**Червь Морриса:**

**Вступление:**

Червь Морриса - Один из первых сетевых червей, распространявшихся через Интернет. Написан аспирантом Робертом Моррисом и запущен 2 ноября 1988 года в Массачусетском технологическом институте. По словам Морриса, он хотел оценить размер сети Интернет - APRANET (компьютерная сеть, созданная в 1969 году в США Агентством Министерства обороны США - прототип сети Интернет). Подошел он к этому основательно - написал сложную программу, которая способна самостоятельно распространяться по сети и препятствовать попыткам ее остановить. Червь Морриса не причинял какого-либо вреда системе, но ошибка в программе приводила к тому, что многие компьютеры запускали червя десятки раз, что перегружало сервер, делая его, по сути, неработоспособным.

**Как заражал:**

Во-первых, уязвимости реализации Finger и Sendmail в популярных UNIX-системах того времени позволяли запустить на удаленном компьютере произвольный код. (Суть воздействия сводилась к тому, чтобы подменить исходный текст письма, отправляемого тогда еще в сети APRANET, с удалением заголовков и окончаний в отладочном режиме Sendmail ИЛИ при переполнении буфера сетевого fingerd-сервиса. Первая часть в новом письме содержала код, компилированный на удаленном терминале, а третья состояла из такого же бинарного кода, но адаптированного под разные компьютерные системы.)

Во-вторых, если эти варианты не проходили, червь пытался подключиться к rsh - консоли удаленного администрирования. Правда, для этого требуется пароль, но червь его подбирал. Весьма впечатляет, что большой процент успешно подобранных паролей был достигнут при помощи словаря всего в 400 слов, плюс несколько очевидных вариантов, таких как пароль, совпадающий с именем пользователя или составленный из тех же букв в обратном порядке.

**Как работал:**

Проникнув на компьютер, червь менял имя своего процесса, удалял временные файлы, каждые три минуты ветвился(использовал fork()) и принимал еще ряд мер, препятствующих своему обнаружению, в частности шифровал свои данные в памяти. Запускаясь на новом компьютере, червь проверял, не является ли компьютер уже зараженным. При обнаружении двух копий на компьютере они «играли в кости», и одна самоуничтожалась. То ли из-за ошибки Морриса, то ли для страховки от создания простой «вакцины», основанной на этом эффекте, в одном случае из семи новая копия переставала играть «в выживание» и продолжала работать при любых условиях. Именно это решение привело к DDoS-эффекту, коэффициент 1/7 оказался слишком большим, и многие компьютеры повторно заражались десятки раз.

**Как боролись:**

Для разбирательства с угрозой пришлось спешно создавать рабочие группы программистов и администраторов в МТИ и Беркли, буквально за два дня были определены и заблокированы «лазейки», через которые червь проникал в систему, а код заразы был целиком уничтожен.

**Последствия:**

Червь Морриса, парализовавшего работу более шести тысяч интернет-узлов ARPANET, к которой, кстати, были подключены и правительственные, и военные организации.

Несмотря на это, на устранение последствий заражения, по разным оценкам, было потрачено от 100 тысяч до 10 млн долларов. Сам ущерб оценивают порядка 96,5 миллиона долларов США.

Интересно, что принятые Моррисом меры конспирации могли бы помочь ему остаться анонимным. Но в дело вступил отец, тоже Роберт Моррис. Соавтор операционной системы UNIX и директор по исследованиям Национального центра компьютерной безопасности при АНБ убедил сына во всем признаться. Суд, состоявшийся в 1991 году, учел этот факт и вынес Моррису довольно мягкий приговор: 3 года условно, штраф 10 тысяч долларов и 400 часов общественных работ.

**Итоги:**

Эпидемия показала, как опасно безоговорочно доверять компьютерным сетям. Впоследствии были выработаны новые ужесточённые нормы компьютерной безопасности, касающиеся безопасности кода программ, администрирования сетевых узлов и выбора защищённых паролей.

К сожалению, такие норма не помогли и как показывает практика, людей, которые пишут такие программы не остановить. Пример:

1)Появился «троянский конь» AIDS - 1989(Вирус делал недоступной всю информацию на жестком диске и высвечивал на экране лишь одну надпись: «Пришлите чек на $189 на такой-то адрес»)

2)Почтовый вирус Melissa (1999) вызвал эпидемию мирового масштаба, поразил десятки тысяч компьютеров и нанес ущерб в $80 млн.

3) Рекорд Melissa побил почтовый вирус I Love You! (2000), поразивший миллионы компьютеров в течение нескольких часов.