# The Case of the Phantom Game Enthusiasts

## INCIDENT STATISTICS

Date: 9-MAY-1983  
Hours: 1530 - 2030 MDT  
Systems: Los Alamos ICN - MX G (VMS) and Telenet  
Accounts: GATE (all SYSTEM privileges are accessible)  
DEMO (normal privileges - bare necessities)  
Suspects: Two Telenet Users  
One identifier of John Hoinacki  
Direct Involvement: Gary C. White, LANL Employee, LS-6, 7-2914  
(ICN user conversing with suspects)  
Interviewer: Charlene Douglass, OS-4, 7-4844  
Interviewees: John Davis, Mary Maestas, C-8, 7-7038  
Gary White, LS-6, 7-2914  
Martin Kellog, C-5, 7-3310  
Art Walker, C-5, 7-3310  
Additional Consultees: Glen Carter, C-8  
Kathryn Berkbigler, C-8

## INCIDENT DESCRIPTION

On 9 May 1983 at 1734 hours MDT, (b)(6) received a message on his terminal from the DEMO account inquiring about games on the system. A brief conversation was entered into between (b)(6) and DEMO. At 1838 hours MDT, an inquiry was initiated from the GATE account to the DEMO account requesting information on the PHONE utility and the UNIX operating system. Another brief conversation was entered into between (b)(6) and DEMO directed towards explanations of the previous subjects and Arpanet. At 1910 hours MDT, an iquiry was initiated from the DEMO account to the DEMO account. The subject was John Hoinacki. The question was "John, when are you going to start work?" At 1917 hours, MDT, user (b)(6) asked DEMO how they accessed the machine. The DEMO account had previously inquired where this machine was geographically located. (b)(6) replied to DEMO that "this machine is at Los Alamos National Laboratory in New Mexico", and that user DEMO was obviously doing something he shouldn't, so the session should be terminated. (This occurred at 1927).

***The above description was derived from the hardcopy log of partial conversations between the three users. We only have verifiable copy of the conversations from the DEMO Mail file.***

At 1922 hours MDT, same date, user (b)(6) sent mail to user (b)(6) describing the current events. He also sent mail to the SYSTEM account describing the same events on the morning of 10 May at 0906. **I have in my possession, a hardcopy of both messages.**

Upon receipt of the information, Mary Maestas, C-8, immediately changed the passwords on both accounts, contacted Art Walker of C-5 to verify telenet access and assess account status. Walker did some checking and verified the telenet access. An account named GATE belonging to Martin Kellog of C-5, that had all system privileges. was used for this access.

le checking, both Maestas and Walker encountered Dennis Perry, C-5, the hallway, once again verified telenet access, and discussed "areas of responsibilities". Charlene Douglass of OS-4 learned of this incident on 17 May in the PM.

An inquiry was made to TELENET SECURITY (Lee Brand) regarding tracing procedures. On May 26, 1983, a memo was sent to Telenet requesting their assistance in determining the origin of Telenet access to our system on 9 May, 1983. Telenet replied on 7 June, 1983 stating that the accesses originated in St. Petersburg, Florida. No other information could be obtained from the logging records they sent us.

Using the one identifier (Hoinacki) that we had, I called information in the St. Petersburg area, and found that there was one phone assigned to the name Hoinacki in the area but it was unlisted. This information was passed on to the FBI.

Investigation of this incident revealed an apparent "lack of knowledge" on the part of the suspects in reference to geographical sign-on location and operating system knowledge.
There have been several unsuccessful attempts to gain access to those same accounts and also one additional account since the incident on 9 MAY.
After investigation of this incident,
is my personal opinion that no damage was caused and the users were king for games.

It is my understanding, at this time, that the FBI is trying to determine whether or not they should open a case.

```
IDG   u 089207
@PORT 45107 ON g: @138 1983-05-18 14:20:57
MMg DP ACCESS LINE  05

DPs available:
    DP2   ADPDP3   ESSDP1   ESSDP2   G         MERLIN   MFE      MPDP0
    AX    PNLB     QVAX1    QVAX2    S1VAX

DP name: G

Username: 089207
Password:
        Welcome to VAX/VMS version V3.2 on node G

$ mail

MAIL> 1
                                                                    MAIL #1
From:         (b)(6)           9-MAY-1983 19:22
To:
Subj:     Unauthorized users


I have repeatedly received mail from two users named GATE and DEMO.
They don't know what state (????) this machine is in, and are asking
questions about games, etc.
They have mentioned telenet, which leads me to believe they have gained
--cess to the machine via telenet.
    users command does not currently show any other users than myself.
   y ideas about what is going on?????????????

MAIL> 2
                                                                    MAIL #2
  om:         (b)(6)           9-MAY-1983 20:31
To:
Subj:     Follow-up on DEMO

User DEMO is logged on through NVA39

MAIL> exit
$ lo\dl\sho sys/bat
   VAX/VMS V3.2    Processes on 18-MAY-1983 14:23:40.95    Uptime 18 21:51:31
    Pid     Process Name       UIC   State Pri Dir. I/O     CPU        Page flts Ph.Mem
  00ED0010 _JOB397           001,004 CUR     5     1759 00:05:13.11      2022    93 B
  01760014 _JOB395           334,003 COM     1      101 00:03:44.98      1449   242 B
  01C80016 _JOB396           206,003 COM     1      144 00:02:50.91      2934  1164 B
  021C0019 _JOB394           334,003 COM     3       37 00:20:28.63      7682   180 B
$ lo
  089207         logged out at 18-MAY-1983 14:24:43.89
OFF ICN
PORT 45107 ON g: CHARS IN 00068 (ERR 00000), CHARS OUT 02021
@138 1983-05-18 14:23:57
```

```
[illegible] STEM MANAGER [illegible] DAIN.COM

  145                                                              MAIL #145

FROM:    (b)(6)                10-MAY-1983 09:06
TO:      SYSTEM
SUBJ:    UNAUTHORIZED USERS

TWO USERS WERE ON G LAST EVENING WHO DIDN'T EVEN KNOW WHAT STATE
THEY WERE IN????
THEY REPEATEDLY SENT ME MAIL ASKING QUESTIONS ABOUT GAMES, ETC.
THE USER NAMES WERE GATE AND DEMO.
HOW DID THEY GAIN ACCESS TO THIS MACHINE?? VIA TELENET????
I LEFT ADDITIONAL DETAILS IN MAIL TO U892UY LAST EVENING.

MAIL  146                                                          MAIL #146

FROM:    (b)(6)                10-MAY-1983 09:16
TO:      SYSTEM
SUBJ:    RE: UNAUTHORIZED USERS

THEY DIDN'T DIAL INTO G, SINCE THE TERMINAL ID WAS NVA39 OR
SOMETHING LIKE THAT.

MAIL  EX
```

yes

Says This IS A TELENET

PSEUDO TERMINAL

```
 D 067061
 .WHITE                       [207,001] 5606F232 NORMAL   4 DPB:[067061]
```

DEMO was DEMO - DEMO — STANDARD DEC Release

GATE was GATE - GATE

Martins account had set Prev

Martin going to get regular account.

Check at Telenet Customer Service 18 May 1983 1630.

Gale Dixon etc [illegible]

56566

```
    Owner                 Username             UIC       Account   Privs  Pri Default Directory

                                             [200,014]  8008X35T  All      4  DRB3:[070926]
                                             [200,012]  8008X35T  All      4  DRB3:[075836]
                                             [200,215]  8008X35T  All      4  DRB3:[076308]
                                             [200,002]  8008X35T  All      4  DRB3:[079395]
                                             [237,001]  8108A459  All      4  DRB3:[080793]
                                             [210,001]  8010X33C  All      4  DRB3:[081937]
                                             [200,017]  8008X35T  All      4  DRB3:[083847]
                 (b)(6)                      [200,014]  8008X35T  All      4  DRB3:[084802]
                                             [210,011]  8010X33C  All      4  DRB3:[086103]
                                             [202,010]  8008X35T  All      4  DRB3:[086525]
                                             [200,022]  8008X35T  All      4  DRA1:[089207]
                                             [336,001]  8005X34P  All      4  DRB3:[089596]
                                             [103,002]  8008X35T  All      4  DRB3:[FRASER]
                                             [200,034]  8008X33T  All      4  DRB3:[090207]
                                             [103,002]  8008X35T  All      4  DRB3:[130556]
 DEFAULT                  A1                 [007,052]  8008X35T  All      4  DISK$CDIV:[A1]
 DEFAULT                X ALLIN1             [007,050]  8008X35T  All      4  DISK$CDIV:[ALLIN1]
                 (b)(6)                      [213,001]  8008X35T  All      4  DBA0:[CHORN]
 Field Service            FIELD              [001,010]  8008X35T  All      4  SYS$SYSROOT:[SYSMAINT]
 XNET GROUP               GATE               [310,310]  8008X35T  All      4  SYS$SYSDEVICE:[GATE]
 DEFAULT                  HAWKINS            [336,002]  8008X35T  All X    4  DRB3:[HAWKINS]
 INTERACTIVE              INTER              [222,222]  8008X35T  All      4  DRB3:[INTER]
 SYSTEM                   OP                 [020,001]  8008X35T  All      4  DRA1:[OP]
 System Manager           SYSTEM             [001,004]  8008X35T  All      4  SYS$SYSROOT:[SYSMGR]
 SYSTEST-UETP             SYSTEST            [001,007]  8008X35T  All      4  SYS$SYSDISK:[SYSTEST]
 N.GOW/C-10               TOOLS              [011,100]  8010X33C  All      4  DRA1:[TOOLS]
                                             [206,001]  9508X895  Devour   4  DRB3:[081856]
                                             [210,005]  8010X33C  Devour   4  DRB3:[084236]
                                             [231,001]  95500000  Devour   4  DRB3:[086632]
                                             [210,025]  8010X33C  Devour   4  DRB3:[089280]
                                             [210,015]  8010X33C  Devour   4  DRB3:[092618]
                (b)(6)                       [200,023]  8010X32C  Devour   4  DRB3:[092798]
                                             [210,006]  8010X33C  Devour   4  DRB3:[093619]
                                             [234,001]  8010X33L  Devour   4  DRB3:[093665]
                                             [200,046]  8008X33T  Devour   4  DRB3:[095045]
                                             [224,001]  8008X35T  Devour   4  DRB3:[AL]
 DEMO                     DEMO               [300,300]  8008X35T  Devour   4  DRB3:[DEMO]
                (b)(6)                       [307,001]  8008X35T  Devour   4  DRB3:[DPTEST]
 SYSTEM MANAGER           GUEST              [300,300]  8008X35T  Devour   4  DRB3:[GUEST]
 DEFAULT                  FTPUSER            [007,007]  8008X35T  Devour   4  DRB3:[FTPUSER]
 SYSTEM                   SPOOLER            [001,004]  8008X35T  Devour   4  SYS$SYSDEVICE:[CDIV]
 DEFAULT                  TEMP               [350,001]  8008X31A  Devour   4  DRB3:[TEMP]
 CLASS                    USER10             [323,001]  8010X32C  Devour   4  DRB3:[USER10]
 CLASS                    USER11             [323,002]  8010X32C  Devour   4  DRB3:[USER11]
 CLASS                    USER12             [323,003]  8010      Devour   4  DRB3:[USER12]
 CLASS                    USER13             [323,004]  8010X     Devour   4  DRB3:[USER13]
 CLASS                    USER14             [323,005]  8010X32C  Devour   4  DRB3:[USER14]
```

```
Y-1983 20:24    LPA0:   9-MAY-1983 20:24    DISK$CDIV:[DEMO]MAIL.MAI;1                          VAX/VMS
Y-1983 20:24    LPA0:   9-MAY-1983 20:24    DISK$CDIV:[DEMO]MAIL.MAI;1                          VAX/VMS
Y-1983 20:24    LPA0:   9-MAY-1983 20:24    DISK$CDIV:[DEMO]MAIL.MAI;1                          VAX/VMS


EEEEE  M   M   OOO
E      MM MM  O   O
E      M M M  O   O
EEEE   M   M  O   O
E      M   M  O   O
E      M   M  O   O
EEEEE  M   M   OOO


IIII    LL
IIII    LL
II      LL
II      LL
II      LL
II      LL
II      LL
II      LL
II      LL
II      LL
II      LL              ....
II      LL              ....
IIII    LLLLLLLLLL      ....
IIII    LLLLLLLLLL      ....


IIII        ;;;;        11
```

```
From:     (b)(6)          9-MAY-1983 17:34
To:       DEMO
Subj:     RE: hi

Games are on UNIX.  I don't know of any here!!!!
```

From: (b)(6) 9-MAY-1983 18:27
To: DEMO
Subj: RE: UNIX

UNIX does not have a telenet address, only arpanet.
Try software tools whois!
Phone only works on VT100 terminlals.
You can raeally mess up a n interactive session by forcing a phone message
onto a terminal in plot mode.

```
From:     GATE                 9-MAY-1983 18:38
To:       DEMO
Subj:     help

HOW DO I USE PHONE AND WHAT IS THE UNIX?
```

From:     (b)(6)          9-MAY-1983 18:50
To:       DEMO

You can't use backspaces to correct errors on VMS. Use DEL or RUBOUT
instead.
I colldn't understand your previous message.

From: (b)(6) 9-MAY-1983 18:53
To: DEMO
Subj: UNIX

UNIX is the Bell Telephone operating system developed for the PDP-11 originally.
It is running on MX A, and requires access through the ICC.
No dial -in capabilities are available except through the ICN.
Arpanet is another computer network much like telenet.
It originated through DoD.

```
From:   DEMO              9-MAY-1983 19:10 *
To:     DEMO
Subj:   john hoinacki

john when are you going to start work??? i will probably start the 16th.
```

```
From:      (b)(6)                9-MAY-1983 19:17
To:        DEMO
Subj:      STATE?

How did you get on this machine????????
If I were on a vt-100 terminal, I could phone you, but am not.
Hence, you chat via mail.
.
```

From:    (b)(6)    9-MAY-1983 19:27
To:      DEMO
Subj:    RE: STATE?

This machine is at Los Alamos National Laboratory, in NM.
Obviously you are doing something you shouldn't be, so better cool it.

Los Alamos

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

|  |  |
|---|---|
| DATE: | May 26, 1983 |
| IN REPLY REFER TO: | OS-DO-83-763 |
| MAIL STOP: | F677 |
| TELEPHONE: | (505) 667-5911 |

Mr. Lee Brand
Manager, Network Security
8229 Boone Blvd.
Vienna, Virginia 22180

Dear Mr. Brand:

As discussed in the telephone conversations of May 19 and 25, 1983, we are requesting your assistance in determining the origin of Telenet access to network address 50560 or 50561 on May 9, 1983, between 1530 and 2030 hours Mountain Daylight Time. Access was gained to critical files at this time.

Additional attempts have been made on the following dates and times:

| Date | Time (MDT) |
|---|---|
| May 10, 1983 | 1050 |
|  | 1051 |
|  | 1451 |
|  | 1452 |
|  | 1453 |
|  | 1456 |
|  | 1524 |
|  | 1555 |
|  | 2024 |
| May 11, 1983 | 1537 |
|  | 1655 |
| May 18, 1983 | 1428 |
|  | 1601 |

An Equal Opportunity Employer/Operated by University of California

| Date | Time<br>(MDT) |
|---|---|
| May 19, 1983 | 1331<br>1924 |
| May 20, 1983 | 1721<br>1730 |
| May 21, 1983 | 1023 |
| May 22, 1983 | 1117 |
| May 23, 1983 | 1327 |

We have contacted Bill Gillespie at the local Federal Bureau of Investigation, and were instructed to contact you directly for this information.

Your prompt reply would be appreciated.

Sincerely,

JFMcClary

J. F. McClary
Division Leader
Operational Safeguards and
Security Division

JFM/ds
cy: C. Douglass, OS-4, MS F679
CRM-4, MS A150
OS-DO File

GTE

**GTE Telenet**
**Communications Corporation**

8229 Boone Boulevard
Vienna, Virginia 22180
703 442-1000

June 7, 1983

Mr. J. F. McClary
Division Leader
Operations Safeguards & Security
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

Dear Mr. McClary,

Due to the large number of connections to your host over the period of May 9 through May 23, 1983 and the limited amount of resources we have, we have only researched May 9th and 10th, 1983. However, I think you will find a pattern of calls which originated from our public service in St. Petersburg Florida (8130016).

Enclosed you will find the detail traffic records for the two days in question. Note that the time stamps of these records (top right) is Eastern Daylight Time and is the time of call termination plus a few seconds. The duration of the calls is determined by subtracting the start time from the termination time. The start time and termination time clock is a different clock from the record time stamp at the top right of the record.

Should you have any questions or choose to pursue this matter further please feel free to call me or my staff at (703) 442-1047.

Sincerely,

M Lee Brand

M. Lee Brand
Manager, Network Security

Where are enclosures?.