

***Эволюция компьютерных вирусов**

Автор: Уваркин Максим

*Компьютеры стали настоящими помощниками человека и без них уже не может обойтись ни коммерческая фирма, ни государственная организация. Однако в связи с этим особенно обострилась проблема защиты информации.

*Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность.

* Вирус - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но, и могут вообще с ним не совпадать! Вирус не может существовать в «полной изоляции»: сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

* Пути проникновения вируса

* Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода А и перезагрузили компьютер, при этом дискета может быть и не системной. Заразить дискету гораздо проще. На нее вирус может попасть, даже если дискету просто вставили в дисковод зараженного компьютера и, например, прочитали ее оглавление.

- * При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов.
- * К ним можно отнести следующие:
 - * -прекращение работы или неправильная работа ранее успешно функционировавших программ;
 - * -медленная работа компьютера;
 - * -невозможность загрузки операционной системы;
 - * -исчезновение файлов и каталогов или искажение их содержимого;
 - * -изменение даты и времени модификации файлов;
 - * -изменение размеров файлов;
 - * -неожиданное значительное увеличение количества файлов на диске;
 - * -существенное уменьшение размера свободной оперативной памяти;
 - * -вывод на экран непредусмотренных сообщений или изображений;
 - * -подача непредусмотренных звуковых сигналов;
 - * -частые зависания и сбои в работе компьютера.

*История появления и эволюции компьютерных вирусов, сетевых червей, троянских программ зародилась в 1980-х годах. Примитивные вирусы постепенно превращались в сложные технологические разработки, осваивали новые ниши, проникали в компьютерные сети.

- * Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.
- * Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

- *Идея вируса, заражающего другие программы и компьютеры, за двадцать лет трансформировалась в криминальный бизнес.
- *Будучи изначально творчеством вирусологов-исследователей, компьютерные вирусы стали оружием в руках интернет-преступников.

* Появившись в конце 1980-х, первые антивирусные разработки получили большую популярность, через 10 лет став обязательным к использованию программным обеспечением.

Вирусы 1980-1986х годов

Компьютеры становятся всё более и более популярными. Появляется всё больше и больше программ, авторами которых являются не фирмы-производители программного обеспечения, а частные лица. Развитие телекоммуникационных технологий даёт возможность относительно быстро и удобно распространять эти программы через серверы общего доступа – BBS (Bulletin Board System).

* «Глобальная сеть» серверов BBS становится популярной и в результате привлекает внимание программистов-хулиганов. Появляется большое количество разнообразных «троянских коней» — программ, не имеющих способности к размножению, но при запуске наносящих системе какой-либо вред.

*Фред Козн, родоначальник компьютерной вирусологии того времени, на семинаре по компьютерной безопасности в Лехайском университете (США) демонстрирует на системе VAX 11/750 вирусоподобную программу, способную внедряться в другие объекты.

* Годом позже, на 7-й конференции по безопасности информации, он дает научное определение термину «компьютерный вирус» как программе, способной «заражать» другие программы при помощи их модификации с целью внедрения своих копий

- * Зарегистрирована первая глобальная эпидемия вируса для IBM-совместимых персональных компьютеров. Вирус Brain, заражающий загрузочные сектора дискет, в течение нескольких месяцев распространился практически по всему миру
- * Причина такого «успеха» заключалась в полной неподготовленности компьютерного общества к встрече с таким явлением, как компьютерный вирус: антивирусных программ просто не было, а пользователи, в свою очередь, ничего не знали о новом компьютерном бедствии.

- * Для защиты от вирусов можно использовать:
- * -общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- * -профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- * -специализированные программы для защиты от вирусов.

* Происходят изменения и в антивирусной индустрии. Корпорация Microsoft активно готовится к выходу на антивирусный рынок и покупает сразу две антивирусные компании. 8 февраля 2005 объявляет о покупке компании Sybari, а 20 июля объявлено о покупке FrontBridge Technologies

Спасибо за внимание