No.26
3rd June 2019

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

The NSS Labs Apology to CrowdStrike

- NSS Labs has finally apologized to CrowdStrike for what it admits were "inaccurate test results" on CrowdStrike's Falcon Platform. The two companies have also resolved the lawsuits between them.
- The apology is further proof that the legacy model of large test houses defining their own test plans and their own approach to transparency is no longer best suited to market requirements.
- NSS Labs still does not appear to have dropped the antitrust lawsuit against the Anti Malware Testing Standards Organization (AMTSO). An attempt to have the suit dismissed last week was unsuccessful.
- Vendors should be migrating toward greater support for the more open security product testing standards being advanced by AMTSO and NetSecOPEN. User organizations need to be far more active in supporting these standards too.

The week of May 20th , NSS Labs issued a statement extending its "sincere apology to CrowdStrike for the publication of inaccurate test results of CrowdStrike's Falcon Platform" back in 2017. The background to this was recapped in a Dark Reading article on Friday May 24th. CrowdStrike also issued a statement to SearchSecurity adding that "CrowdStrike and NSS Labs have resolved the lawsuits between them pursuant to a confidential settlement agreement."

The more transparent, consensual, standards-based approach of NetSecOPEN and AMTSO represents the right way forward now.

HardenStance's take-aways from these developments are as follows:

- **This walk back materially weakens the credibility of NSS Labs.** CrowdStrike was unsuccessful in securing an injunction against NSS Labs publishing these inaccurate findings at the time of RSA Conference in 2017. The market – including buyers and CrowdStrike itself - has had to live with a big name test house steadfastly standing by its inaccurate findings for more than two years.
- **The cloud of an NSS Labs antitrust lawsuit still hangs over the important work of the Anti Malware Testing Standards Organization (AMTSO).** In September 2018, NSS Labs filed suit against vendors CrowdStrike, ESET and Symantec as well as AMTSO. HardenStance is not aware of any further public comment from NSS Labs on the status of its suits against the other three parties. An attempt by one or more party to have the suit dismissed by the US Northern District Court of California last Thursday was unsuccessful, according to sources known to HardenStance. In the absence of other information, this suggests that at this juncture NSS Labs remains intent on pursuing its antitrust suit against AMTSO.
- **Introducing advanced machine learning and AI into the End Point Protection (EPP) and Endpoint Detection and Response (EDR) space has created new challenges in benchmarking these products accurately**. The architectures of many of these products differ greatly, for example as regards their interaction with enterprise environments on-premises and in the cloud, as well as with their own cloud. A related challenge is the use of cloud services and AL/ML based automation of sample processing. This introduces complexity in terms of maintaining sample hygiene. Whereas it used to take days for samples to be shared, AI/ML-driven automation now allows sample sharing in hours, minutes or potentially

even seconds. Testing different products fairly therefore requires that tests be run on different products as close to simultaneously as possible.

- **Test houses defining their own test plans with their own approach to transparency isn't suited to the changing requirements of security product testing.** The more consensual, standards-based, approach to testing being advanced by AMTSO and NetSecOPEN represents the right way forward now. NetSecOPEN is backed by nearly all the big Next Gen Firewall (NGFW) vendors. AMTSO is supported by nearly all the major vendors in the AV and EPP/EDR space.
- **NSS Labs is committing the cardinal failing identified by Cisco's former CEO, John Chambers: it is missing a market transition.** NSS Labs doubtless has a lot of excellent people. It could be a leader in supporting testing based on AMTSO and NetSecOPEN standards. But rather than evolving its business model to emerging requirements, NSS Labs management appears set on fighting them.

Vendors need to be incentivized by their customers to wean themselves off their dependence on the traditional test house-defined test results.

- **Security vendors continue to face what HardenStance refers to as the IT security equivalent of 'St Augustine's Test'.** Leading vendors are riding 'both horses' – working with incumbent test houses on their own testing methodologies as well as cooperating in open standards bodies. It was Saint Augustine who is said to have prayed "Lord, make me chaste [sexually pure] but not yet". Similarly, it's one thing for vendors to publicly embrace the ideal of more transparent, real-world, testing standards within AMTSO and NetSecOPEN. It's another thing for them to actually use certification around these new standards front and centre in their day to day sales engagements - especially if the certified performance outcomes aren't as good as those coming from a test house's own test methodology.
- **NetSecOPEN and AMTSO are chalking up important technical and commercial milestones.** Arriving at agreed testing methodologies through multi-party, standards-based, consensus inevitably takes time. In particular it takes longer than any one test house takes doing it by itself. That may be the price of consensus but it's a price worth paying. NetSecOPEN and AMTSO do also have recent and upcoming milestones that count in the market-place. A week ago Spirent announced that it has fully incorporated the NetSecOPEN test suite into its CyberFlood testing platform. The first certification testing of NGFW products to NetSecOPEN standards is due to get underway in June, leveraging both Spirent and IXIA test kit. A year ago AMTSO announced the adoption of its first testing protocol standard. This prescribes how test houses must disclose the way their tests were conducted in order to achieve AMTSO certification.
- **More testing capacity needs to be dedicated to open testing standards.** The European Advanced Networking Test Centre (EANTC) and the University of New Hampshire InterOperability Laboratory (UNH-IOL) are both ready to serve as NetSecOPEN certification houses. That's a good start but more participants need to join to provide the right level of capacity and competition for a thriving ecosystem.
- **User organizations are not doing enough to support AMTSO and NetSecOPEN. They need to support these organizations much more vocally and find ways to participate directly in them.** Vendors need to be incentivized by their customers to wean themselves off their dependence on the traditional test house-defined test results. Users need to see greater participation by other buyers to satisfy them that their voice is being properly heard and acted upon within standards bodies like AMTSO and NetSecOPEN. Both these organizations are heavily vendor-driven today. Both need – and very much welcome – higher levels of participation by end users. ■

More Information

- Briefing: "NetSecOPEN Faces St Augustine's Test" (April 2018)
- Briefing: "AMTSO's Malware Testing Standard: Some Progress in End Point Security" (July 2018)
- Blog: "The NSS Labs Suit Shouldn't Succeed" (September 2018)
- White Paper: "AI in Cyber Security: Filtering out the Noise" (February 2019)
- HardenStance received no payment for publishing this Briefing.
- NSS Labs has declined previous interview requests with HardenStance. HardenStance did not request an interview with NSS Labs on this occasion.
- **Contact HardenStance's Principal Analyst:** patrick.donegan@hardenstance.com
- **Register here** for free email notifications whenever new IT and telecom security content is made available by HardenStance.
-

HardenStance Ltd Disclaimer of Warranty and Liability

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same. The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.