

InformationWeek

http://informationweek.in/Security/11-11-24/Palo_Alto_aims_to_counter_malware_in_one_hour.aspx

Palo Alto aims to counter malware in one hour

Palo Alto Networks discussed the changing security landscape in enterprises at the recently concluded NetEvents APAC summit held in Phuket, Thailand By [Ayushman Baruah](#), InformationWeek, November 24, 2011

The complexity of IT security problems facing enterprises is increasing by the day. Hackers are becoming highly professional, financially motivated and more targeted. To counter the rising targeted malware attacks, network security company Palo Alto Network recently launched the WildFire, a cloud-based service where all Palo Alto devices in the world, with the flip of a switch can start sending objects to it.

“The objects get scanned within a few minutes and the customer gets back a message if it was a new exploit or a new attack that nobody has seen before. And in the next signature update which today is about 24 hours, the entire customer base is protected against that attack,” Nir Zuk, CTO of Palo Alto Networks said.



The objects get scanned within a few minutes and the customer gets back a message if it was a new exploit or a new attack that nobody has seen before. And in the next signature update which today is about 24 hours, the entire customer base is protected against that attack

Nir Zuk, CTO, Palo Alto Networks

The network security vendor in fact claims to bring down the response time to one hour with the future version of WildFire. The claim is huge given that traditional security companies take a few weeks or a more than a month to do the same.

Zuk explained the changing nature of the attacks as to how attackers these days do not directly attack the data center but they attack an end-user that has access to the data center. "It takes just five steps," said Zuk, as he detailed the way 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. Moreover, "If it only happens once, security vendors will not find it," he 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."

"Our 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 data center and generate signatures for each piece of malware," Zuk said.

Palo Alto has been selling products for more than four years now and they are being used by more than 5,000 enterprise customers worldwide. More than 20 of these customers, such as Qualcomm, eBay, Cricket, VeriSign, and the Los Angeles Community College District, have deployed over USD 1 million worth of Palo Alto Networks next-generation firewalls.

(The writer was hosted by NetEvents in Phuket)