

22 October 2008

By: Lucian Constantin, Web News Editor



McAfee tags Vista component as malware  
McAfee, Inc.

## [McAfee Faulty Definitions Update Quarantine Vista Components](#)

### *Windows Vista console IME was detected as PWS-LegMir*

The Windows Vista console IME was incorrectly tagged by McAfee's security products as Trojan [PWS-LegMir](#) due to a faulty definitions file. The false positive was corrected in a later definitions update.

The 5409 DAT files released on October 20, 2008 contained a bad signature that falsely detected a legit Windows Vista component as malware. Due to the faulty signatures, the McAfee products quarantined or completely deleted the conime.exe (Windows Vista console IME) file, which they generically detected as belonging to the PWS-LegMir Trojan.

McAfee explains that the false positive resulted because that particular definition is designed to generically detect multiple Trojan-type malicious applications that steal passwords. "This includes trojans written in multiple HLLs, including MSVC, MSVB and Delphi," claims McAfee.

The name of the PWS-LegMir.gen or PWS-LegMir.gen.b comes from the fact that in addition to stealing password from various locations on the system, the trojans which are detected under this signature also steal information for the Legend of Mir computer game if the game is installed on a compromised machine.

McAfee fixed this problem by releasing the 5410 DAT files the next day, on October 21. The new signature successfully corrected the issue and the affected users were able to restore the legit file. "The 5409 DAT files contain an incorrect identification on PWS-LegMir. McAfee Avert Labs have released DAT 5410&nbsp; to correct this issue," announced the company.

This is not the first time faulty definitions affect the users of anti-virus products. Last week, a bad malware definition caused the AVG Antivirus to incorrectly [detect and block](#) critical components of the ZoneAlarm firewall, while last month a similar generic definition caused Trend Micro security products to [tag several system files](#) as Trojans and caused computers to crash.

McAfee is not at its first incident this year. In August, its products tagged a plug-in for the Microsoft Office Live Meeting as a Trojan. 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.