1. **ПОНЯТИЕ ВИРУСА**

В настоящее время, стараниями основной массы пользователей, к компьютерным вирусам причисляют все вредоносные программы, независимо от их назначения. Отчасти, такая ситуация сложилась по причине банального незнания основ безопасности персонального компьютера. С другой стороны, не существует единой системы классификации и именования вредоносных программ, хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году. Это происходит потому, что вирусописателями ежедневно производится множество вирусов, и некоторые из них, могут иметь признаки сразу нескольких классов вредоносных программ. Так же, любой уважающий себя разработчик антивирусного программного обеспечения, в первую очередь для удобства, создаёт свою классификацию вирусов. Но, если оценивать классификации большинства антивирусов, то можно разделить вредоносные программы на несколько основных групп.

**Вредоносные программы** – общее название для всех программ и приложений, целью которых заведомо является нанесение того или иного вреда конечному пользователю. Классы вредоносных программ чрезвычайно многочисленны и разнообразны, однако в целом по характеру поведения и распространения все антивирусные компании подразделяют их на три главных рода – трояны, черви и классические вирусы.

**Троян** - вредоносная программа, не имеющая механизма самостоятельного распространения, в отличие от червей, которые распространяются самопроизвольно. Это один из самых простых видов вредоносных программ, сложность которых зависит исключительно от сложности истинной задачи и средств маскировки. Самые примитивные экземпляры (например, стирающие содержимое диска при запуске) могут иметь исходный код в несколько строк.

Большинство троянов осуществляют различные несанкционированные пользователем действия: сбор и передача информации злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера.

Название «троянская» программа исходит из легенды о «Троянском коне» — дарёном деревянном коне, послужившим причиной падения Трои. В коне, подаренном в знак ложного перемирия, прятались греческие воины, ночью открывшие ворота армии завоевателя. Большая часть троянских программ действует подобным образом — маскируется под безвредные или полезные программы, чтобы пользователь запустил их на своем компьютере. Считается, что первым этот термин в контексте компьютерной безопасности употребил Дэниэл Эдвардс, сотрудник NASA, в своём отчёте «Computer Security Technology Planning Study».

Троянские программы распространяются людьми — как непосредственно загружаются в компьютерные системы злоумышленниками, так и побуждают пользователей загружать и/или запускать их на своих системах. Также они помещаются злоумышленниками на открытые или индексируемые ресурсы (файл-серверы и системы обмена файлами), носители информации, присылаются с помощью служб обмена сообщениями (например, электронной почтой), попадают на компьютер через бреши безопасности или загружаются самим пользователем с адресов полученных одним из перечисленных способов.

Иногда использование троянов является лишь частью спланированной многоступенчатой атаки на определенные компьютеры, сети или ресурсы.

Троянские программы хуже обнаруживаются контекстными методами антивирусов (основанных на поиске известных программ), потому что их распространение лучше контролируется, и экземпляры программ попадают к специалистам антивирусной индустрии с большей задержкой, нежели самопроизвольно распространяемые вредоносные программы.

**Червь** – разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети. Зачастую черви перегружают и временно выводят из строя сети только за счёт интенсивного распространения. Очень часто, из зараженных червём компьютеров, возможна организация автономной сети зараженных компьютеров для проведения сетевых атак или рассылки спама.

Одним из наиболее известных компьютерных червей является «Червь Морриса», написанный Робертом Моррисом-младшим, который был в то время студентом Корнельского Университета. Распространение червя началось 2 ноября 1988, после чего червь быстро заразил около 10 % всех компьютеров, подключённых в то время к Интернету.

Все способы распространения червей делятся на две большие группы:

* Использование уязвимостей и ошибок администрирования в программном обеспечении, установленном на компьютере. Такие черви способны распространяться автономно, выбирая и атакуя компьютеры в полностью автоматическом режиме.
* Используя средства так называемой социальной инженерии, провоцируется запуск вредоносной программы самим пользователем. Данный метод широко применяется в рассылках спама, социальных сетях и т. д.

Иногда встречаются черви с целым набором различных способов распространения, стратегий выбора жертвы, и даже эксплойтов под различные операционные системы. Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

**Вирус** – самый старый род вредоносных программ, классические вирусы. Именно из-за этих представителей вредоносные программы как целое стали называть вирусами. Их отличительной особенностью является способность к размножению (саморепликация). В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и компьютеру. Эти программы изменяют исполняемые файлы, то есть «заражают» их, дописывая в них свой код. Как следствие, каждый раз при исполнении зараженного файла выполняется код вируса. Сейчас количество программ этого рода значительно уменьшилось, однако они по-прежнему представляют угрозу: для антивируса этот тип вредоносных программ наиболее сложен в лечении.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере.

Кроме того, существует род группы риска и прочих вредоносных программ. Это не очень многочисленная группа программ, которые не выполняют непосредственно вредоносных действий, но потенциально опасны. Сюда относят рекламные программы, программы-розыгрыши, хакерские инструменты и некоторые другие.

**Рекламная программа** - это приложение, предназначенное для загрузки на компьютер пользователя информации рекламного характера для последующей демонстрации этой информации пользователю. Можно выделить две категории рекламных программ:

1) Программы, распространяемые по рекламной лицензии. Данные программы воспроизводят рекламу в качестве неявной оплаты за их использование, при этом реклама должна воспроизводится только во время использования программы в контексте ее окон;

2) Независимое приложение, предназначенное для воспроизведения рекламы. Такие программы, как правило, маскируются от обнаружения и удаления пользователем и могут существенно досаждать пользователю. Рекламная информация обычно выводится в виде всплывающих окон, хотя известны и широко применяются и другие методики демонстрации рекламы, такие как внедрение рекламной информации в рабочий стол в виде фоновых рисунков или с использованием возможностей размещения WEB элементов на рабочем столе.

**Программа-розыгрыш** – данный тип программ вредоносный не является. Её основное предназначение - заставить пользователей поверить, что они заражены вирусом. Данные программы обычно имитируют действия вирусов, либо рассылают ложные сообщения по электронной почте, предупреждающие пользователей о несуществующей опасности. Хотя они являются больше раздражающими, чем вредоносными, пользователям строго рекомендуется не открывать любые файлы, прикрепленные к подозрительным электронным сообщениям.

**Хакерские инструменты** – в данный тип программ входят множество подгрупп программ, используемые злоумышленниками для нанесения вреда компьютерам пользователей. К этим программам относятся конструкторы вирусов, утилиты для проведения DDoS-атак, программы рассылки спама и т. д. Но в отличии от остальных вредоносных программ, данные утилиты приносят вред только когда ими пользуются злоумышленники.

Отдельной группой следуют:

**Бэкдор** – вредоносная программа, предоставляющая злоумышленнику удаленный доступ к зараженному компьютеру. Функционал программ этого типа может быть очень широк. После установки в систему бэкдор может ожидать входящих соединений от компьютера злоумышленника, сам пытается с ним соединиться, либо компьютеры обмениваются данными через дополнительный сервер. Основное назначение бэкдора – скрытное управление компьютером. Как правило, данная программа позволяет копировать файлы с пораженного компьютера и наоборот, передавать на пораженный компьютер файлы и программы. Кроме того, обычно бэкдор позволяет получить удаленный доступ к реестру, производить системные операции и т.д. Ещё одной особенностью этих программ является то, что они позволяют использовать компьютер пользователя для сканирования сети, проведения сетевых атак взлома сетей – при этом попытки взлома ведутся с компьютера ничего не подозревающего пользователя.

**Руткит** – вредоносная программа, перехватывающая и изменяющая системные функции с целью скрытия или маскировки файлов, процессов, ключей реестра и так далее. Термин «руткит» исторически пришёл из мира UNIX, и под этим термином понимается набор утилит или специальный модуль ядра, которые взломщик устанавливает на взломанной им компьютерной системе сразу после получения прав суперпользователя. В операционной системе Windows, из-за системы защиты файлов, переписывание системных файлов затруднено, поэтому основной способ внедрения в систему - модификация памяти. Это происходит посредством перехвата системных функций Windows на уровне пользователя и на уровне ядра системы, изменения системных структур данных, модификации загрузочной записи диска и загрузки до ядра операционной системы. Данный вид вредоносных кодов в среде Windows известен с начала 1990-х годов под названием стелс-вирусов.

**Шпион -** вредоносная программа, которая скрытным образом устанавливается на компьютер с целью сбора информации о конфигурации компьютера, пользователе, пользовательской активности без согласия последнего. Данный тип вредоносных программ очень разнообразен, и может осуществлять широкий круг задач: собирать информацию о привычках пользования интернетом и наиболее часто посещаемые сайты, запоминать нажатия клавиш на клавиатуре и записывать снимки экрана для дальнейшей отправки злоумышленнику, несанкционированно и удалённо управлять компьютером, устанавливать на компьютер пользователя дополнительные программы, анализировать состояния систем безопасности, перенаправлять активность браузеров и т.д.