



Issued 10/26/17

Kaspersky Says NSA Hacking Tools Obtained After Malware Was Found

Kaspersky has acknowledged that code belonging to the US National Security Agency (NSA) was lifted from a PC for analysis but insists the theft was not intentional.

In October, a report from The Wall Street Journal claimed that in 2015, the Russian firm targeted an employee of the NSA known for working on the intelligence agency's hacking tools and software. It was actually a year earlier than the Journal believed, in 2014, that code belonging to the NSA's Equation Group was taken. Kaspersky's antivirus detected the sample on a home computer which had Kaspersky's Security Network (KSN) enabled, a system which automatically collects threat data and sends it to the cloud. The company claims that the user in question had installed pirate software on their machine as illegal Microsoft Office keygens were present. Later, although the exact timeframe has not been specified, the antivirus was enabled and the malware was blocked. The user then ran a number of scans to remove the Trojan, which also caught the Equation group hacking tools in the mix.

Kaspersky says that the samples were not shared with third parties, although a New York Times report claims that Israeli intelligence officers hacked into the firm's network in 2014 and discovered Russian hackers were exploiting Kaspersky software to "turn [it] into a sort of Google search for sensitive information."