

9 September 2008

By: Lucian Constantin, Web News Editor

## [Trend Micro Antivirus Definitions Crash Computers](#)

*Flawed malware definitions released by Trend Micro crippled users' computers*



Trend Micro released  
bogus antivirus  
definitions  
Trend Micro Inc.

The antivirus definitions released by Trend Micro Inc. for several of its products on September 5 caused computers to become unstable or unusable. The definitions falsely identified vital system files on both Windows Vista and Windows XP computers as malware, and added them to quarantine. Upon rebooting, this situation left computers unstable or unable to boot into the operating system.

The updates were issued for the Trend Micro AntiVirus, Internet Security and Internet Security Pro products, and identified several system files as Troj\_Generic or Troj\_Generic.ADV. Amongst the legit files falsely identified as malware were Windows Vista's Network Location Awareness 2 Service (nlasvc.dll), the Win32 Cabinet Self-Extractor (wextract.exe) or the OpenSSL Library (libeay32.dll).

Trend Micro became aware of the problem after its customer support centers were assaulted with phone calls from upset users and, 10 hours later, issued another definition update that fixed the error. The company claimed that mainly European users were affected. "For a brief period of time late last week primarily some continental European consumers were affected by a Trend Micro pattern-file update with a false positive that could have led to quarantining a few Windows components," commented spokeswoman Andrea Mueller.

According to another Trend Micro statement, "customers who downloaded OPR 5.525.50 needed only to update to the latest OPR." However, this doesn't apply for the users who can no longer boot into Windows, because they have no way to update to the bug-free new definition. Fortunately, Trend Micro [released](#) a detailed technical support document for users finding themselves in this situation. The solution involves booting Windows in "Safe Mode with Networking," then downloading and running a restore tool developed by the company specifically for this incident.

This is not the first time a security company issues bogus definitions updates that affect the normal behavior of users' computers, nor is it even the first time for Trend Micro. A previous Trend Micro incident involved a bug in the definitions file that overloaded the CPU and crashed computers, but it was restricted mostly to users in Japan. Symantec Inc. was also responsible for another highly similar incident, where signatures generated false positives on vital system files and left thousands of computers unbootable.