как можно быстрее испортить как можно больше файлов. Их очень легко заметить из-за их негативных последствий. - Медленные инфекторы постепенно снижают производительность компьютера. Они распространяются более широко, поскольку могут оставаться незамеченными гораздо дольше.

# Резидентный вирус памяти

**Защита:** Сильные антивирусные инструменты могут удалить вирус из памяти. Они могут поставляться в виде патча для ОС или обновления существующего антивирусного программного обеспечения.

Если вам повезет, в вашем антивирусном ПО может быть расширение или плагин, который можно загрузить на флешку и запустить, чтобы удалить вирус из памяти. В противном случае, возможно, придется переформатировать машину и восстановить все, что можно, из имеющейся резервной копии.

# Макровирус

**Примеры:** Bablas, Concept и вирус Melissa
**Может поражать:** файлы .mdb, .PPS, .Doc, .XLs.

Эти вирусы написаны на том же макроязыке, который используется в популярных программах, таких как Microsoft Excel и Word. Они вставляют вредоносный код в макросы, связанные с электронными таблицами, документами и другими файлами данных, заставляя зараженную программу запускаться сразу после открытия документа.

# Макровирус

Макровирусы предназначены для повреждения данных, вставки слов или изображений, перемещения текста, отправки файлов, форматирования жестких дисков или передачи еще более разрушительных видов вредоносных программ. Они передаются через фишинговые электронные письма. В основном они поражают файлы MS Excel, Word и PowerPoint. Поскольку этот тип вируса действует на приложения (а не на операционные системы), он может заразить любой компьютер под управлением любой операционной системы, даже Linux и macOS.

# Макровирус

**Защита:** Отключите макросы и не открывайте электронные письма из неизвестных источников. Вы также можете установить современное антивирусное программное обеспечение, которое легко обнаруживает макровирусы.

# Вирус-компаньон

**Примеры:** Stator, Terrax.1096
**Может поражать:** Все файлы .exe

Вирусы-компаньоны были более популярны в эпоху MS-DOS. В отличие от обычных вирусов, они не изменяют существующий файл. Вместо этого они создают копию файла с другим расширением (например, .com), которая запускается параллельно с настоящей программой.

# Вирус-компаньон

Например, если существует файл с именем abc.exe, этот вирус создаст еще один скрытый файл с именем abc.com. И когда система вызывает файл 'abc', .com (расширение с более высоким приоритетом) запускается раньше расширения .exe. Он может выполнять вредоносные действия, например, удалять исходные файлы. В большинстве случаев вирусы-компаньоны требуют вмешательства человека для дальнейшего заражения машины. После появления Windows XP, которая больше не использует интерфейс MS-DOS, у таких вирусов стало меньше путей для распространения.

# Вирус-компаньон

Однако вирус все еще работает в последних версиях операционных систем Windows, если пользователь открывает файл непреднамеренно, особенно при отключенной опции "показывать расширение файла".

**Защита:** Вирус можно легко обнаружить благодаря наличию дополнительного файла .com. Установите надежное антивирусное программное обеспечение и избегайте загрузки вложений нежелательных писем.

# Многосторонний вирус

**Примеры:** Ghostball, Invader.
**Может повлиять на:** файлы и загрузочный сектор.

Многосторонний вирус заражает и распространяется разными способами в зависимости от операционной системы. Обычно он остается в памяти и заражает жесткий диск.

# Многосторонний вирус

В отличие от других вирусов, которые поражают либо загрузочный сектор, либо программные файлы, многосторонний вирус атакует как загрузочный сектор, так и исполняемые файлы одновременно, вызывая еще больший ущерб. Попадая в систему, он заражает все диски, изменяя содержимое приложений. Вскоре вы начнете замечать отставание в производительности и нехватку виртуальной памяти, доступной для пользовательских приложений.

# Многосторонний вирус

Первым зарегистрированным многосторонним вирусом был "Ghostball". Он был обнаружен в 1989 году, когда Интернет еще находился на ранней стадии своего развития. В то время он не смог охватить многих пользователей. Однако с тех пор все сильно изменилось. Сейчас, когда в мире насчитывается более 4,66 миллиарда активных пользователей Интернета, многокомпонентные вирусы представляют серьезную угрозу для предприятий и потребителей.

**Защита:** Очищайте загрузочный сектор и весь диск перед сохранением новых данных. Не открывайте вложения из ненадежных интернет-источников и установите надежный и проверенный антивирусный инструмент.

# FAT-вирус

**Пример:** Вирус ссылок
**Может поражать:** Любой файл

FAT расшифровывается как file allocation table, это раздел диска, который используется для хранения информации, такой как расположение всех файлов, общий объем памяти, доступное пространство, использованное пространство и т. д.

# FAT-вирус

Вирус FAT изменяет индекс и делает невозможным для компьютера выделение файла. Он достаточно силен, чтобы заставить вас отформатировать весь диск. Другими словами, вирус не изменяет хост-файлы. Вместо этого он заставляет операционную систему выполнять вредоносный код, изменяющий определенные поля в файловой системе FAT.

В результате компьютер не может получить доступ к определенным разделам жесткого диска, где находятся важные файлы. По мере распространения вируса несколько файлов или даже целые каталоги могут быть перезаписаны и безвозвратно потеряны.

# FAT-вирус

**Защита:** Избегайте загрузки файлов из ненадежных источников, особенно тех, которые определены браузером или поисковой системой как "атакующие/небезопасные сайты". Используйте надежное антивирусное программное обеспечение.

Другие вредоносные программы, которые не являются вирусами, но не менее опасны.

# Троянский конь

**Примеры:** ProRat, ZeroAccess, Beast, Netbus, Zeus

Троянский конь (или троян) - это невоспроизводимый тип вредоносного ПО, который выглядит легитимным. Пользователей обычно обманом заставляют загрузить и выполнить его на своей системе. Он может уничтожить/изменить все файлы, модифицировать реестр или вывести компьютер из строя. Более того, он может дать хакерам удаленный доступ к вашему компьютеру.

# Троянский конь

Как правило, трояны распространяются с помощью различных форм социальной инженерии. Например, пользователей обманом заставляют нажимать на поддельные рекламные объявления или открывать вложения электронной почты, замаскированные под настоящие.

**Защита:** Избегайте открытия неизвестных файлов (особенно с расширениями .exe, .bat и .vbs), атакованных по электронной почте. Используйте надежное антивирусное программное обеспечение высокого класса и регулярно обновляйте его.

# Червь

**Пример:** Code red, ILOVEYOU, Morris, Nimda, Sober, WANK.

Червь - это отдельная вредоносная программа, которая воспроизводит себя для распространения на другие компьютеры. Для перемещения от одной системы к другой он использует сети (в основном электронную почту) и бреши в системе безопасности. В отличие от вирусов, он перегружает сеть, реплицируясь или отправляя слишком много данных (превышая пропускную способность), заставляя хозяев отключать сервер.

# Червь

Червь способен реплицировать себя без какого-либо участия человека. Ему даже не нужно подключать приложение, чтобы нанести ущерб. Большинство червей предназначены для изменения содержимого, удаления файлов, истощения системных ресурсов или внедрения на компьютер дополнительного вредоносного кода. Они также могут красть данные и устанавливать черный ход, облегчая злоумышленникам контроль над компьютером и его системными настройками.

# Червь

**Защита:** Обновляйте операционную систему и убедитесь, что вы используете надежное программное обеспечение для обеспечения безопасности.

# Логические бомбы

Логические бомбы - это не вирус, но по своей сути вредоносны, как черви и вирусы. Это часть кода, намеренно вставленная (скрытая) в программу. Код выполняется при соблюдении определенных критериев. Например, взломщик может вставить код кейлоггера в любое расширение веб-браузера. Код активируется каждый раз, когда вы посещаете страницу входа в систему. Затем он перехватывает все нажатия клавиш, чтобы украсть ваше имя пользователя и пароль.

# Логические бомбы

Логические бомбы могут быть вставлены в существующее программное обеспечение или в другие формы вредоносного ПО, такие как черви, вирусы или троянские кони. Они находятся в спящем состоянии до момента срабатывания и могут оставаться незамеченными годами.

**Защита:** Периодически сканируйте все файлы, включая сжатые, и обновляйте антивирусное программное обеспечение.