

### **Прочие "вредные программы"**

К "вредным программам", помимо вирусов, относятся также троянские кони (логические бомбы), хакерские утилиты скрытого администрирования удаленных компьютеров ("backdoor"), программы, "ворующие" пароли доступа к ресурсам Интернет и прочую конфиденциальную информацию; а также "intended" -вирусы, конструкторы вирусов и полиморфик-генераторы.

### **Троянские кони (логические бомбы)**

К троянским коням относятся программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от каких-либо условий или при каждом запуске уничтожающая информацию на дисках, "завешивающая" систему и т.п.

Большинство известных мне троянских коней являются программами, которые "подделываются" под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по BBS-станциям или электронным конференциям. По сравнению с вирусами "троянские кони" не получают широкого распространения по достаточно простым причинам - они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.

К "троянским коням" также можно отнести "дропперы" вирусов - зараженные файлы, код которых подправлен таким образом, что известные версии антивирусов не определяют вируса в файле. Например, файл шифруется каким-либо специальным образом или упаковывается редкоиспользуемым архиватором, что не позволяет антивирусу "увидеть" заражение.

Следует отметить также "злые шутки" (hoax). К ним относятся программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К "злым шуткам" относятся, например, программы, которые "пугают" пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в незараженных файлах (как это делает широко известная программа [ANTITIME](#)), выводят странные вирусоподобные сообщения (драйвер диска CMD640X от какого-то коммерческого пакета) и т.д. - в зависимости от чувства юмора автора такой программы. Видимо, к "злым шуткам" относится также строка ["CHOLEEPA"](#) во втором секторе винчестеров фирмы Seagate.

К такой же категории "злых шуток" можно отнести также заведомо ложные сообщения о новых супер-вирусах. Такие сообщения периодически появляются в электронных конференциях и обычно вызывают панику среди пользователей.

### **Утилиты скрытого администрирования (backdoor)**

Троянские кони этого класса по своей сути являются достаточно мощными утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов.

Единственная особенность этих программ заставляет классифицировать их как вредные троянские программы: отсутствие предупреждения об инсталляции и запуске. При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянца в системе. Более того, ссылка на троянца может отсутствовать в списке активных приложений. В результате "пользователь" этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Будучи установленными на компьютер, утилиты скрытого управления позволяют делать с компьютером все, что в них заложил их автор: принимать/отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т.д. В результате эти троянцы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т.п. - пораженные компьютеры оказываются открытыми для злоумышленных действий хакеров.

### **Intended-вирусы**

К таким вирусам относятся программы, которые на первый взгляд являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (что в подавляющем большинстве случаев завешивает компьютер) и т.д.

К категории "intended" также относятся вирусы, которые по приведенным выше причинам размножаются только один раз - из "авторской" копии. Заразив какой-либо файл, они теряют способность к дальнейшему размножению.

Появляются intended-вирусы чаще всего при неумелой перекомпиляции какого-либо уже существующего вируса, либо по причине недостаточного знания языка программирования, либо по причине незнания технических тонкостей операционной системы.

### **Конструкторы вирусов**

Конструктор вирусов - это утилита, предназначенная для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для DOS, Windows и макро-вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули, и/или непосредственно зараженные файлы.

Некоторые конструкторы (VLC, NRLG) снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса,

поражаемые объекты (COM и/или EXE), наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса и т.п. Прочие конструкторы (PS-MPC, G2) не имеют интерфейса и считывают информацию о типе вируса из конфигурационного файла.

### **Полиморфные генераторы**

Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т.е. открытия, закрытия и записи в файлы, чтения и записи секторов и т.д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

Обычно полиморфные генераторы распространяются их авторами без ограничений в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор. Во всех встречавшихся генераторах этот модуль содержит внешнюю (external) функцию - вызов программы генератора.

Таким образом автору вируса, если он желает создать настоящий полиморфик-вирус, не приходится копировать над кодами собственного за/расшифровщика. При желании он может подключить к своему вирусу любой известный полиморфик-генератор и вызывать его из кодов вируса. Физически это достигается следующим образом: объектный файл вируса линкуется с объектным файлом генератора, а в исходный текст вируса перед командами его записи в файл вставляется вызов полиморфик-генератора, который создает коды расшифровщика и шифрует тело вируса.

### **IRC-черви**

IRC (Internet Relay Chat) - это специальный протокол, разработанный для коммуникации пользователей Интернет в реальном времени. Этот протокол предоставляет возможность Интернет-"разговора" при помощи специально разработанного программного обеспечения. IRC чем-то похож на телефонный разговор, за исключением того, что в разговоре могут участвовать более двух собеседников, объединяющихся по интересам в различные группы IRC-конференций.

Для поддержки IRC-конференций созданы различные IRC-сервера, к которым подключаются участники IRC-"разговоров". Во всем мире насчитывается огромное количество IRC-серверов, объединенных в так называемые сети. Самой большой является сеть EFnet, сервера которой каждый день одновременно посещают несколько десятков тысяч пользователей.

Для подключения к IRC-серверу и ведения IRC-"разговоров" разработаны специальные программы - IRC-клиенты. Подключившись к IRC-серверу при помощи программы-клиента пользователь обычно выбирает тему IRC-конференции, командой join входит в одну или несколько конференций

("каналы" в терминах IRC) и начинает общение с другими "обитателями" этих каналов.

Помимо посещения общих (public) конференций пользователи IRC имеют возможность общаться один-на-один с любым другим пользователем (private), при этом они даже не обязательно должны быть на одном канале. Кроме этого существует довольно большое количество IRC-команд, при помощи которых пользователь может получить информацию о других пользователях и каналах, изменять некоторые установки IRC-клиента и прочее. Существует также возможность передавать и принимать файлы - именно на этой возможности и базируются IRC-черви.

### **IRC-клиенты**

На компьютерах с MS Windows самыми распространенными клиентами являются mIRC и PIRCH. Это не очень объемные, но довольно сложные программные продукты, которые кроме предоставления основных услуг IRC (подключение к серверам и каналам) имеют еще и массу дополнительных возможностей.

К таким возможностям относятся, например, сценарии работы (скрипты) и задание автоматической реакции на различные события. Например, при появлении во время разговора определенного слова IRC-клиент передает сообщение пользователю, пославшему это слово. Также возможно отключение пользователя от канала; посылка персональных сообщений новым пользователям, подключающимся к каналу; и многое другое. В PIRCH-клиенте, например, событий, на которые предусмотрена реакция, более 50.

### **Скрипт-черви**

Как оказалось, мощная и разветвленная система команд IRC-клиентов позволяет на основе их скриптов создавать компьютерные вирусы, передающие свой код на компьютеры пользователей сетей IRC, так называемые "IRC-черви". Первый инцидент с IRC-червем зафиксирован в конце 1997 года: пользователями mIRC-клиента был обнаружен скрипт (файл SCRIPT.INI), переносивший свой код через каналы IRC и заражавший mIRC-клиентов на компьютерах пользователей, подключавшихся к зараженным каналам. Как оказалось, скрипт-черви являются достаточно простыми программами, и через довольно короткое время на основе первого mIRC-червя были созданы и "выпущены" в сети несколько десятков различных скрипт-червей.

Принцип действия таких IRC-червей примерно одинаков. При помощи IRC-команд файл сценария работы (скрипт) или реакции на IRC-события автоматически посылается с зараженного компьютера каждому вновь присоединившемуся к каналу пользователю. Присланный файл-сценарий замещает стандартный и при следующем сеансе работы уже вновь зараженный клиент будет рассылать червя.

Черви при этом используют особенности конфигурации клиента (всех версий mIRC младше 5.31 и всех версий PIRCH до PIRCH98), благодаря которой принимаемые файлы всех типов помещаются в корневой каталог клиента.

Этот каталог также содержит и основные скрипты клиента, включая автозагружаемые mIRC-скрипты SCRIPT.INI, MIRC.INI и PIRCH-скрипт EVENTS.INI. Данные скрипты автоматически исполняются клиентом при старте и в дальнейшем используются как основной сценарий его работы.

Некоторые IRC-черви также содержат троянский компонент: по заданным ключевым словам производят разрушительные действия на пораженных компьютерах. Например, червь "pIRCH.Events" по определенной команде стирает все файлы на диске пользователя.

В скрипт-языках клиентов mIRC и PIRCH также существуют операторы для запуска обычных команд операционной системы и исполняемых модулей (программ) DOS и Windows. Эта возможность IRC-скриптов послужила основой для появления скрипт-червей нового поколения, которые помимо скриптов заражали компьютеры пользователей EXE-вирусами, устанавливали "троянских коней", и т.п.

Скрипт-черви работоспособны только в том случае, если пользователь разрешает копирование файлов из сети на свой компьютер. Данная опция IRC-клиентов называется 'DCC autoget' - получение файлов по протоколу DCC автоматически и без предупреждающего сообщения. При отключенной опции зараженный файл принимается, помещается в каталог клиента и в следующем сеансе работы продолжает свое распространение. При этом пользователь не получает никаких предупреждающих сообщений.

Следует отметить, что фирма-изготовитель клиента mIRC отреагировала достаточно оперативно и буквально через несколько дней после появления первого червя выпустила новую версию своего клиента, в которой были закрыты пробелы в защите.

### **mIRC.Acoragil и mIRC.Simpsalapim**

Первые известные mIRC-черви. Обнаружены в конце ноября - начале декабря 1997. Названия получили по кодовым словам, которые используются червями: если в тексте, переданном в канал каким-либо пользователем присутствует строка "Acoragil", то все пользователи, зараженные червем "mIRC.Acoragil" автоматически отключаются от канала. То же самое происходит с червем "mIRC.Simpsalapim" - он аналогично реагирует на строку "Simpsalapim".

При размножении черви командами mIRC пересылают свой код в файле SCRIPT.INI каждому новому пользователю, который подключается к каналу. Содержат троянскую часть. "mIRC.Simpsalapim" содержит код захвата канала IRC: если mIRC владельца канала заражен, то по вводу кодового слова "ananas", злоумышленник перехватывает управление каналом.

"mIRC.Acoragil" по кодовым словам пересылает системные файлы DOC, Windows или UNIX. Некоторые кодовые слова выбраны таким образом, что не привлекают внимания жертвы - hi, суа или the. Одна из модификаций этого червя пересылает злоумышленнику файл паролей UNIX.

### **Win95.Fono**

Опасный резидентный файлово-загрузочный полиморфик-вирус. Использует mIRC как один из способов своего распространения: перехватывает

системные события Windows и при запуске файла MIRC32.EXE активизирует свою mIRC-процедуру. При этом открывает файл MIRC.INI и записывает в его конец команду, снимающую защиту:

```
[fileservr]
```

```
Warning=Off
```

Затем создает файлы SCRIPT.INI и INCA.EXE. Файл INCA.EXE содержит дроппер вируса, скрипт файла SCRIPT.INI пересылает себя и этот дроппер в канал IRC каждому присоединившемуся к каналу и каждому выходящему с канала.

### **pIRCH.Events**

Первый известный PIRCH-червь. Рассылает себя каждому присоединившемуся к каналу пользователю. По ключевым словам выполняет различные действия, например:

по команде ".query" происходит своего рода переключки, по которой зараженные системы отвечают <Да, я уже заражена>;

по команде ".exit" завершает работу клиента.

По другим командам червь удаляет все файлы с диска C:, предоставляет доступ к файлам на зараженном компьютере, и т.д.