

zardoz





?

?

?

HAVE

YOU

EVER

HEARD

A PYGMY


```
$ls -l
```

```
drwx----- 1 root ro
```

```
4 zardoz
```

```
$du -s zardoz
```

```
1267982 zardoz
```

```
$ls zardoz
```

```
vol1.txt      vol7.txt      v
```

```
vol2.txt      vol8.txt      v
```

```
vol3.txt      vol9.txt      v
```

```
vol4.txt
```



2 am



c s i r o

cal and inform



vol4.txt vol10.txt vol15.
vol5.txt vol11.txt vol16.
vol6.txt
\$more zardoz/vol1.txt
zardoz edition 1

item 1/1:
for immediate release: jan
sept. 22, 1989 301/975-276

tn-xxxx

computer security experts
to reduce the risk of virus
to reduce the risk of dama

reports of a new variety of computer virus," says dennis steinauer, Manager of the computer security Management and evaluation group at nist.

while incidents of malicious software attacks are relatively few, they have been increasing. Most recently, a potentially serious personal computer virus has been reported. the virus is known by several names, including "columbus day," "datacrime" and "friday the 13th." in infected machines it is designed to attack the hard-disk data-storage devices of IBM-compatible personal computers on or after october 13. the virus is designed to destroy disk file directory information, making the disk's contents inaccessible. (a fact sheet on this virus is attached and includes precautionary measures to help prevent damage.)

<more>q
\$tar cf t.tar zardoz
\$compress t.ta


```
$ cat /etc/crontab
$ compress -t .
$ mv -t . tar .z
$ cd /tmp
$ uuencode .t
$ mail .t
```



10 IN"U@H.D"

MAIL>Quit

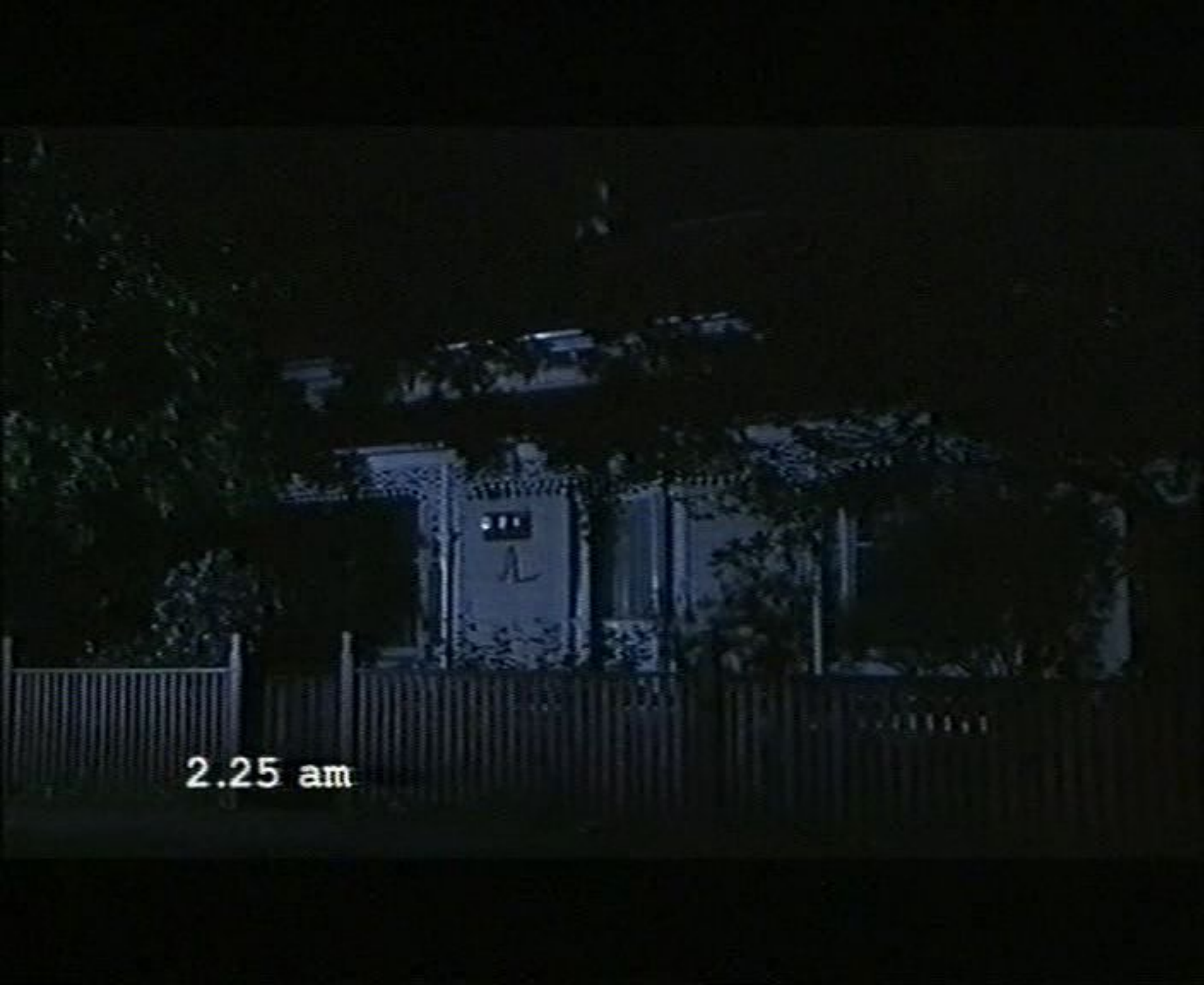
\$WARNING WARNING WARNIN

WARNING WARNING WARNING

WARNING WARNING WARNING







2.25 am



=====

THE COMPUTER INCIDENT ADVISORY CAPABILITY C I A C
ADVISORY NOTICE: *Warning: new and systems*

The U.COM Worm affecting UNIX and Systems
... .. September 9-2

The 9-006 Work affecting USA and Dept
October 14, 1989 10:27 PM/Author 8-2

The 9-CDM Work affecting USA US system
October 11, 1989 18:27 PPTVnumber 2-2
This is a mess but to kill and could have done a lot of damage.
The main purpose of each successful penetration
is to kill the main purpose of each successful penetration

October 14, 1989 13:27 PPTGnumber 2-2
This is a mass bug to kill and would have done a lot of damage.
Since it notified (Ry. Hall) someone of such successful penetration and
there is a telephone, but the system is not secure. The bug is not
that the password is not the same as the actual name.

E. David Thomas

E. David Sherwin
Advisory Notice

2. Kevin Oberon
Advisory Notice
A worm is attacking NASA's TDRS network via LAN/WAN systems connected to Internet. It is unclear if the worm has been changed. It may spread to other systems such as NASA's network within a few days. Our system managers should prepare now.

[illegible]

Since the movie has successfully penetrated your system, it will infect your files and create new, virulent subnormal files. It then goes to broadcast these virulent files to the outside world. It may also change files as well, either unintentionally or otherwise.

[illegible]

ZARDOZ

VOLUME 1

ADVISORY CAPABILITY C I





misix who

users on mis1.csiro.au:

user tty x11 from

root p1 4623 128.260.2.12

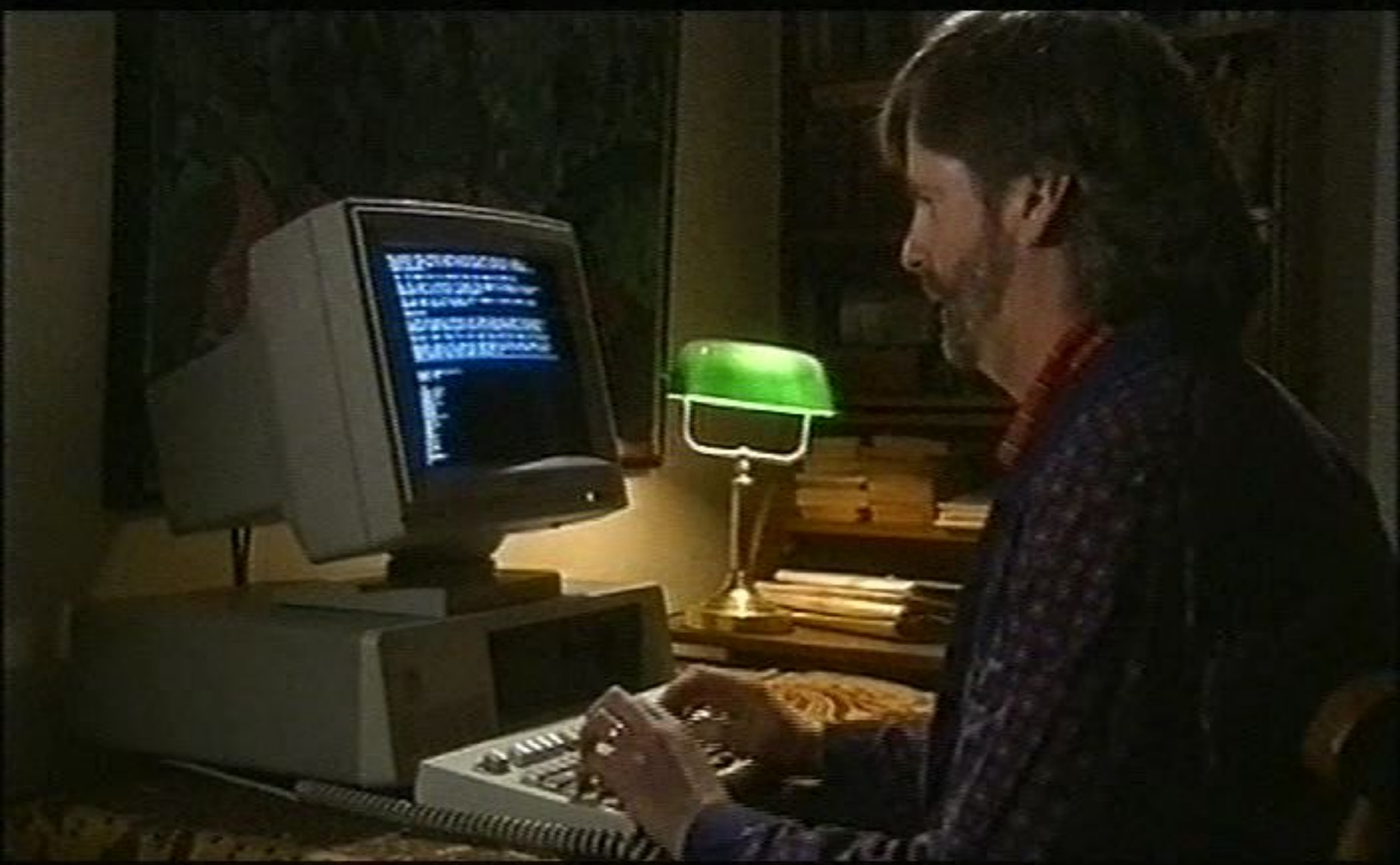
misix ps -auxxwlsrep p1

root	134	0.0	2.1	640	428	p1	ls	2:10PM	0:54.49	seconds
top	connect	0.0 <td>2.1<td>640<th>428</th><th>p1</th><td>ls</td><td>2:10PM<td>0:54.49<td>seconds</td></td></td></td></td>	2.1 <td>640<th>428</th><th>p1</th><td>ls</td><td>2:10PM<td>0:54.49<td>seconds</td></td></td></td>	640 <th>428</th> <th>p1</th> <td>ls</td> <td>2:10PM<td>0:54.49<td>seconds</td></td></td>	428	p1	ls	2:10PM <td>0:54.49<td>seconds</td></td>	0:54.49 <td>seconds</td>	seconds
top	connect	0.0 <td>2.1<td>640<th>428</th><th>p1</th><td>ls</td><td>2:10PM<td>0:54.49<td>seconds</td></td></td></td></td>	2.1 <td>640<th>428</th><th>p1</th><td>ls</td><td>2:10PM<td>0:54.49<td>seconds</td></td></td></td>	640 <th>428</th> <th>p1</th> <td>ls</td> <td>2:10PM<td>0:54.49<td>seconds</td></td></td>	428	p1	ls	2:10PM <td>0:54.49<td>seconds</td></td>	0:54.49 <td>seconds</td>	seconds
top	connect	0.0 <td>2.1<td>640<th>428</th><th>p1</th><td>ls</td><td>2:10PM<td>0:54.49<td>seconds</td></td></td></td></td>	2.1 <td>640<th>428</th><th>p1</th><td>ls</td><td>2:10PM<td>0:54.49<td>seconds</td></td></td></td>	640 <th>428</th> <th>p1</th> <td>ls</td> <td>2:10PM<td>0:54.49<td>seconds</td></td></td>	428	p1	ls	2:10PM <td>0:54.49<td>seconds</td></td>	0:54.49 <td>seconds</td>	seconds

host@mis1.csiro.au

misix







1. The following program will block the worm code and execute it. It will use minimal resources process named NETU_BLOCK which will prevent the

Editors note: This fix will work only with this

Mutated worms will require modification of this program should prevent the worm from running on your system from the worms attacks. is
////////////////////////////////////

```
nisix% nisix ls -l
total 75
```

```
.t
pin-1.8.9
anko.txt
asct.0
gener.c~
gener
gnone
libnu-1.7
tnp.c
tnp.c~
tnp
tnp.c
nu.c
nu.c~
p.txt
^
```



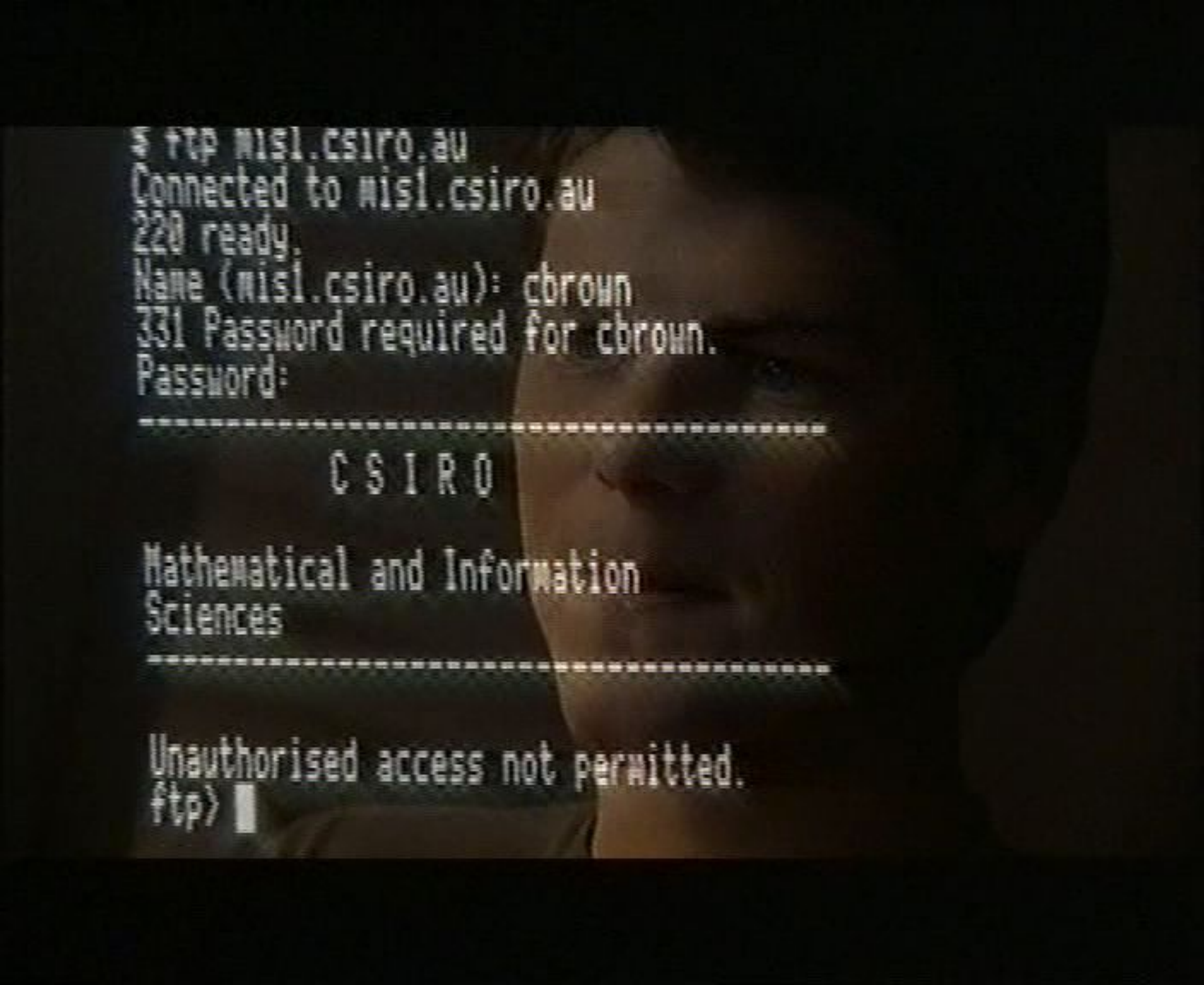







Welcome to the
University of Texas System Network Interface Processor
Node UTUAS,VAX,VMS V 5.1
Last interactive login on Friday, 23-FEB-1990 17:05

\$ ftp misl.csiro.au



```
$ ftp m1s1.csiro.au
Connected to m1s1.csiro.au
220 ready.
Name (m1s1.csiro.au): cbrown
331 Password required for cbrown.
Password:
```

CSIRO

Mathematical and Information
Sciences

Unauthorised access not permitted.
ftp> █

[illegible]

1998

[illegible]

1000 1000 1000

1999

[illegible]

000-000-000-000

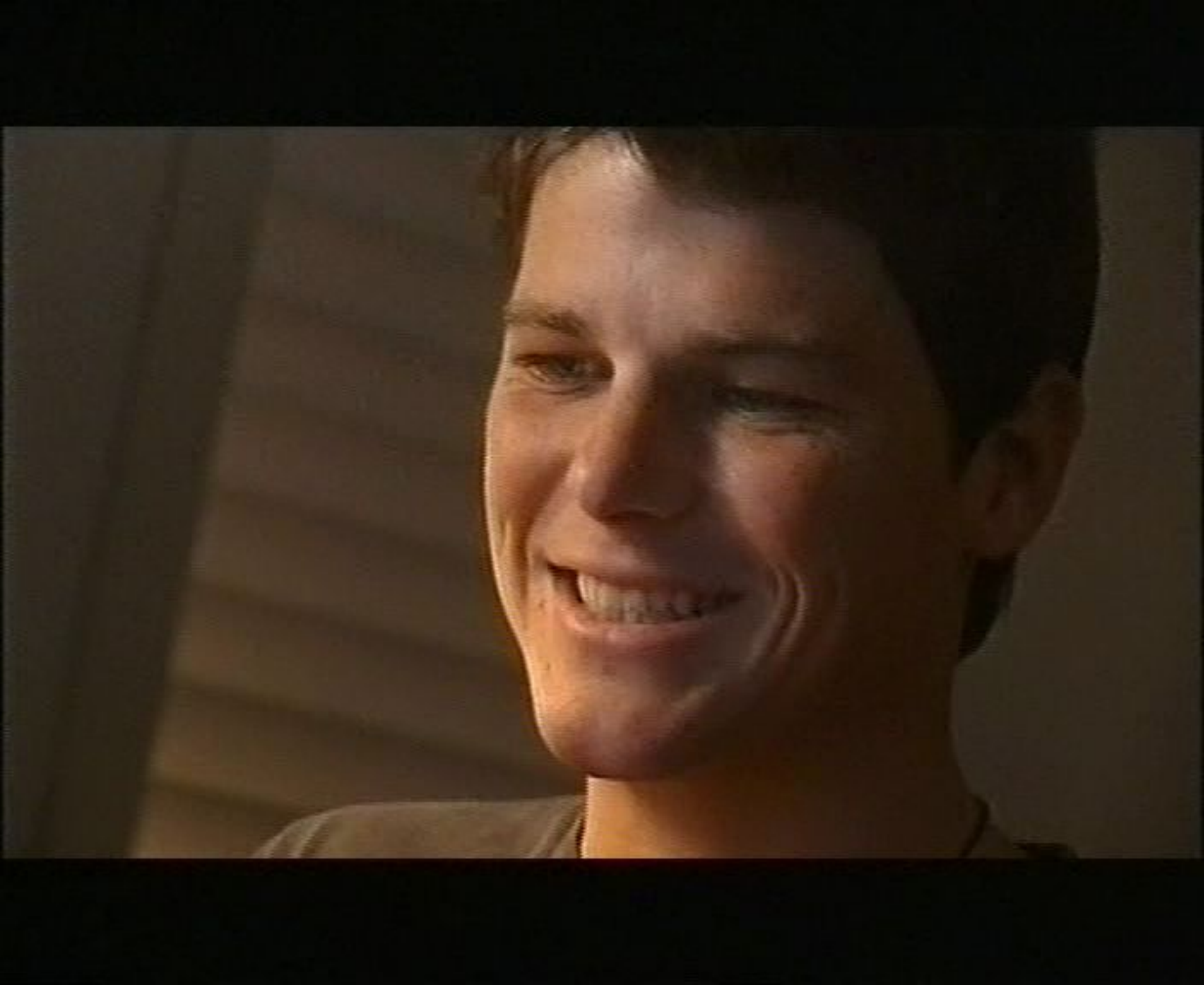
[illegible][illegible][illegible]



CONFIRM
CONFIRM
CONFIRM
CONFIRM
CONFIRM

DELETE
DELETE
DELETE
DELETE
DELETE


DATA
DATA
DATA
DATA
DATA



100% TRANSFER COMPLETED

UNCOMPRESS ZARD002.Z



A close-up, low-key photograph of a man with dark, curly hair. He is looking down and to the right, with his right hand resting against his chin and cheek in a contemplative or pensive pose. The lighting is very low, coming from the side, which highlights the texture of his hair and the contours of his face and hand. The background is dark and out of focus, showing some indistinct shapes that might be furniture or wall decorations. In the bottom left corner, the text "3.44 am" is displayed in a white, sans-serif font.

3.44 am

