**Червь Морриса:**

**Вступление:**

(2 слайд) 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 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. Тем не менее Моррис на всякий случай конспирировал не только вторжение вируса в систему каждого компьютера, но и сам запуск вируса: он запустил его с внутренней компьютерной системы Массачусетского технического института, рассчитывая на то, что при возможном последующем расследовании подозрение падет на студентов этого института, в то время как сам Моррис учился в тот момент в Корнелльском университете.

**Как заражал:**

(3 слайд) Структурно червь состоял из трех частей — «головы» и двух «хвостов». «Голова» представляла собой исходный текст на языке C (99 строк) и компилировалась непосредственно на удаленной машине.

«Голова» забрасывалась при помощи следующих методов:

* использование отладочного режима в sendmail;
* использование уязвимости типа «переполнение буфера» в сетевом сервисе Finger;
* вызов удаленного командного интерпретатора (rsh) путем подбора логина и пароля.

(4 слайд) Sendmail — самый старый сетевой сервис, обрабатывающий прием и отправку почты по протоколу SMTP. Во времена распространения червя, в Sendmail имелась недокументированная возможность — разработчиками был запрограммирован отладочный режим, который не должен был находится в рабочей версии программы и был оставлен по ошибке. Одна из возможностей отладочного режима заключалась в том, чтобы почтовое сообщение обрабатывалось не самим Sendmail, а другой программой.

Пример почтового сообщения, отправляемого червем вы можете видеть на слайде.

Как видно, из тела письма убирались заголовки (при помощи текстового препроцессора sed) и производилось сохранение файла исходного кода «головы». Далее командному процессору давались инструкции на компилирование кода «головы», запуск получившегося исполняемого файла и стирание временных файлов.

(5 слайд) На слайде представлена лазейка используемая для доступа к системе с помощью Finger – сетевой протокол осуществляющей поиск информации о пользователях. Вы можете видеть часть кода написанного для срыва стека на си.

Доступ к системе с помощью Finger червь получал через уязвимость в функции gets() библиотеки libc, используемой демоном для чтения запроса с удаленной машины. Червь передавал демону 536 байт в буффер, чем вызывал срыв стека и передачу управления шелл-коду.

На самом деле червь выполнял не что иное, как строку execve("/bin/sh", 0, 0) на языке си, то есть открытие доступа к командной строке. Далее, как и в предыдущем случае, червь загружал на машину исходный код своей «головы» и исполнял его. Это срабатывало только для компьютеров VAX с установленной ОС 4.3BSD, на компьютерах SUN под управлением SunOS данной уязвимости не было.

(6 слайд) Если эти варианты не проходили, червь пытался подключиться к rsh - консоли удаленного администрирования. Для использования метода распространения rsh - собирался список пользователей локальной машины. На его основе производился подбор наиболее часто используемых паролей, в надежде что многие пользователи имеют одинаковые имена и пароли на всех машинах в сети, что впрочем оказалось недалеким от истины.

При подборе червь пробовал следующие варианты паролей:

* пустой;
* имя пользователя (user);
* имя пользователя, написанное наоборот (resu);
* двойной повтор имени пользователя (useruser);
* имя или фамилия пользователя (John, Smith);
* имя или фамилия пользователя в нижнем регистре (john, smith);
* (7 слайд) встроенный словарь размером 432 слова;

На слайде вы можете заметить пример команды rsh. Тут происходит добавление файла worm хранящегося на локальной машине к файлу lizard.file хранящемуся на удаленной машине lizard

(8 слайд)

**Как работал:**

Комплексное использование нескольких методов распространения значительно повлияло на массовое распространение червя в сети.

Червь использовал несколько приемов для затруднения своего обнаружения администраторами компьютеров:

* удаление своего исполняемого файла после запуска;
* отключались все сообщения об ошибках, а размер аварийного дампа устанавливался в ноль;
* исполняемый файл червя сохранялся под именем sh, такое же имя использовалось командным интерпретатором Bourne Shell, таким образом, червь маскировался в списке процессов;
* примерно каждые три минуты порождался дочерний поток, а родительский завершался, при этом происходило постоянное изменение pid процесса червя и обнулялось время работы, показываемое в списке процессов;

Также стоит отметить, что 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. Из-за ошибки Морриса 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.

(9 слайд)

**Как боролись:**

Для разбирательства с угрозой пришлось спешно создавать рабочие группы программистов и администраторов в MIT и Бёркли, буквально за два дня были определены и заблокированы «лазейки», через которые червь проникал в систему, а код заразы был целиком уничтожен. Нужно понимать, что многие машины заражались повторно, нагрузка на системы и сеть увеличивалась и становилась весьма ощутимой, часто приводящей к отказу в обслуживании, в результате чего червь собственно и был обнаружен и обезврежен намного быстрей, чем если бы повторных заражений не было.

(10 слайд)

**Последствия:**  
Несмотря на «грандиозность» задумки, червь имел в себе некоторые ошибки, как проектирования, так и реализации. Именно неправильно реализованный алгоритм проверки, не является ли система уже зараженной, привел к массовому распространению червя в сети, вопреки задумке его автора. На практике, компьютеры заражались многократно, что, во-первых, приводило к быстрому исчерпанию ресурсов, во-вторых — способствовало лавинообразному распространению червя в сети. По некоторым оценкам червь Морриса инфицировал порядка 6200 компьютеров. Сам разработчик, осознав масштабы результатов своего поступка, добровольно сдался властям и обо всем рассказал. Слушанье по его делу закончилось 22 января 1990 года. Изначально Моррису грозило до пяти лет лишения свободы и штраф в размере 25 тысяч долларов. В действительности приговор был достаточно мягок, суд назначил 400 часов общественных работ, 10 тысяч долларов штрафа, испытательный срок в три года и оплату расходов, связанных с наблюдением за осужденным. 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.

(11 слайд)

**Мораль:**

Данная эпидемия наглядно 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.

Инцидент с «червем Морриса» заставил специалистов в области IT серьезно задуматься о вопросах безопасности и качественном тестировании, в частности именно после этого случая для повышения безопасности системы стало внедряться использование пауз после неправильного ввода пароля и хранение паролей в /etc/shadow, куда они перенесены из доступного на чтение всем пользователям файла /etc/passwd.

Но наиболее важным событием стало создание в ноябре 1988 года координационного центра CERT, деятельность которого связана с решением проблем безопасности в Интернете.

(12 слайд)

К сожалению, такие нормы 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.

Примечательно, что многие технические решения, используемые «червем Морриса», такие как использование перебора паролей, компиляция кода загрузчика на удаленной ЭВМ под управлением \*NIX систем, сканирование сети для выявления целей и т.д. применяются и в современных образцах вредоносного программного обеспечения.

(13 слайд)

И напоследок — в 1988 году, будучи под впечатлением от атаки червя Морриса, американская Ассоциация компьютерного оборудования объявила 30 ноября международным Днем защиты информации (Computer Security Day), который отмечается и по сей день.

(14 слайд)

На этом все, спасибо за внимание!