

17 October 2008

By: Lucian Constantin, Web News Editor

[AVG Detects ZoneAlarm as Trojan](#)



AVG definition updates tag ZoneAlarm as malware
AVG Technologies

A faulty definition update caused AVG anti-virus to block and quarantine the ZoneAlarm firewall

People that use the AVG anti-virus, along with the ZoneAlarm firewall, had an unpleasant surprise when AVG suddenly started to block and quarantine Check Point's popular firewall solution. The false positive was caused by a bogus malware definition file update and AVG eventually addressed the issue.

This problem affected all versions of ZoneAlarm and AVG, both free and commercial; thus, the users assaulted the ZoneAlarm support forum with reports that AVG started to detect ZoneAlarm as a Trojan by the name of Agent_r.CX. Several ZoneAlarm components were being blocked and quarantined and attempts at reinstalling the firewall software failed. At the same time, similar reports popped up on the AVG forums.

"AVG updated on reboot around 8:30 p.m., 10/13/2008. Then AVG Resident Shield blocked Zone Alarm Pro vsmon.exe from loading after identifying five (5) ZA files in Windows/System32/ZoneLabs/lib as infected with Trojan Horse Agent_r.CX: ConfigWizard.zip.dll, licenseui.zip.dll, zlsvc.zip.dll, zpy.zip.dll, zui.zip.dll. Files have been there for 3 months," a user [described](#) the technical details.

According to Laura Yecies, General Manager at Check Point, the company that develops ZoneAlarm, AVG was immediately notified and issued a definitions fix in a matter of hours. During the few hours of uncertainty, the users devised a workaround that consisted in adding the ZoneAlarm folder to the exceptions list of the anti-virus.

[The Register](#) reports that an AVG spokeswoman confirmed a time of seven hours and a half since the first faulty update until the fix was issued. "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. We were made aware of it around 3 am and the issue was addressed and resolved within a few hours," the spokeswoman noted.

This incident comes after last month bogus definitions released by anti-virus vendor Trend Micro [tagged](#) several system files as malware and caused computers to crash. Symantec pulled a similar stunt that resulted in thousands of unbootable computers. Cases where bogus definition updates tag Windows system files as malware occur more often and generally affect more users. However, since both AVG and ZoneAlarm products have free versions that are quite popular, it's safe to assume that a considerable number of users were affected in this incident, too.