


CrowdStrike fails in last-ditch legal attempt to block publication of testing results

Next-gen security vendor tried to block NSS Labs publishing results of its end-point-protection test but failed to obtain an injunction



Tom Wright

 @TomWrightCRN

14 February 2017

CrowdStrike has failed to block the publication of results from an NSS Labs' end-point security test after a US court rejected its request for an injunction.

The end-point security vendor sought an injunction on Friday, claiming that NSS Labs illegally accessed its software; breached a contract it has with CrowdStrike; and carried out "improper security testing".

NSS Labs is one of several anti-virus (AV) testing houses to test products from a number of security vendors and publish its findings online.

The US court, however, ruled against CrowdStrike, and NSS Labs is now set to release the results of the test at the RSA security conference in San Francisco.

CrowdStrike claimed in court that it initially had a contract in place that would allow NSS Labs to test its Falcon software privately, but was unimpressed by NSS Labs' "deeply flawed" testing methods and as a result refused to participate in further tests.

NSS Labs then acquired CrowdStrike software through a reseller and carried out the testing without CrowdStrike's permission - which the security firm claimed breached the contract that was already in place.

The vendor also claimed that publication of the results could negatively affect its business but the court said that CrowdStrike would have to address this publicly, rather than try to stop the results being made public.

The court document summarising the case stated: "While it is possible that CrowdStrike will suffer a decrease in sales and revenue as a result of NSS's report, CrowdStrike could mitigate that hardship by challenging the veracity of NSS's results and their testing methods.

"The court finds that the public has a very real interest in the dissemination of information regarding products in the marketplace. If it turns out, in this case, that NSS's data is inaccurate, CrowdStrike could publicly rebut that data with evidence of its faults. The public would, in fact, benefit from such an exchange between the parties because it would serve to inform them about the trust they should put in NSS's future reports."

CrowdStrike responds

In a damning blog on its website, CrowdStrike stood by its claims in court and slammed NSS Labs for its testing methods.

"After explicitly telling NSS on multiple occasions that they were prohibited from using our software for public testing, they colluded with a reseller and engaged in a sham transaction to access our software to conduct the testing," the blog read.

"We believe the actions of NSS are detrimental to the security industry and they need to be held accountable. We reject the unethical, illicit, and subversive way that NSS does business and the harm it brings to our industry, security research, and most of all, the users of security technologies. We hope that other leaders in the security industry will join us in speaking out and taking action against those who seek to harm our industry and security for their own gain.

"To be crystal clear, the results of the report are unknown to us at this time and irrelevant. We are suing NSS because of their illicit activity, breach of contract and misappropriation of our intellectual property."

In a statement on its website NSS Labs said: "NSS Labs' mission is to arm the public with the fact-based and objective information required to get secure and stay secure.

"Per our mission, on Friday 3 February, NSS Labs announced its intent to release the much-anticipated results of our Advanced Endpoint Protection group test at the RSA 2017 conference in San Francisco.

"This past Friday, 10 February, CrowdStrike Inc sought a temporary restraining order and preliminary injunction in Delaware to block publication of our test results of CrowdStrike's Falcor product. Today, 13 February, the Federal Court denied CrowdStrike's requests and we will publish our test results."

Grey area

This is not the first time NSS Labs has found itself in hot water with security vendors.

In 2013 **WatchGuard accused** NSS Labs of not being impartial after performing badly in a test; in April 2014 **FireEye accused** it of having a "severely flawed" methodology; and later that year **Palo Alto Networks claimed** it operated a "pay-for-play" testing model.

Carl Gottlieb, founder of security reseller Cognition, explained that there is a power struggle within the AV sector over whether vendors should be obliged to make their products available for testing.

He explained that some testers have had their credit cards blocked by certain vendors, after they were caught posing as customers and downloading the software to carry out tests without the vendor's permission.

"It's a grey area," he said. "Some of the vendors are saying 'I've looked at you as a tester and I don't like your methodology and I don't like the quality of your work, therefore why should you have access to our product to go out and put a statement around it?'"

"NSS have quite a patchy reputation for the quality of their testing - some love it and some don't and so some vendors like CrowdStrike have said 'we don't want you having our software', and in this case they've got it.


"You've got this battle going on. The testers want access and the vendors want to restrict it. Personally I think it's the vendor's prerogative. If they don't trust the tester then why should they have access to the product?"

0 Comments

ChannelWeb

 Carl Gottlieb ▾

 Recommend

 Share

Sort by Best ▾



Start the discussion...

Be the first to comment.

ALSO ON CHANNELWEB

Microsoft crowned king of SaaS

1 comment • a month ago•



Ian Moyses — What a turnaround and a poster child for legacy vendors on how to cloud transform your products and go ...

Carbon Black takes aim at Sophos, Kaspersky and Symantec partners

1 comment • 20 days ago•



iank — full marks for entering a contest without knowing how it works: he can't say what margins he will pay and he ...

Citrix partners finger Microsoft as a likely suitor

3 comments • a month ago•







doug_woodburn_inc — Yes, thanks for pointing that out!

HPE 'becomes the new guard' with Nimble acquisition, say partners

1 comment • a month ago•



Bruce — HPE have certainly put a stake in the ground here. Two very interesting and quick acquisitions. Like Jonathan ...

 [Subscribe](#)
 [Add Disqus to your site](#)
[Add Disqus](#)
 [Add](#)
 [Privacy](#)


© Incisive Business Media (IP) Limited, Published by Incisive Business Media Limited, Haymarket House, 28-29 Haymarket, London SW1Y 4RX, are companies registered in England and Wales with company registration numbers 9177174 & 9178013