The Cloud Computing News India
News And Info On Cloud Computing And Virtualization

http://cloudcomputingnews.in/javelin-networks-redefines-detection-and-prevention-of-active-cyberattacks/

Javelin Networks Redefines Detection and Prevention of Active Cyberattacks

26/09/16

September 26, 2016

Emerging from stealth mode, Silicon Valley start-up uses Artificial Intelligence to prevent any malicious movement inside an organization.

Javelin Networks, the only company able to effortlessly prevent an attacker from stealing credentials and moving laterally, announced its emergence from stealth mode to unveil its breakthrough cyber defense software solution.

Javelin ZeroMove uses artificial intelligence to autonomously randomize the internal topology of organizations and expose cyber attacker movements, preventing them from further penetrating an organization. The Javelin solution is generally available to customers worldwide.

“IT staff are constantly and manually searching for attackers on computers and networks. It’s impossible to do this adequately and accurately with the technology and processes used today”, said Roi Abutbul, founder and CEO of Javelin Networks.

“We saw a pressing need for a proactive, autonomous and seamless, post-breach attack detection and prevention solution that automates attacker detection and stops their subsequent movement,” Roi added.

Nine out of ten companies have been compromised, whether by stolen remote access credentials, third party network connections, web and API vulnerability exploits or malware according to HBS studies.

In order for the attacks to progress, attackers need knowledge of the organization’s internal topology: the critical servers, identities, applications and endpoints. Once they’re on a computer, they begin internal reconnaissance, collecting information and planning their next move based on what they’ve discovered. Javelin Networks unique approach makes what the attacker learns – useless.

To thwart attackers, Javelin is applying a radically new approach to masking the attacker’s view of the internal topology. When attackers move within the masked topology they are detected immediately. Simultaneously all forensics evidence is collected before the attacker can delete it and the mitigation process is initiated, preventing the attacker from further movement.
Photo: Greg Fitzgerald, COO of Javelin Networks
(NetEvents)