



www.ciol.com/Security/Enterprise-Security/News-Reports/'Not-enough-security-researchers-in-the-world'/157165/0/

NetEvents APAC & Analyst Press Summit 'Not enough security researchers in the world'

With the rise in number of targeted attacks today, there are not enough security researchers in the world that can detect, monitor and analysis those attacks and create signatures in quick time, says Nir Zuk, Palo Alto Networks' founder & CTO

Pankaj Maru

Tuesday, November 29, 2011

PHUKET, THAILAND: “There have been numerous attacks against companies like RSA, [Sony PlayStation](#), Epsilon, Google’s Gmail and others, where the attackers used a new kind of malware,” said Nir Zuk, Palo Alto Networks’ founder & CTO, during his keynote address at NetEvents APAC & Analyst Press Summit.

Giving detailed insight into those attacks, Zuk pointed that the attackers first identify any victim within the organization using professional network sites, then the victim is attacked and credentials are used to target attack on [datacenters](#) to steal information.

Today’s attackers are well organized whereby some states and nations are being involved in carrying out targeted or specific attacks that bring more money rather than attacking millions of machines as happened in past.

'Spear phishing,' according to Zuk, the new five step attack method exploits vulnerability at each and every step, wherein the traditional network security or intrusion protection system (IPS) can only scan web browsing and emails, but fails to scan all other applications such as [Skype](#), SharePoint, Excel sheets, PowerPoint presentations and PDF documents.

“It takes many months from the time of an attack happens and until the IPS industry responds to it. It can take two months or even more and the reason is these are targeted attacks and not widespread attacks,” Zuk pointed out.

“If those attack are untraced in short time than an IPS vendor would need to hire an army of tens of thousands of security analysts to analyze each and every PDF document, Excel sheet or PowerPoint presentation moving or entering into the network to check if they are good or bad,” he argued.

In comparison with wild attacks in past, Zuk stressed that today a single PDF document or PowerPoint presentation can ruin the company, bring down an entire network and steal all the data and information.

“It’s impossible today to research each and every documents and executable downloads. There aren’t enough researchers in the world to do that. That’s the real problem why IPS today takes two months or more to detect a targeted attack.”

Such delays are “just unacceptable” and there’s need to be able to respond much quicker. “The situation is bad as today’s technology cannot stop targeted attacks as the IPS or anti virus vendor doesn’t come up with signatures in quick time to block those targeted attacks.”

With targeted attacks there are too many things to analyze. “We have to analyze each and every document, files, MP3s, websites and URLs because even one of them coming or getting on a network to an end-user can bring down the datacenter or at least get all the data leak from datacenter to the world,” Zuk added.

He suggested that we need to completely automate the process of analyzing objects and respond to attacks by replacing the security researcher with an automated software system using concepts like a sand box.

Further Zuk said his company has developed a firewall technology that addresses the security issues by analyzing documents and executables in virtual machines and then detect for any malware behaviors.

“These behaviors are monitored by software system in a datacenter and accordingly generate signatures for malware and blocks them. We can block it within an hour,” Zuk claimed.

(Author was hosted by NetEvents APAC & Analyst Press Summit in Phuket, Thailand)

©CyberMedia News