http://www.tynglobal.com/javelin-networks-redefines-detection-and-prevention-of-active-cyberattacks/

Javelin Networks redefines detection and prevention of active cyberattacks

23/09/16

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.

TYN STAFF

Javelin Networks 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 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.”

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.

Regardless of how attackers have successfully penetrated a machine, whether an internal server or a user’s computer, they initiate two actions: They model the environment looking for assets, such as servers or desktops, where they can move or expand the breach and they attempt to steal identities such as usernames, passwords and other credentials that will allow privileged access to servers, databases, security tools and other network-attached equipment without further detection.

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.

Javelin ZeroMove, next generation attacker detection and prevention system immediately and unmistakably detects attacker’s activities within the obfuscated environment and takes action to isolate the breached device. It’s a simple, undetectable, agentless approach to actively detect and prevent intruders where they naturally proceed in the attack sequence, without false positives, heavy network traffic, or operational overhead. Using artificial intelligence within Javelin ZeroMove enables it to autonomously build and maintain a consistent, customized mask topology across all devices in the enterprise. With Javelin ZeroMove, it’s now possible to effortlessly prevent malicious movement inside the network.