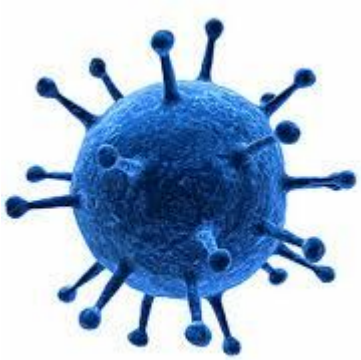
Классификация вредоносного ПО (**malware**)

Защита информационных ресурсов компьютерных систем



Сетевые черви

это вредоносный программный код, распространяющий свои копии по локальным или/и глобальным сетям с целью проникновения на компьютер-жертву, запуска своей копии на этом компьютере и дальнейшего распространения

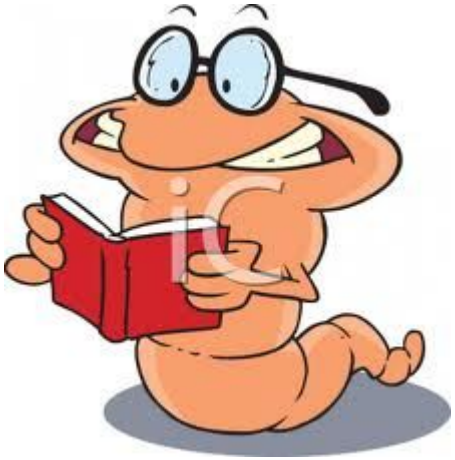
email-worm - Почтовые черви

Данный класс сетевых червей использует для распространения электронную почту.

Червь может просканировать файлы, хранящиеся на дисках, и выделить из них строки, относящиеся к адресам электронной почты. Черви могут отсылать свои копии по всем адресам, обнаруж

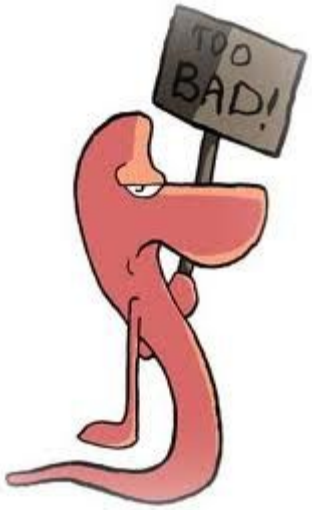
im-worm - черви, использующие интернет-пейджеры

Известные компьютерные черви данного типа используют единственный способ распространения — рассылку на обнаруженные контакты (из контакт-листа) сообщений, содержащих url на файл, расположенный на каком-либо веб-сервере



irc-worm - черви в irc-каналах

Черви этого класса используют два вида распространения: посылание пользователю url-ссылки на файл-тело; отсылку пользователю файла (при этом пользователь должен подтвердить прием)

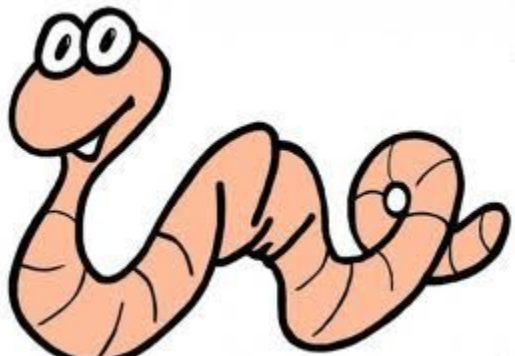


p2p-worm - черви для файлообменных сетей

Механизм работы большинства подобных червей достаточно прост: для внедрения в p2p-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по его распространению p2p-сеть берет на себя — при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для его скачивания с зараженного компьютера.

net-worm - прочие сетевые черви

- копирование червя на сетевые ресурсы;
- проникновение червя на компьютер через уязвимости в операционных системах и приложениях;
- проникновение в сетевые ресурсы публичного использования;
- паразитирование на других вредоносных программах.



Компьютерный вирус

Это программа способная к саморазмножению и выполнению разных деструктивных действий.

Вирусы, в отличие от червей, не пользуются сетевыми сервисами для распространения своих копий. Компьютерный вирус, как правило, попадает на компьютер-жертву по причинам, не от функционала кода

overwriting - перезаписывающие вирусы

Самый распространенный способ заражения. Вирус переписывает код программы (заменяет его своим), после чего, естественно, файл перестает работать. Файл, зараженный данным способом, восстановлению не подлежит. Перезаписывающий вирус быстро обнаруживает себя, так как зараженная система (или программа) перестает функционировать.

parasitic - паразитические вирусы

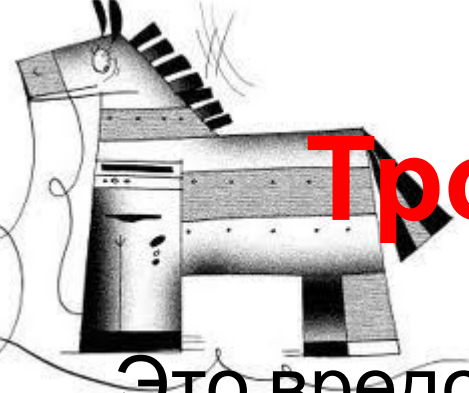
К таковым относятся все вирусы, которые изменяют содержимое файла, но при этом оставляют его работоспособным. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (**prepending**), в конец файлов (**appending**) и в середину файлов (**inserting**).

companion - вирусы-компаньоны

Данный способ подразумевает создание файла-двойника, при этом код файла-жертвы не изменяется. Обычно вирус изменяет расширение файла, потом создает свою копию с именем, идентичным имени файла-жертвы, и дает ему расширение, тоже идентичное

другие вирусы

- вирусы, заражающие объектные модули (obj);
- вирусы, заражающие библиотеки компиляторов (lib);
- вирусы, заражающие исходные тексты программ.



Троянские программы

Это вредоносный код, совершающий не санкционированные пользователем действия (например, кража информации, уничтожение или модификация информации, использование ресурсов машины в злонамеренных целях и т.д.). Троянские программы являются наиболее распространенными в киберсреде, так как существует множество конструкторов, позволяющих даже неопытному пользователю создавать собственные программы данного типа

backdoor - троянские утилиты удаленного администрирования

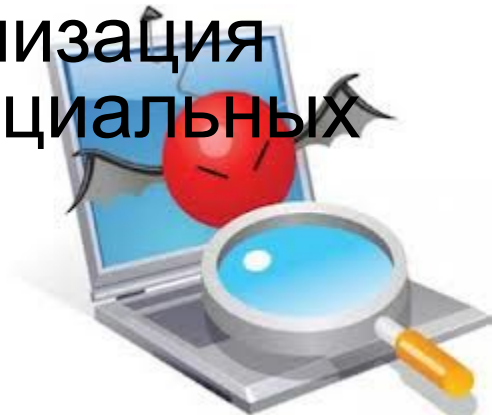
Троянские программы этого класса являются утилитами удаленного администрирования (управления) компьютеров. В общем, они очень похожи на «легальные» утилиты того же направления. Единственное, что определяет их как вредоносные программы, — это их действия без ведома пользователя.

trojan-psw - похитители паролей

Проникнув на компьютер и инсталлировавшись, троянец сразу приступает к поиску файлов, содержащих соответствующую информацию. Кража паролей — не основная спецификация программ этого класса — они также могут красть информацию о системе, файлы, номера счетов, коды активации другого ПО и т.д.

trojan-clicker - интернет-кликеры

Данное семейство троянских программ занимается организацией несанкционированных обращений к интернет-ресурсам путем отправления команд интернет-браузерам или подмены системных адресов ресурсов. Злоумышленники используют данные программы для следующих целей: увеличение посещаемости каких-либо сайтов (с целью увеличения количества показов рекламы); организация атаки на сервис; привлечение потенциальных жертв для заражения вредоносным программным обеспечением.



trojan-downloader - загру

Эти трояны занимаются несанкционированной загрузкой программного обеспечения (вредоносного) на компьютер ничего не подозревающего пользователя. После загрузки программа либо инсталлируется, либо записывается трояном в автозагрузку (это в зависимости от возможностей операционной систе

trojan-dropper - установщики

ти устанавливают на компьютер-жертву программы — как правило вредоносные. Анатомия троянцев этого класса следующая: основной код, файлы. Основной код собственно и является троянцем. Файлы — это программа/ы, которая/ые он должен установить. Троянец записывает ее/их в каталог (обычно временных файлов) и устанавливает

trojan-proxy - троянские прокси-серверы

Семейство троянских программ, скрытно осуществляющих доступ к различным интернет-ресурсам — обычно с целью рассылки спама

trojan-spy - шпионские программы

Данные трояны осуществляют шпионаж за пользователем: записывание информации, набранной с клавиатуры, снимки экрана и т.д. В данной категории также присутствуют «многоцелевые» троянские программы — например, те из них, которые одновременно шпионят за пользователем и предоставляют proxy-сервис удаленному злоумышленнику

rootkit - сокрытие присутствия в операционной системе

Программный код или техника, направленная на сокрытие присутствия в системе заданных объектов (процессов, файлов, ключей реестра и т.д.).

arcbomb - архивные бомбы

такого рода архив при попытке архиватора его обработать вызывает «нестандартные» действия последнего.

Встречаются три:

некорректный заголовок архива;

повторяющиеся данные;

одинаковые файлы в архиве.

trojan-notifier - оповещение об атаке, увенчавшейся успехом

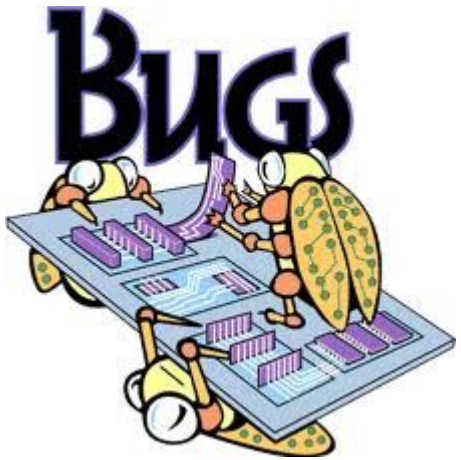
Троянцы данного типа предназначены для сообщения своему «хозяину» о зараженном компьютере. При этом на адрес «хозяина» отправляется информация о компьютере — например, его ip-адрес, номер открытого порта, адрес электронной почты и т.п.

Прочие вредоносные программы

К прочим вредоносным относятся разнообразные программы, не представляющие угрозы непосредственно компьютеру, на котором исполняются, а разработанные для создания других вирусов или троянских программ, организации dos-атак на удаленные серверы, взлома других компьютеров и т. п.

exploit - взломщики удаленных компьютеров

Эти программы используются хакерами для удаленного взлома компьютеров с целью дальнейшего управления ими. При этом эксплойты направлены непосредственно на работу с уязвимостями.

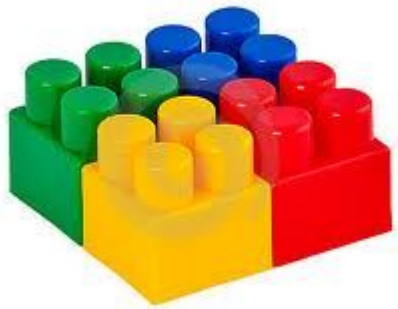


flood - «замусоривание» сети

Забивание интернет-каналов бесполезной информацией.

constructor - конструкторы

Софт, использующийся позволяют наиболее просто создавать троянские программы и т.д



nuker - фатальные сетевые атаки

Утилиты, отправляющие специально оформленные запросы на атакуемые компьютеры в сети, в результате чего атакуемая система прекращает работу. Используют уязвимости в программном обеспечении и операционных системах, в результате чего сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении.

bad-joke - введение пользователя в заблуждение

Это программка, которая заставляет пользователя испытать страх, эквивалентный тому, который он ощущает при виде надписи типа: «warning! system has bin delete», ну, или что-то в этом роде.

cryptor - шифровальщики вредоносного ПО

Это утилиты, которые занимаются тем, что скрывают другое вредоносное ПО от антивирусных программ

polyengine - «полиморфы»

Запутывания бинарного кода

Используемые источники

- Классификация вредоносного ПО
- Цикл статей. Rootkit. Введение.
- Вредоносная программа
- Компьютерные вирусы