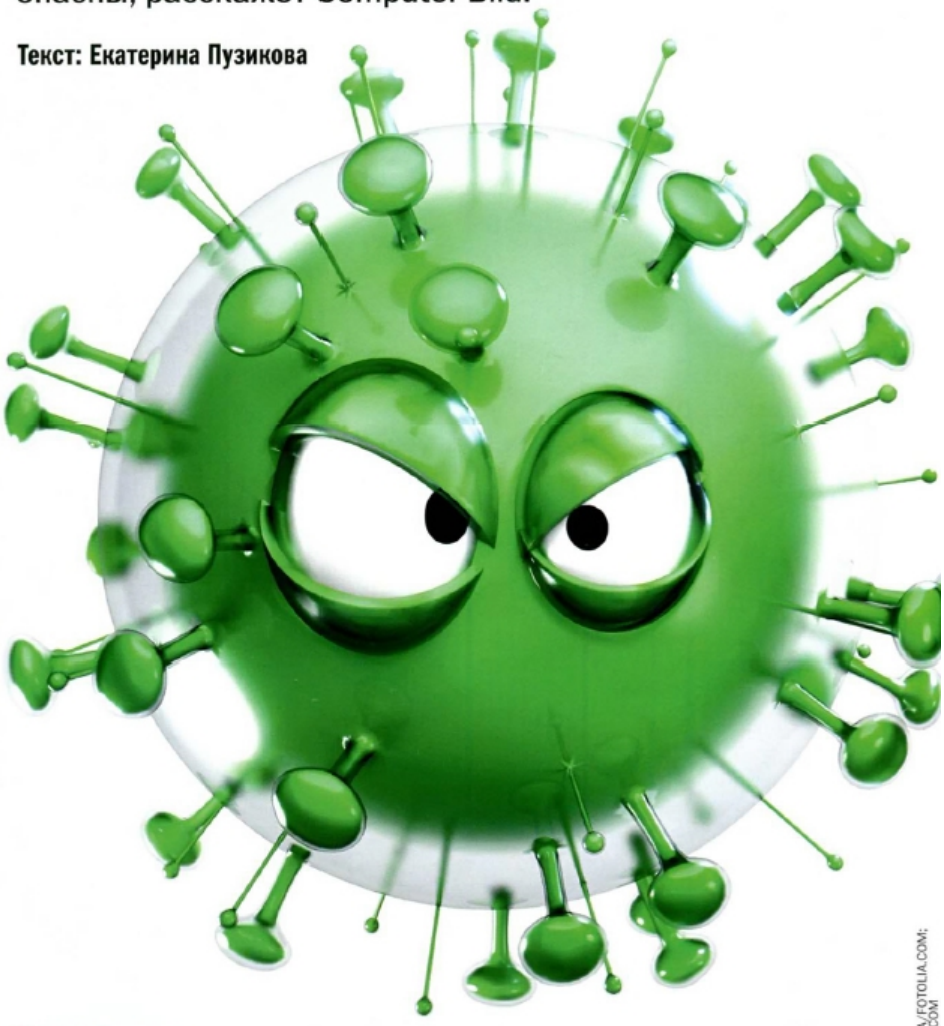
ТЕХНИЧЕСКИЕ

Компьютерный вирус способен наломать таких дров, что остается только хвататься за голову и ждать приезда технодоктора. О том, какими бывают вирусы и чем они опасны, расскажет Computer Bild.

Текст: Екатерина Пузикова



САМЫЙ ИЗВЕСТНЫЙ

Одним из самых известнейших вирусов, несомненно, можно считать CIH, или «Чернобыль».

Он был написан тайваньским студентом в июне 1998 года и работал только на Windows 95/98. 26 апреля 1999 года, в годовщину аварии на Чернобыльской АЭС, вирус активизировался и уничтожил данные на жестких дисках инфицированных компьютеров. На некоторых ПК было испорчено содержимое микросхем BIOS. Совпадение даты активации вируса и даты аварии на ЧАЭС дали вирусу второе название – «Чернобыль», которое в народе известно даже больше, чем CIH.

По разным оценкам – от вируса пострадало около полумиллиона персональных компьютеров по всему миру.

Классификация

Почти сорок лет назад, когда прототип интернета ARPANET уже существовал, группа людей устроила в сети своеобразные войны программ, разделившись на группы. Каждая из групп писала несколько программ под названием Creeper, чьей задачей было найти в сети крип-программу соперника и уничтожить ее, а также проникнуть в наибольшее количество ЭВМ и оставить там свою копию.

Технически крипер не являлся ни вирусом, ни опасной для здоровья ЭВМ программой, так как вреда системе не наносил. Тем не менее он положил начало так называемому компьютерному террору – и к настоящему моменту существует огромное количество вредоносного контента всех мыслимых форм и размеров.

Ниже мы расскажем об основных видах вредоносного ПО, готового поселиться на вашем компьютере.

Файловые вирусы

Эти пакостники стали одним из первых типов полноценных вирусов. Их задача – заразить исполняемые файлы на ПК,

ФОТО: КОМПАНИИ-ПРОИЗВОДИТЕЛИ; VIRINAFLORA/FOTOLIA.COM; LITLETROLL/FOTOLIA.COM; LITLETROLL/FOTOLIA.COM

БАЦИЛЛЫ

разрушая тем самым операционную систему, и по сети перепрыгнуть на другие компьютеры. Схема стара как мир, но навести порядок в хаосе, устроенном вирусом, очень и очень непросто. Сейчас подобные вирусы не столь актуальны, поскольку злоумышленники предпочитают еще и получать хороший доход от своих программ, примитивное заражение системных файлов их уже не интересует.

Блокираторы

Одно время этот тип вирусов получил широчайшее распространение. Представьте, вы ищете в сети рецепт борща, объявления о продаже спиннингов или что-то еще совершенно безобидное. Через часа два поисков вас заносит на какой-то сайт, где ежесекундно выскакивают десятки баннеров с рекламой. Вы кликаете на все подряд, лишь бы избавиться от этих назойливых штуковин, а в это время в ваш компьютер проникает вирус-блокиратор. В итоге поверх «Рабочего стола» вылезает огромный баннер с рекламой. Злоумышленники указывают в рекламе номер, на который следует отправить SMS, и вам якобы пришлют код для получения доступа к вашей же системе. Разумеется, за отправку SMS снимают приличные деньги, и вряд ли вам что-то пришлют в ответ.

Adware

Еще одно вредоносное ПО. Работе системы не мешает, но опасно тем, что может служить лазейкой для проникновения на компьютер более зубастых вирусов. Adware – это та самая реклама, которая есть на большинстве сайтов. Она может вылезти где угодно и когда угодно, причем без вашего согласия. Функционирует в основном в браузерах и выдает новое окно с рекламой онлайн-игры, лотереи или чего-то похожего. Несмотря на кажущуюся безобидность, благодаря Adware (особенно если посидеть на рекламном сайте подольше) можно легко «поймать», например, трояна.

Трояны

Вредоносное ПО, разработанное для кражи информации с компьютера жертвы. Логины, пароли, банковская и личная информация – большинство троянских программ воруют все, что только можно, и отправляют краденое своему разработчику. Подвидом троянов можно считать кейлоггеры – программы, которые фиксируют все нажатия клавиш и все действия пользователя за компьютером и опять-таки отправляют собранные сведения разработчику вируса.

Бэкдоры

Этот тип вирусов тоже можно считать подвидом троянов. Их задача – поставить компьютер жертвы под контроль разработчика вируса. В случае заражения бэкдором вирусописатель может не только воровать данные, но и управлять компьютером.

Боты

Еще одни представители семейства троянов, более продвинутые, чем бэкдоры. Установившись на компьютер, бот с помощью интернета вступает в контакт с разработчиком и другими зараженными компьютерами, сплетая, таким образом, огромную компьютерную сеть, называемую ботнетом. То есть разработчик вируса берет под контроль не один компьютер, а сотни и тысячи. Ботнеты могут использоваться для рассылки спама, проведения DDoS-атак или распространения других вирусов.

Вирусы-полиморфы

Пожалуй, это один из самых неуловимых вирусов. Секрет его в том, что, попадая на новую машину, вирус кардинально преображается, так что его очень трудно обнаружить. Сравнить полиморф можно разве что с вирусом гриппа, который меняется каждый сезон до неузнаваемости, хотя принцип действия его остается прежним.

Conficker

Один из опаснейших на сегодняшний день компьютерных червей. Написанный на Microsoft Visual C++, он впервые появился в сети 21 ноября 2008 года. Атакует операционные системы семейства Windows (от Windows 2000 до Windows 7 и Windows Server 2008 R2). На январь 2009-го поразил 12 миллионов компьютеров во всем мире. Типичный червь, паразитирует на системе и практически полностью заражает ее. Может распространяться через USB-накопители, создавая файл autorun.inf и файл RECYCLED\ {SID} \RANDOM_NAME.vmx. В системе хранится в виде dll-файла со случайным именем, состоящим из латинских букв. Conficker занимает третье место по нанесенному ущербу, уступая только почтовым червям MyDoom и I LOVE YOU.

НЕУЯЗВИМЫХ НЕ БЫВАЕТ

Многие считают компьютеры на Linux и Mac OS неуязвимыми для вирусов. Однако первый полноценный вирус был написан именно для Apple II.

Elk Cloner – один из первых вирусов, обнаруженный на компьютерах пользователей, а не в системе, на которой он был разработан. Был написан в 1981 году пятнадцатилетним школьником Ричардом Скрента для компьютеров Apple II.

Elk Cloner распространялся, заражая операционную систему DOS для Apple II, записанную на гибких дисках. После того как компьютер загружался с зараженной дискеты, автоматически запускалась копия вируса. Вирус не влиял на работу ПК, он лишь наблюдал за доступом к дискам. Когда выполнялся доступ к незараженной дискете, вирус копировал себя на нее – и так, шаг за шагом, завоевывал один плацдарм за другим.

Вирус не причинял вреда намеренно, хотя и мог повредить диски, содержащие нестандартный образ DOS, затирая резервные дорожки вне зависимости от их содержимого.