

15 November 2008

By: Lucian Constantin, Web News Editor



AVG faulty definitions tag Adobe Flash Player component as malware
AVG Technologies

[AVG Tags Adobe Flash Player as Malware](#)

Only days after bogus definitions caused the removal of a vital Windows component

Users of the popular AVG antivirus product [reported](#) on the company's support forum that an Adobe flash component had been detected as a generic password stealing Trojan. This was caused by a faulty definition file that was pushed to users on Friday and followed a similar incident that occurred earlier this week, when the product wrongly identified a Windows component as malware and "cleaned" it.

According to user reports, the antivirus identified the flashUtil10a.exe file as Trojan Horse PSW.Generic6.AQPD. The file is actually an Adobe Flash Player 10 utility, which is used to automatically check for updates and also see if the player has been properly installed. AVG has not commented on this new incident, but according to a forum moderator, the problem has been fixed. Other users reported that the problem only affected version 8 of the antivirus product, while users of version 7.5 did not encounter the issue. However, since this information was not confirmed by AVG officials, it should be treated as such.

This is the third time in a month and second time in only a few days when AVG issues bogus definition files. The [first](#) of the three incidents consisted of false positives on no less than five components of the popular ZoneAlarm firewall, claiming that the files were infected with Trojan Horse Agent_r.CX. "We did accidentally tag Check Point's Zone Alarm as a trojan. The detection was out for approximately 7.5 hours. As soon as we were notified of the issue, it was resolved and added to our whitelist," said an AVG spokeswoman at the time.

The [second incident](#) was more serious because it involved a vital Windows component, user32.dll. This file, which is otherwise known as the Windows User API Client DLL, stores instructions for graphical elements such as dialog boxes and windows. By removing the file, AVG rendered the users' systems unbootable. Fortunately, the issue only affected the Dutch, French, Italian, Portuguese, and Spanish language versions of Windows XP Professional. The company compensated the users affected by the user32.dll issue with a free one-year license extension and apologized by saying that "it sincerely regrets the inconvenience users have experienced."

Such false positives being caused by bugs in definition files are not an uncommon thing. Most vendors have been affected by them at one point or another, [some](#) even recently. They are certainly more serious when they involve vital operating [system components](#), but blocking other third-party popular applications is at least annoying for many users. Even so, three such incidents in a month is more than what should be acceptable and this should prompt AVG to take a closer look at their quality assurance policies or the people who are responsible for implementing them.