Kaspersky Lab denies involvement in Russian hack of NSA contractor

Eugene Kaspersky, the founder of the Moscow-based cybersecurity firm, called allegations of role in government hack 'like the script of a C movie'

Alex Hern

Friday 6 October 2017 10.38 BST

Moscow-based cybersecurity firm Kaspersky Lab has hit back at a report in the Wall Street Journal which accused it of being involved in a Russian government hack of an NSA contractor in 2015.

The paper reported on Thursday that the NSA contractor, a Vietnamese national who was working to create replacements for the hacking tools leaked by Edward Snowden, was hacked on his personal computer after he took his work home.

There, the report says, the contractor's use of Kaspersky's antivirus software "alerted Russian hackers to the presence of files that may have been taken from the NSA". Once the machine was in their sights, the Russian hackers infiltrated it and obtained a significant amount of data, according to the paper.

Calling the allegations "like the script of a C movie", Eugene Kaspersky, the infosec firm's founder, gave his own explanation of what might have happened.

Mr Kaspersky vehemently denied that his company had played any active role in the breach, noting: “We never betray the trust that our users put into our hands. If we would do that a single time that would be immediately spotted by the industry and our business would be done.”

Instead, he implied that the root of the problem was that Kaspersky Lab had correctly identified the hacking tools the contractor was working on as malware - perhaps through Kaspersky Lab’s own research into the Equation Group, a “sophisticated cyber espionage platform” believed to be linked to the NSA.

From there, Mr Kaspersky implies, it may be the case that Kaspersky Lab’s own data was hacked by the Russian government. “Even though we have an internal security team, and do bug bounties, we can’t give 100% guarantee that there are no security issues in our products, name another security software vendor who can!”

Kaspersky’s defence is roughly in line with the general consensus amongnonaligned information security experts. Matthew Green, a cryptography professor at Johns Hopkins University, wrote: “Consensus on infosec Twitter is that Kaspersky may not have colluded with [the Russian government]; just maybe their product may be horrendously compromised.

“Not quite sure how that’s qualitatively different from the point of view of Kaspersky customers. But I guess it’s something.”
In an unusual move for a technology chief executive, Mr Kaspersky republished Green’s tweet calling his product “horrendously compromised” in his own blogpost.

The hacking incident in question may be the key evidence used in September to drive a US government-wide ban of Kaspersky products.

At the time, the Department of Homeland Security said it “is concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks”.

In an official statement about the allegations, Kaspersky Lab said: “As a private company, Kaspersky Lab does not have inappropriate ties to any government, including Russia, and the only conclusion seems to be that Kaspersky Lab is caught in the middle of a geopolitical fight.”

Topics

- Technology
- Data and computer security
- Data protection
- Russia
- Europe
- news