Tech Info Library

WDEF Virus: Information

```
Revised:        3/4/90
Security:       Everyone
```

"WDEF" Virus: Information

===

This article last reviewed: 18 January 1990

TOPIC ---

This article contains information on spotting and neutralizing a new virus
(sometimes called the "WDEF virus")

DISCUSSION --

There is a Macintosh virus (sometimes called the "WDEF virus") that uses a
different method to transfer itself between machines. Because this virus
attaches itself to the Desktop file of a disk, it infects a hard disk when the
infected floppy disk is inserted into the Macintosh.

If you want to check a disk for infection, follow these steps:

1) Start your machine in Finder, NOT MultiFinder.

2) Run ResEdit.

3) Insert the suspect floppy disk.

4) Open the Desktop file.

5) If it contains a WDEF resource with ID=0, it is infected.

If you insert an infected floppy disk when running MultiFinder, the Desktop
file is automatically opened, and your system will be infected.

There is a way to keep this virus from infecting your system:

1) Your current application must be the Finder. If you are running
   MultiFinder, you should have the Finder's menus in the menu bar.

2) Hold down both the Command and Option keys.

3) With these keys held down, insert the unlocked floppy disk.

4) You will be asked if you want to rebuild the Desktop file.

5) Choose "Yes". If you choose "Cancel" at this point, and the floppy is
   infected, you will infect your system.

Rebuilding the Desktop removes the virus.

As of February 1990, Apple is aware of several virus tools that can
automatically detect this virus:

- SAM v1.5

- AntiToxin v1.3

- Virex v2.3

- Disinfectant v1.6

- Eridicator (Public Domain)

- Kill WDEF (Public Domain)

For more information, search on the above product names in the Tech Info
Library.

Copyright 1990 Apple Computer, Inc.

Tech Info Library Article Number:5048