Tech Info Library

ALERT: Steroid Trojan Horse

Revised: 7/16/90
Security: Everyone

ALERT: "Steroid" Trojan Horse

==========

This article last reviewed: 21 June 1990

TOPIC ----------

This article discusses the effects of a Trojan Horse called "Steroid", and some suggestions on repairing the losses it can cause.

DISCUSSION ----------

The Trojan Horse called "Steroid" is an INIT that claims to speed up QuickDraw on Macintosh computers with 9-inch screens. The INIT contains code that checks for the date being greater than June 6, 1990. If it is, it erases all mounted drives.

We have performed some tests on a Macintosh SE. Having Comm Toolbox installed seemed to interfere with the INIT and kept the erase from happening: the Macintosh SE simply crashed instead.

We then installed the INIT on a floppy disk and booted the Macintosh SE. The floppy and hard disk were promptly erased. NOTE: We had set the date to one LATER than June 6, 1990.

So far, we know that the code does the following operations at restart:

Operations at Restart

DATE & TIME CHECK (Loop)
SYSENVIRONS CHECK
GETS VOLUME INFORMATION (probably checking for HFS)
GETS SOME ADDRESSES (Toolbox traps)
DOES SOME HFS DISPATCH OPERATIONS
VOLUME IS REINITIALIZED to "Untitled"

Information

```
TYPE:      INIT
CREATOR:   qdac
CODE SIZE: 1080
DATA SIZE: 267
ID:        148
Name:      QuickDraw Accelerator
File Name: "  Steroid" (first two characters are ASCII 1)
```

What To Do

If your disk becomes erased, you can use SUM II Disk Clinic to recover the deleted files. We have tried this and it seems to work.

Tech Info Library Article Number:5833