NSS Labs publishes the IT industry's first test of EPP solutions against live drive-by exploits

Date: ***Thu, 04/30/2015 - 18:26***

NSS Labs, the world's leading information security research and advisory company, announced the results of its 2015 Enterprise Endpoint Protection (EPP) test

Rob Ayoub, Research Director, NSS Labs, at NetEvents Cloud Innovation Summit, San Francisco, California

PHOTO / telecomkh.com

This test marked a technology milestone as the first to measure the defenses of endpoint solutions against hundreds of live drive-by exploits being used in active campaigns by Threat Actors, over a span of several weeks in March 2015.

The products covered in the 2015 Enterprise EPP Group Test are:

- Bitdefender Endpoint Security v5.3
- ESET Endpoint Antivirus v6.1
- Fortinet FortiClient v5.2
- F-Secure Client Security Premium v11.60
- G Data Endpoint Protection 13.1
- Kaspersky Endpoint Security v10.2.2
- Sophos Endpoint Security and Control v10.3
- Symantec Endpoint Protection v12.1
- Trend Micro OfficeScan v11.0

NSS's key findings include:

- There was a wide variance between the most and least effective products with overall protection ranging between 85.3% and 100%.
- Consistency of protection over time is important: The less effective products fluctuated between 62% and 100% instantaneous protection throughout the test.
- Cloud makes a difference: Products with strong cloud-based reputation systems demonstrated more effective protection than those without.

"The adaptation of cloud-based technologies has resulted in dramatic improvements in the security effectiveness of endpoint protection solutions," said Randy Abrams, Research Director at NSS Labs. "In addition to increasing expertise in detecting exploits, endpoint protection products are leveraging cloud-based technologies to block both known and unknown exploits."