Kaspersky blames NSA hack on infected Microsoft software

November 16 2017

The Moscow headquarters of Kaspersky Lab, which the US has alleged has links to Russian intelligence

Embattled computer security firm Kaspersky Lab said Thursday that malware-infected Microsoft Office software and not its own was to blame for the hacking theft of top-secret US intelligence materials.

Adding tantalizing new details to the cyber-espionage mystery that has

rocked the US intelligence community, Kaspersky also said there was a China link to the hack.

The Moscow-based anti-virus software maker, which is now banned on US government computers because of alleged links to Russian intelligence, confirmed that someone did apparently steal valuable National Security Agency programs from an NSA worker's home computer, as first reported by the Wall Street Journal on October 5.

According to the Journal, the person had top secret files and programs from the NSA hacking unit called the Equation Group on his computer, which was also using Kaspersky software protection.

They believe that Russian spies used the Kaspersky program as a back door to discover and siphon off the files, reportedly causing deep damage to the NSA's own cyber-espionage operations.

US allegations that Kaspersky, which sold more than $600 million of anti-virus software globally in 2015, knowingly or unknowingly helped Russian intelligence in the theft have effectively killed its US business and hurt its worldwide reputation.

Kaspersky software 'disabled'

Using its own forensic analysis, Kaspersky said the breach of the NSA worker's computer took place between September and November 2014, rather than 2015 as the Journal reported.

Kaspersky said what was stolen included essential source code for some Equation Group malware, as well as classified documents. Based on the materials, it said the computer appeared to belong to someone involved in creating malware for the Equation Group.

The company claimed, however, that the computer was infected by other malware, including a Russian-made "backdoor tool" hidden in Microsoft Office.

Kaspersky said that the malware was controlled from a computer server base in Hunan, China, and would have opened a path into the computer for anyone targeting an NSA worker.

"Given that system owner's potential clearance level, the user could have been a prime target of nation-states," it said.

Kaspersky's own software would have detected that malware, the company said, except that its software had been turned off.

"To install and run this malware, the user must have disabled Kaspersky Lab products on his machine," it claimed.