

<http://pcworld.com.ph/from-bad-boy-hacker-to-founder-and-cto-of-silicon-valley-%E2%80%99Hot-start-up%E2%80%9D-palo-alto-networks-%E2%80%93-nir-zuk-launches-netevents-2011-apac-summit/>

## **From bad boy hacker to founder and CTO of Silicon Valley “hot start-up” Palo Alto Networks – Nir Zuk launches NetEvents 2011 APAC Summit**

November 18, 2011

New threats demand new solutions.

This, according to CTO of Palo Alto Networks Nir Zuk, is something that needs to be realized by businesses.

Speaking at the opening keynote of the NetEvents 2011 APAC Summit, the founder and CTO of one of this year’s most talked-about Silicon Valley start-ups highlighted the complexity of the IT security problems facing enterprises today. He explained how hackers were becoming highly professional, financially motivated, and are able easily to penetrate the perimeter defences of the corporation.

“It takes just five steps,” said Zuk, as he detailed the way that hackers target individual employees using social media, and persuade them to open a back door into the enterprise network by downloading an infected document that appears to contain information about one of their hobbies or interests.

Zuk said that it takes security companies two months to respond to such attacks because they are not widespread but

highly targeted.

“If it only happens once, security vendors will not find it,” Zuk said. “And even then it can take a week or more to fix. Every executable is a suspect, and there aren’t enough security researchers in the world to fix all the vulnerabilities.”

Zuk said that his company’s firewall technology fixes the problem because it looks at all documents and executables in a virtual machine and watches for malware-like behaviour. “We do it in software in

a datacentre and generate signatures for each piece of malware," Zuk said. "We can then block it within an hour."

Zuk created some of the first computer viruses before going straight and laying the foundations for stateful inspection, a technique now used by all firewalls, and intruder prevention systems, which offer inline protection for enterprise networks.