

CyberSoft White Papers

Field Guide to Antivirus False Alarms

Joe Wells

CyberSoft, Inc.

Copyright © May 1999 by CyberSoft, Inc. All Rights Reserved.

Consider this: If you're not using any antivirus product and you suspect you have a virus, chances are good you don't. If you do have a virus, chances are very good that it's one of a few common ones. However, it's extremely unlikely that you will ever have a rare virus that has never infected anyone else.

Keep these facts in mind.

Expect False Positives

A false positive (or false alarm) occurs when an antivirus product falsely detects a virus. That is, the antivirus product reports a virus in a file or other location (such as memory or a boot sector) where there is, in fact, no virus present.

All antivirus users need to be aware that it is impossible for an antivirus product to detect all viruses that could ever exist and not make mistakes. Antivirus products will always fail to detect some viruses, incorrectly claim that uninfected programs are infected, or both.

This is not a failure of antivirus technology. Rather, this is a fact that has been proven mathematically by Dr. Fred Cohen.

Recognize False Positives.

Most false positives involve one of the following conditions.

1. An executable file virus found in a data file.
2. A "zoo" virus detected in an executable file.
3. A macro virus is detected in a "cleaned" data file.

These conditions are detailed below.

Condition 1. Users often think they should scan "all files" for viruses. This often causes false alarms where older DOS executable-file viruses are detected in data files (such as databases, picture files, etc.)

There are thousands of such DOS viruses detected by antivirus programs, but virtually all of them infect only executable programs with a .exe or .com extension. They do not infect data files.

Using an antivirus product to scan "all files" is not recommended, but, if the user does so, he or she needs to be aware that DOS file viruses do not infect data files.

Condition 2. The vast majority of older DOS viruses that antivirus products scan for have never infected any user, anywhere, ever.

Such viruses were created by some virus writer somewhere and shared with other virus writers. Sometimes such viruses are sent (unsolicited) directly to antivirus product developers. Ultimately these viruses end up in virus collections called zoos.

Viruses that actually infect users that actually spread, and are a real threat to you are not considered to be "zoo" viruses. These are in-the-wild (ITW) viruses. Antivirus companies report ITW viruses to the WildList Organization International, who in turn reports them in a monthly WildList (www.wildlist.org).

If your antivirus product is reporting a virus, check the virus against the WildList. (Note that each virus may have aliases listed. You may need to look for the virus name here also.)

If the virus is on the list, bear this in mind: The WildList has reporters' initials by each virus. Generally speaking, the more initials the more common the virus.

If your antivirus product is reporting a "zoo" virus it is probably a false positive. This is especially so if any of the following conditions are true:

- The virus is reported only in a single file.
- The virus name starts with "HLL".
- The virus is a polymorphic engine virus.

Even though you probably don't have a virus, you should send a copy of the executable file to your antivirus vendor for them to examine. This way they can eliminate the false positive from their product.

Condition 3. Macro viruses are those that infect Microsoft Office data files (Word Documents, Excel Spreadsheets, Access databases, or PowerPoint presentations). Sometimes one antivirus product will detect a macro virus in a file that has been "cleaned" by another antivirus product.

Some antivirus products "clean" macro viruses by modifying the OLE2 stream within the file, but leave the actual virus body in the file. Since the elements of the infective code and data are still present, another antivirus product may still detect this information.

Summary

Inductive Premises:

- If you think you have a virus, you probably don't.
- If you do have a virus, it's probably a common one.

Application:

- If your antivirus product reports a virus in a data file, you're not infected.
- If your antivirus product reports a zoo virus in a program file, you're probably not infected.
- If your antivirus product reports an ItW virus, you might be infected.
- If your antivirus product reports an ItW virus that has lots of people reporting it, you very probably are infected.

Back

[Home](#) | [Products](#) | [Support](#) | [Purchase Info](#) | [About Us](#) | [News](#) | [Contact](#)

Questions or comments about this website? Please contact the webmaster. 

© Copyright 2009 CyberSoft, Inc. All rights reserved.



This site certified 508 Compliant