Статистика вирусных заражений

Компьютерные вирусы в цифрах и фактах

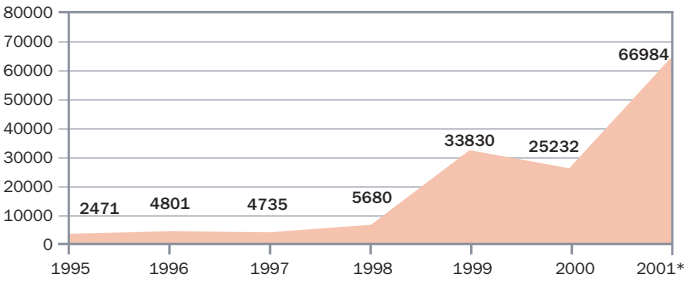
Черви, вирусы, трояны, бэкдоры, любовные письма, сибирская язва… Сегодня все это пестрое разнообразие компьютерной фауны прочно слилось в одну аморфную массу, наводящую суеверный ужас на непросвещенных пользователей. А вместе с тем компьютерная зараза, которая поджидает нас во всех возможных уголках Интернета, электронной почте, на дискетках и CD, стала реалией повседневной жизни.

Хотим мы того или нет, вирусы все равно проникают в наши компьютеры, и нам приходится с ними как-то бороться. «Врага нужно знать в лицо», — гласит народная мудрость. Давайте последуем ей, поближе познакомимся с вирусами, рассмотрим их разновидности и сферы их разрушительной деятельности.

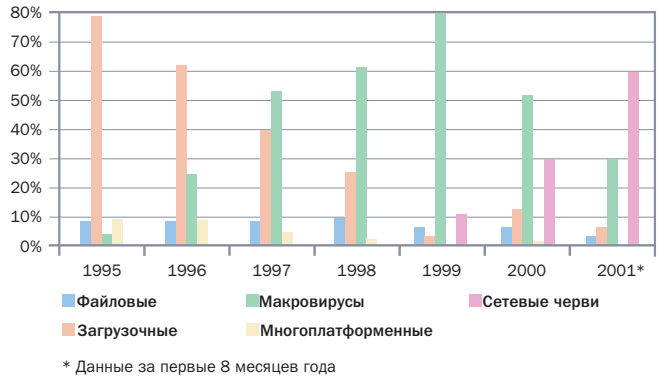
Виды вредоносных программ

С точки зрения компьютерной вирусологии все то, что в народе именуется «вирусами», правильно называть «вредоносными программами». Среди них выделяются три основных класса: компьютерные вирусы, сетевые черви и троянские программы.

Вирусы — это такая разновидность вредоносной программы, которая, попав в »



▲ Рис. 1. Количество зарегистрированных вирусных инцидентов



▲ Рис. 2. Наиболее распространенные типы вредоносных программ

» компьютер, начинает «размножаться», то есть внедрять свои копии в другие программы. Вирусы бывают разные: файловые (заражающие исполняемые файлы), загрузочные (заражающие загрузочные секторы), макро (написанные на макроязыках и заражающие, например, документы Word или Excel), скрипт (написанные на скрипт-языках) и т. д. Встречаются также многоплатформенные вирусы, например файлово-загрузочные.

Черви обладают способностью самостоятельно рассылаться по сетевым ресурсам (например, по электронной почте). Троянские программы не умеют ни того ни другого и засылаются на компьютеры непосредственно своими авторами.

В последнее время уже практически вымерли вредоносные программы, которые можно было бы отнести к одному из описанных типов. Сегодня они сочетают в себе два, а то и все три типа. Такие вредоносные программы называются многокомпонентными.

«Лучшие» показатели

История вредоносных программ насчитывает не один десяток лет. Еще в начале 70-х годов 20-го века в предшественнике Интернета, компьютерной сети ARPAnet, был обнаружен первый в истории вирус, получивший название Creeper. Журнал Virus Bulletin, связанный с одной из британских антивирусных компаний, уже многие годы ведет статистику вредоносных программ, регистрируя количество вызванных ими инцидентов, и публикует эти данные (табл. 1).

Что больше всего хочется узнать, когда речь заходит об общей вирусной статистике? Ну, конечно, Его имя. Имя самого страшного и разрушительного вируса, который принес компьютерному сообществу больше всего страданий. К удивлению многих, им оказался малоизвестный интернет-червь Naked.

Материальный ущерб

Вирусы наносят компьютерному сообществу колоссальный материальный ущерб, и недостатка в его экспертных оценках от действия вирусов сегодня нет.

Фантастические цифры, сравнимые с ВВП США и характеризующие небывалый размах вредительской деятельности компьютерных вирусов, можно увидеть на страницах многих авторитетных изданий, — как западных, так и российских (рис. 1). Например, исследовательская группа Information Week опубликовала цифру $1,6 трлн — именно во столько оценивается ущерб, причиненный мировой экономике в 2000 году вирусной и хакерской активностью.

Важно отметить, что предлагаемые цифры означают количество успешных вирусных атак, которым подверглись компьютерные субъекты. А это могут быть как домашние компьютеры, так и крупные корпорации, в инфраструктуре которых задействованы десятки и даже сотни тысяч рабочих станций. Так что, если вы видите цифру 66984 инцидентов в 2001 году, знайте: это более условное число, а реальное количество зараженных компьютеров многократно превосходит указанные значения и может исчисляться сотнями тысяч.

Прогнозы на будущее

В сентябре английская компания MessageLabs опубликовала результаты исследования статистики вирусных атак в Интернете. По их мнению, уже в 2013 году каждое второе электронное письмо будет содержать вредоносный код, а Интернет будет работать наполовину вхолостую, обслуживая рассылку всякой компьютерной заразы.

Однако далеко не все эксперты согласны со столь пессимистичным прогнозом. Как утверждает Евгений Касперский, руководитель антивирусных исследований компании «Лаборатория Касперского» (www.kaspersky.ru), это может произойти, только если все эксперты мира будут сидеть сложа руки и лишь подсчитывать количество вирусных атак: «Сегодня компьютерная вирусология сделала большой шаг вперед. Приятно осознавать, что в этом процессе Россия уверенно занимает ведущее место».

Как изменятся вредоносные программы в будущем? По данным Virus Bulletin (рис. 2), однозначно можно утверждать, что первое место по распространению займут сетевые черви, оттеснив на второй план другие разновидности вирусов.

Подводя итоги

По данным «Лаборатории Касперского» в 2001 году начали набирать обороты вредоносные программы, созданные специально для Linux. Так, в начале года сразу несколько разновидностей Linux-червей вызвали панику среди пользователей этой, до недавней поры казавшейся неуязвимой, ОС. Черви Ramen, Lion, Adore доказали, что в компьютерной индустрии пока не создано ПО, абсолютно защищенного от проникновения вредоносных программ.

В будущем электронная почта, Интернет и прочие сетевые ресурсы останутся и даже укрепят свои позиции в качестве наиболее опасных источников вирусной инфекции. »

Top 10

Название	Тип	Количество инцидентов	Доля от общего количества инцидентов, %
Naked	интернет-червь	19026	13,2
SirCam	интернет-червь	16713	11,6
ColdApe	макровирус	8858	6,2
Hybris	windows-вирус/интернет-червь	8440	5,9
MTX	windows-вирус/интернет-червь	6319	4,4
Navidad	интернет-червь	6008	4,2
Anna Kournikova	интернет-червь	4758	3,3
Ethan	макровирус	4509	3,1
Magistr	windows-вирус/интернет-червь	4318	3,0
Class	макровирус	4096	2,8

▲ Табл. 1. Самые распространенные по количеству зарегистрированных заражений вирусы

» Кроме того, вряд ли изменится пристрастие создателей вирусов к Windows и приложениям из состава MS Office. Это вполне понятно: чем больше популярность ПО, тем больше искушение различного рода маргиналов насолить ближнему своему и прославиться на геростратовом поприще. Однако та же участь постигла бы MacOS или Linux, будь они на месте Windows.

Скорее всего, в будущем вирусные эпидемии станут более продолжительными, а главным их возбудителем окажутся многокомпонентные вредоносные программы. На их фоне будут происходить частые, но непродолжительные вспышки простых и легко излечиваемых вирусов.

Компьютерный андерграунд все больше внимания обращает на бреши в системах безопасности ПО (например, Nimda, CodeRed). Действительно, сейчас уже мало кого можно провести с помощью известного трюка с вложенным файлом и привлекательным сопроводительным письмом. Даже новички с опаской относятся к подобным программам, помня известную притчу о бесплатном сыре и мышеловке. Через невидимую брешь червь может пробраться в компьютер абсолютно незаметно для пользователя.

Заключение

Хотелось бы еще раз призвать читателей регулярно устанавливать обновления к используемым операционным системам и приложениям. Они будут закрывать бреши в системах безопасности, и тогда уже никакой, использующий их, червь не попадет к вам в компьютер. Все эти обновления — бесплатны, а их установка (особенно для Windows) занимает не более пяти минут. К чему ждать, когда в вашем компьютере заведется какая-нибудь вредоносная программа?

Удачи в борьбе с вирусами!

■ ■ ■ Денис Зенкин

Naked и другие...

Житие и деяния

Naked

Обнаруженный в марте 2001 года Naked пошумел и быстро замолк. Правда, надо согласиться, что «пошумел» он действительно капитально и всего за полторы недели своего «буйства» по числу заражений смог обогнать всех конкурентов. Этот червь проникал в компьютеры под видом файла с интригующим названием Naked Wife («Голая женушка»).

Кстати, письма с якобы порнографическими фотографиями до сих пор остаются одной из самых эффективных «приманок», подкидываемых создателями вирусов наивным пользователям.

SirCam

Следующим в списке значится печально известный интернет-червь SirCam. Впервые появившись на горизонте в июле 2001 года, он повлек за собой одну из самых долгих эпидемий в истории Интернета. Червь не перестает терроризировать компьютеры во всем мире и по сей день. У него есть 8 вариантов текстов сообщений, а вложенные файлы вообще всегда имеют разные имена и размеры. Так что даже искушенный пользователь не всегда сможет его распознать.

Антивирусные программы уже много месяцев без проблем ловят эту заразу. Однако многие пользователи до сих пор не считают необходимым обзавестись антивирусной программой или просто забывают ее периодически обновлять.

ColdApe

В действительности этот макровирус проник в хит-парад Virus Bulletin нечестным путем. А все из-за того, что вредоносная программа каждый день рассылала свои копии с зараженных компьютеров на электронный адрес редактора Virus Bulletin Ника Фитцджеральда. Приходящее письмо содержало сообщение: «Dear Nicky... my name is [имя пользователя] and I want to make hot monkey love with you. You anti-virus stud!» («Дорогой Ники... Меня зовут [имя пользователя], и я хочу заняться с тобой любовью по-обезьяньи. Мой антивирусный жеребец!») Таким образом, один зараженный компьютер мог отослать в редакцию журнала огромное количество писем, и все они, конечно, считались отдельными сообщениями о заражении. Из-за этого в феврале 2000 года ColdApe удалили из вирусных чартов.

Happy

Известный интернет-червь Happy занимает лишь 10 место. В 1999 году мало кто мог предположить, что за поздравлением с Новым годом может скрываться вредоносный код. При запуске вложенного файла-носителя Happy действительно показывал красочный фейерверк, а сам тем временем незаметно заражал компьютер. Далее он просто рассылал себя от имени владельца зараженного компьютера по электронной почте. А новым получателям и в голову не могло прийти, что их коллега или знакомый может помимо своей воли подсовывать им интернет-червей.

Отдельно надо отметить присутствие в хит-параде таких сложных и опасных вредоносных программ, как Hybris, Magistr, MTX и Navidad. Это еще раз подтверждает факт, что, несмотря на то что такие «шедевры» появляются всего несколько раз в году, ущерб от них превосходит совокупный ущерб от всех прочих вирусов.