

## Сетевые вирусы

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. "Полноценные" сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, "подтолкнуть" пользователя к запуску зараженного файла.

Бытует ошибочное мнение, что сетевым является любой вирус, распространяющийся в компьютерной сети. Но в таком случае практически все вирусы были бы сетевыми, даже наиболее примитивные из них: ведь самый обычный нерезидентный вирус при заражении файлов не разбирается - сетевой (удаленный) это диск или локальный. В результате такой вирус способен заражать файлы в пределах сети, но отнести его к сетевым вирусам никак нельзя.

Наибольшую известность приобрели сетевые вирусы конца 1980-х, их также называют сетевыми червями (worms). К ним относятся вирус Морриса, вирусы "Cristmas Tree" и "Wank Worm&". Для своего распространения они использовали ошибки и недокументированные функции глобальных сетей того времени - вирусы передавали свои копии с сервера на сервер и запускали их на выполнение. В случае с вирусом Морриса эпидемия захватила аж несколько глобальных сетей в США.

Сетевые вирусы прошлого распространялись в компьютерной сети и, как правило, так же как и компаньон-вирусы, не изменяли файлы или сектора на дисках. Они проникали в память компьютера из компьютерной сети, вычисляли сетевые адреса других компьютеров и рассылали по этим адресам свои копии. Эти вирусы иногда также создавали рабочие файлы на дисках системы, но могли вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

После нескольких эпидемий сетевых вирусов ошибки в сетевых протоколах и программном обеспечении были исправлены, а "задние двери" закрыты. В результате за последние десять лет не было зафиксировано ни одного случая заражения сетевым вирусом, как, впрочем, не появилось и ни одного нового сетевого вируса.

Вновь проблема сетевых вирусов возникла лишь в начале 1997-го года с появлением вирусов "Macro.Word.ShareFun" и "Win.Homer". Первый из них использует возможности электронной почты Microsoft Mail - он создает новое письмо, содержащее зараженный файл-документ ("ShareFun" является макро-вирусом), затем выбирает из списка адресов MS-Mail три случайных адреса и рассылает по ним зараженное письмо. Поскольку многие пользователи устанавливают параметры MS-Mail таким образом, что при

получении письма автоматически запускается MS Word, то вирус "автоматически" внедряется в компьютер адресата зараженного письма.

Этот вирус иллюстрирует первый тип современного сетевого вируса, которые объединяют возможности встроенного в Word/Excel языка Basic, протоколы и особенности электронной почты и функции авто-запуска, необходимые для распространения вируса.

Второй вирус ("Homer") использует для своего распространения протокол FTP (File Transfer Protocol) и передает свою копию на удаленный ftp-сервер в каталог Incoming. Поскольку сетевой протокол FTP исключает возможность запуска файла на удаленном сервере, этот вирус можно охарактеризовать как "полу-сетевой", однако это реальный пример возможностей вирусов по использованию современных сетевых протоколов и поражению глобальных сетей.

Возможны, конечно же, и другие способы проникновения вирусов в современные сети, однако мне не хотелось бы излагать их здесь, поскольку это подтолкнет вирусописателей на реализацию этих идей.