WDEF Virus: May Cause AppleShare Performance Problems

Revised: 3/4/90
Security: Everyone

WDEF Virus: May Cause AppleShare Performance Problems

==========

This article last reviewed: 7 February 1990

TOPIC ----------

Over the past 2 weeks, some of my AppleShare workstations are sporadically slowing down.

When a server volume is mounted and the mouse is moved, the pointer changes to a watch, and the AppleTalk arrows activate. Trashing the server volume makes the problem go away.

These workstations are Macintosh II and Macintosh Plus Systems running System Software 6.0.2 and using AppleShare 2.0.1.

I also have a question regarding a network problem.

I have a six-system network on PhoneNET cabling, with one Macintosh SE/30 as an AppleShare server. After using the one Macintosh IIcx for about a minute, it freezes, and the server activity bar just bounces back and forth for several minutes. I connected only the Macintosh IIcx to the Macintosh SE/30 to lessen the problem, but it is still there. I've replaced the connectors on both machines.

The hardware passes all diagnostics. The Macintosh SE/30 has an HD80 SC, and the Macintosh IIcx has an HD40 SC.

Can you explain why these things are happening?

DISCUSSION ----------

There are two likely causes for these problems.

The first would be poor network connections or wiring that causes excessive packet loss and retries, resulting in poor performance. The second possibility is that the AppleShare File Server client stations are infected with the WDEF

virus.

Since you are reporting multiple occurrences of what seems to be the same problem, a cable or connector malfunction seems unlikely. We would suspect that the WDEF virus has spread at your sites.

While the WDEF virus does not appear to cause malicious damage (other than propagating), it does have bugs and side effects that are very annoying at best. It is spread via the Desktop file of Macintosh disks, and is activated when the Finder opens this file as part of its normal disk-mounting process. Once activated, WDEF copies itself to the Desktop files of other mounted volumes.

This virus effects server performance because it tries to infect the Desktop file of mounted server volumes as well as locally mounted disks. It first tests the target Desktop file to see if it's already infected, and if not, copies itself there. With network volumes, this activity requires many AFP (AppleTalk Filing Protocol) requests and is noticeably time-consuming on a LocalTalk- or PhoneNET-based network. This would be the effect you are noticing.

Fortunately, this virus is easy to detect and eliminate. One way is to scan your disks with a recent version of an anti-virus utility that has been updated to recognize the WDEF virus. Disinfectant 1.5, which is known to detect current strains of the WDEF virus as well as many other viruses, is one such utility. We recommend using it to scan all floppies and hard disks that may have been used recently.

Disinfectant 1.5 is also available under the AppleLink Developer Services icon by following this path:

```
Developer Services
  Macintosh Developer Technical Support
    Tools
      Virus Tools
        Disinfectant 1.5
```

Disinfectant is capable of detecting and removing WDEF, but WDEF is also simple to remove by simply rebuilding the Desktop file of an infected disk. Hold down the Command and Option keys while the Macintosh is loading the Finder. Confirm the dialogs asking if you really want to rebuild the Desktop file on each mounted volume. The new Desktop file will be free of WDEF. Remember to restart the Macintosh after disinfecting volumes. This is necessary to remove any copies of WDEF that may be currently executing.

Another means of WDEF detection and removal is to use ResEdit. It allows you to view all the resources in a file, and can, therefore, be used as a primitive means of detection. If there are any WDEF resources present in a Desktop file, delete them. A normal Desktop file will not contain any WDEF resources.

To remove WDEF from server volumes, mount the volumes on a client Macintosh and use ResEdit to delete the server volume Desktop files. A Desktop file is not necessary on an AppleShare File Server volume, and by removing it you reduce

the risk of a future WDEF outbreak affecting server performance. Do not try to remove the files Desktop DB and Desktop DF. These are the files used by AppleShare instead of a Desktop file. They are not infected by WDEF, but are needed by AppleShare.

Other anti-virus software is available, both commercially and non-commercially, to detect viruses and to prevent future infections. SAM is a commercial package from Symantec Corp. that contains a detection and repair program from Symantec Corp. with similar functionality to Disinfectant. It also contains an INIT that alerts the user to, and prevents, infection attempts by known viruses.

There is also a public domain INIT, Eradicator!, that prevents infections of the WDEF virus, and removes any occurrences it detects.

We strongly recommend the installation of this or some similar type of program to help prevent infection.

For more information, search under: "Symantec" or "WDEF" or "Viruses".

Copyright 1990 Apple Computer, Inc.

Tech Info Library Article Number:5030