1. **ЦИКЛ ФУНКЦИОНИРОВАНИЯ ВИРУСОВ**

В цикле существования большинства вредоносных программ можно условно выделить два этапа:

* Загрузка вируса в память компьютера.
* Выполнение вредоносного кода.

В свою очередь по способу загрузки вирусов в память компьютера, их тоже можно разделить на два типа:

* Вирусы, не способные к самостоятельному распространению.
* Вирусы, распространяющиеся самостоятельно, без участия пользователя.

К вирусам, которые не способны распространяться самостоятельно, можно отнести классические вирусы, трояны, макровирусы, скрипт-вирусы и т.д.

К вирусам, распространяющиеся без участия пользователя относятся, в основном, черви.

## Вирусы, не способные к самостоятельному распространению

Итак, сначала опишем каналы распространения вирусов этого типа:

* *Сменные накопители* – к этому каналу относятся оптические диски, USB флеш-накопители, внешние USB-винчестеры, и морально устаревшие дискеты. При подключении сменных накопителей информации в ОС Windows, вплоть до 7-ой версии, автоматически запускается файл Autorun.inf, используемый для автоматического запуска или установки приложений. И большинство вирусописателей внедряют в вирусы алгоритм самокопирования вируса и создания своего файла автозагрузки.
* *Электронная почта* - заражение компьютера посредством этого канала происходит либо с помощью ссылок на заражённые сайты (файлы), либо с помощью вложенных в письма данных. При этом используется метод, так называемой, «социальной инженерии» - это управление действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора.
* *Системы обмена мгновенными сообщениями* – заражение компьютера с помощью этого канала аналогично заражению с помощью электронной почты.
* *Веб-страницы* – заражение компьютера происходит путём загрузки заражённых данных непосредственно со страницы, которая уже заражена. При этом злоумышленники используют уязвимости программного обеспечения администрации сайта. Так же не исключена вероятность попадания на фишинговый сайт, специально созданный для обмана пользователя и нанесения того или иного вреда.

После загрузки вируса в оперативную память моментально выполняется сам вредоносный код.

У абсолютного большинства вирусов сперва выполняется алгоритм самокопирования в определённую злоумышленником папку. Далее вредоносная программа внедряет в систему механизм автоматической загрузки, который срабатывает при запуске операционной системы. При этом, в большинстве случаев, происходит добавление ключа вируса в системный реестр, либо модификация стандартных ключей с добавлением нужных вирусу параметров. Так же не исключена возможность использования особенности операционной системы Windows, связанной с очерёдностью запуска исполняемых файлов. К примеру, в папке находятся два исполняемых файла с одинаковым именем, но у одного из них будет расширение *com*, а у другого *exe*. Если при запуске из командной строки не использовать расширение исполняемого файла, сразу запустится файл с расширением *com*. Так, как абсолютное большинство исполняемых файлов Windows имеют расширение *exe*, некоторые вирусописатели используют эту особенность для обмана пользователей. Но, значительно чаще, злоумышленники либо заменяют исполняемые файлы вредоносными, либо модифицируют *exe*-файлы программ.

Так же, немаловажное значение имеет механизм маскировки вируса. Так как, большая часть процессов и служб, выполняемых в операционной системе, отображается во вкладке «процессы», «Диспетчера задач Windows». Процесс с неизвестным, или подозрительным названием может вызвать недоверие пользователя, поэтому вирусописатели скрывают вредоносные программы под именами системных процессов, или служб. Чаще всего используется процесс *svchost*, который отвечает за запуск большого количества служб Windows. По этой причине процессов с этим именем всегда несколько, что затрудняет выявление вируса. Кроме того, нередко встречаются и производные от этого имени, к примеру: *svchast*, *scvhost* и т.д. Нередко используется и *explorer* – процесс проводника Windows.

Очень часто, во избежание завершения процесса вируса пользователем, авторы используют дублирование, переименование, и запуск нескольких копий вредоносной программы. И, если пользователь заподозрит вредоносный процесс и завершит его, другой экземпляр тут же восстановит копию процесса.

В настоящее время, становятся распространены вирусы, которые вообще не отображают себя в диспетчере задач. Некоторые из них, могут полностью скрывать своё присутствие в системе, посредством уязвимостей безопасности. Нередки случаи заражения выполняемых процессов в оперативной памяти, без непосредственного запуска вируса с жёсткого диска.

Большинство вредоносных программ заражают не только исполняемые файлы, а так же DLL-библиотеки, заменяя их модифицированными злоумышленниками файлами. По этой причине, некоторые программы, использующие эти библиотеки, могут отказаться работать. Так же, часто используется перехват функций API, которые используют огромное количество программ. При этом, вредоносный код будет исполнятся только потому, что в абсолютно безвредной программе была запущена, к примеру, функция сохранения данных, или любая другая.

Некоторые злоумышленники, во избежание удаления вируса, добавляют алгоритм слежения за антивирусными программами, запрещая их запуск, установку, или выполнение. Так же, возможно добавление в системный реестр ключей, блокирующий запуск диспетчера задач и редактора реестра Windows.

## Вирусы, распространяющиеся самостоятельно

И так, теперь рассмотрим цикл функционирования червей.

Каналами распространения классических червей являются локальные и глобальные компьютерные сети. Как уже писалось ранее, механизм распространения можно разделить на две большие группы.

* Первая группа червей сканируют сетевые порты различных протоколов передачи данных, отыскивая ошибки в службах безопасности операционных систем и приложений. Такие ошибки называются эксплойтами.
* Вторая группа использует метод «социального инжиниринга», провоцируется запуск вредоносной программы самим пользователем. Данный метод широко применяется в рассылках спама, социальных сетях и т. д.

Черви, в отличие от всех остальных типов вредоносных программ, более автоматизированы, и представляют более совершенные механизмы заражения, распространения и нанесения вреда пользователям. Именно они в наибольшей степени соответствуют термину *вирус*, если сравнивать его с «биологическими» аналогами.

Червь, после попадания в компьютер пользователя, как и остальные типы вредоносных программ, сохраняется в какой-либо папке и прописывается в системном реестре для последующего автоматического запуска. Затем, после окончательного укрепления в операционной системе, червь переходит к активной фазе размножения.

В первую очередь идёт сканирование адресных книг почтовых клиентов, просмотр локальных файлов на предмет поиска сетевых адресов, сканирование IP-адресов текущей подсети и генерация случайного IP-адреса для последующей рассылки.

После этого червь, проверяет каждый из адресов на предмет наличия нужного программного обеспечения и возможной копии, которой уже может быть заражён данный компьютер, посредством безобидного сетевого запроса. И предпринимает дальнейшие действия, в зависимости от ответа.

Затем распространение идёт дальше, от одного компьютера к другому, основательно нагружая сеть, занимая канал передачи данных. Кроме загрузки канала, черви могут выполнять все функции классических вирусов.

Так же, в последние годы, черви активно используются для создания бот-нета – компьютерной сети, скрытно используемой злоумышленниками для рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.

Самая главная опасность червей – это то, что антивирусы не могут справиться с червями. Потому, что даже при полном удалении вредоносного кода антивирус не может заделать брешь в системе безопасности, через который проник данный вирус. Поэтому, при использовании локальных сетей, или глобальной сети интернет, всегда есть риск заразится каким-либо червём, использующим нестандартный алгоритм распространения.