

# **5 самых опасных компьютерных вирусах**

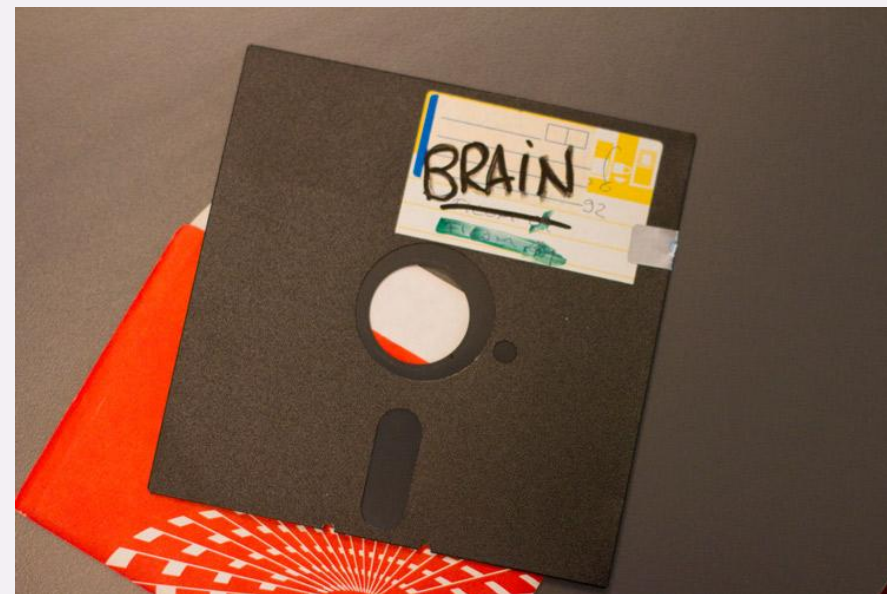
Работу выполнила ученица 11 "А" класса  
Тагакова Дарья

# Brain

19 января 1986 года ровно 30 лет назад появился первый компьютерный вирус Brain.

Вирус «Brain» был создан двумя братьями-программистами Амджат и Базит Алви из Пакистана в 1986 году. Первоначально он создавался как оружие против местных пиратов, ворующих созданное братьями программное обеспечение. Однако вместо этого программа стала распространяться и заражать десятки тысяч компьютеров по всему миру.

Brain записывался в загрузочные сектора дискет, а при сканировании компьютера он подставлял вместо зараженного сектора специально созданную нейтральную копию.



Амджат и Базит Алви

# ILOVEYOU

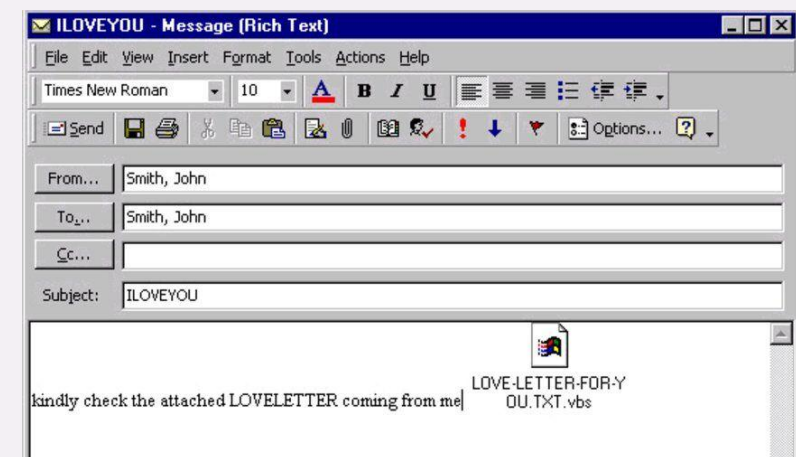
Вирус был разослан на почтовые ящики с Филиппин в ночь с 4 мая по 5 мая 2000 года.

ILOVEYOU — компьютерный вирус, успешно распространявшийся по электронной почте письмом с темой «ILOVEYOU» и вложением «LOVE-LETTER-FOR-YOU.TXT.VBS». После открытия вложения вирус рассылал себя по всем адресам из адресной книги, а также выполнял многочисленные изменения в операционной системе.

Ущерб, нанесённый созданным в 2001 году вирусом, составляет 10–15 миллиардов долларов. В честь данного события ILOVEYOU был занесён в книгу рекордов Гиннеса, как самый разрушительный компьютерный вирус в мире.

Червь ищет все подключенные диски и заменяет файлы с расширениями JPG, JPEG, VBS, VBE, CSS, WSH, JS, JSE, SCT, DOC, HTA, MP2 и MP3 на копии самого себя. Кроме того, он также добавляет расширение VBS, которое затем делает компьютер пользователя не загружаемым.

(автор неизвестен)

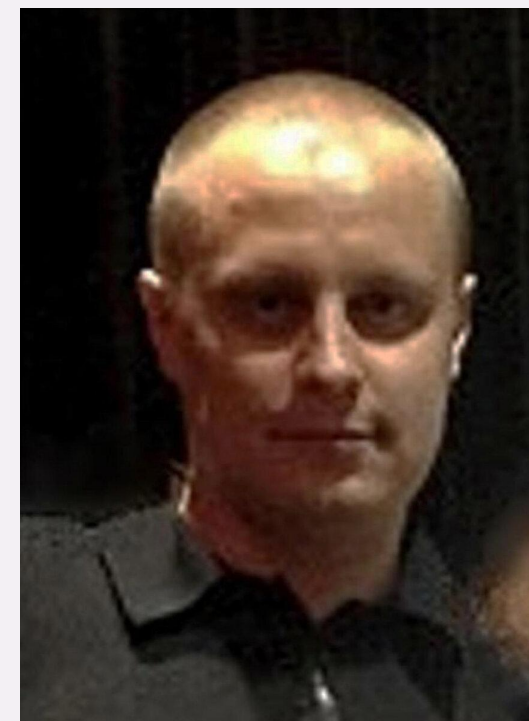




# Zeus Gameover

Zeus впервые был обнаружен в 2011 году. Это приложение представляет собой разновидность вредоносного программного обеспечения, нацеленного на операционную систему Microsoft Windows. Два основных метода заражения – спам-сообщения и скрытые загрузки. Основная цель Zeus Gameover – получить доступ к конфиденциальным реквизитам банковского счета жертвы и списать с него все средства. Вирус может обходить защиту централизованных серверных систем и сканировать личную информацию пользователя. Пользователи даже не могут отследить каналы, по которым уходят их украденные данные. Также в некоторых случаях Zeus может загрузить программу-вымогатель, шифрующую файлы и требующую денег в обмен на их разблокировку.

Создал российский хакер Евгений Богачев.



Евгений Богачев

# CodeRed

19 июля началась эпидемия сетевого червя Code Red, который атаковал американский Белый дом.

Червь Code Red был обнаружен двумя сотрудниками eEye Digital Security Марком Майффретом и Райаном Перме. Они назвали найденную вредоносную программу в честь любимой газировки Code

Red Mountain Dew. Появившаяся в 2001 году, она была нацелена на компьютеры с установленным веб-сервером Microsoft IIS. Проникая в компьютер, Code Red делает сотни копий всех данных и в конечном итоге потребляет так много ресурсов, что система не справляется и выходит из строя. Затем запускается алгоритм атаки "отказ в обслуживании" и открывается удаленный доступ к инфицированному серверу через бэкдор.

Интересный факт — Майффрет назвал Code Red в честь газировки со вкусом вишни, которая не давала ему уснуть ночами, пока он исследовал уязвимость Microsoft IIS.

Источником распространения червь считается город Макати (Филлиппины). Но это неточная информация (автор неизвестен)

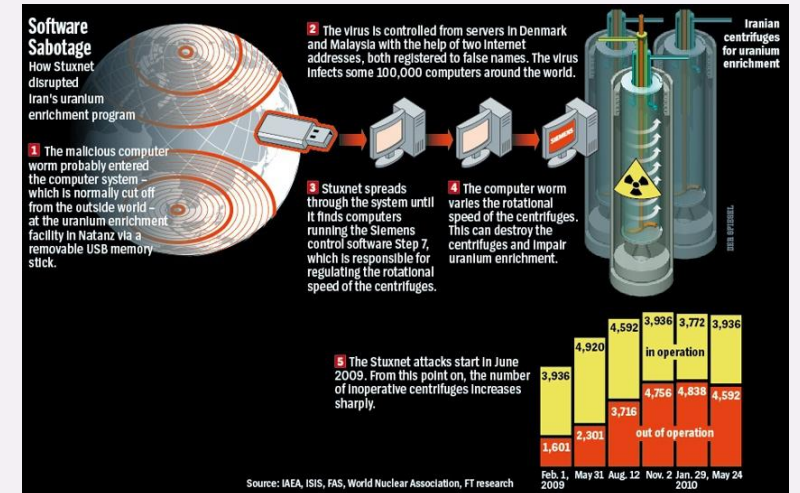
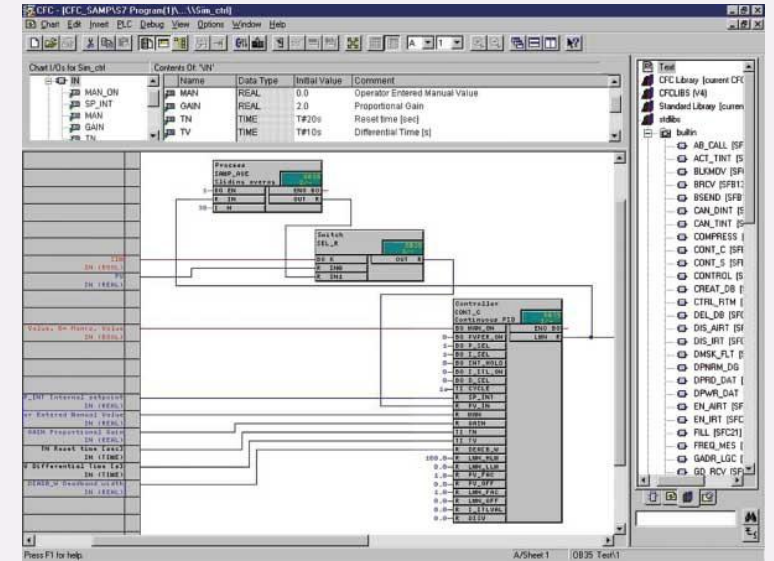


# Stuxnet

Большой, очень большой компьютерный червь (примерно в 10 раз больше обычного), ставший оружием промышленного шпионажа и диверсий. Впервые был замечен в 2010 году. Для своего быстрого распространения использовал уязвимость нулевого дня (уязвимость, которая не была еще обнаружена разработчиками ПО). Распространялся с помощью USB-флеш накопителей. Основной целью червя были программируемые логические контроллеры (ПЛК / PLC) от компании Siemens. ПЛК позволяет автоматизировать электромеханические процессы (линия сборки на предприятиях, к примеру).

Такими действиями Stuxnet смог нарушить работы и фактически вывести из строя 1000 центрифуг для обогащения урана. Это отбросило ядерную программу Ирана на несколько лет назад.

Точной информации о том, кто создал Stuxnet и для чего, нет. Однако многие считают Stuxnet общим творением США и Израиля, нацеленным именно на Иранскую ядерную программу. Поскольку по статистическим данным именно Иран пострадал больше всех (58.85%)





# Заключение

Никто не любит вирусы, червей и троянов (кроме их создателей, конечно). Но невозможно недооценивать их вклад в развитие технологий, а именно систем безопасности. Ведь не имея противника, достойного Вам противостоять, Вы не будете развиваться, чтобы побороть его. И последнее, не забывайте обновлять свой антивирус.

