Securing Network Assets when Exposed to the Mobile Internet

MAHWAH, N.J., /PRNewswire-FirstCall/ -- With smartphone adoption on the rise across professional users, IT departments have found themselves alerted to a new bevy of corporate network security threats. Offering insight on the types of security dangers opened up by the habits of mobile Internet users. Radware, a provider of integrated application delivery and network security solutions for business-smart networking, is helping enterprises understand, address and deploy new security technologies to protect corporate assets when exposed to the mobile Internet.

The combination of smartphones, characterized by all portable computing devices that run standard operating systems and networking stacks, and 3G connectivity services, open the device to being a preferable target for attackers that seek to misuse the phone's software in the same manner that desktop and laptop computers can be hacked into when connected to non-secure DSL/cable lines at the home, the office, or on a hot spot.

Smartphones, left exposed to mobile Internet threats, can cause a corporate network to fall victim to one or more of the following attacks:

•Battery Drain: A type of attack that sends packets to a mobile device preventing it from going into sleep mode. The attack can involve as little as sending 40 bytes every 10 seconds and wastes resources to drain the smartphone battery.

•Malware Spread: While an organization's IT department may invest resources to secure internal applications and users, they traditionally do not place emphasis on how to secure the network from individual users' smartphones. Malware can infect a user's smartphone from the public mobile network, and then spread to the corporate network, bypassing perimeter security measures.

•Misuse of Smartphone Resources: Smartphones are an easy recruitment target into botnets. Botnet operators can install bot malware and then remotely control the smartphone to send spam or launch network attacks such as network flooding, application flooding, brute force, network scanning, application vulnerability hacking and more. In this case, the botnet operator takes advantage of the smartphone's security lag, when the device is connected to a high speed mobile Internet connection.

"A combination of security technologies must be deployed across the corporate network to mitigate application attacks caused when mobile devices are 'opened up' to threats from social networking sites, sending/receiving emails, or searching the Internet," said Avi Chesla, Vice President, Security and Management Products, Radware. "By 2011-12, we expect organizations will implement a mix of standard signature, IP and website reputation feeds and behavioral-based real-time signature

technologies, based on adaptive expert systems, to fight emerging mobile threats."

Looking at comprehensive ways to mitigate mobile device attacks from permeating the corporate environment, Radware recommends a solution of signature detection technology coupled with network behavioral analysis (NBA) technologies.

By pairing these two technologies, IT organizations can ward off malware and botnet attacks based on action and user profile; without the need for millions of signatures to block every instance of malware that exists out in the mobile network. Chesla continued, "Signature detection technology has been in the industry for nearly 20-years, and was designed to detect attacks that exploit known application vulnerabilities but not zero-minute malware and application misuse attacks. Therefore, adding a complementary behavioral analysis system allows IT departments to have greater control of their network domain."

Behavioral analysis technologies create a baseline of normal user, application transaction and network bandwidth behavior. A behavioral engine has the ability to detect - in real time - cyber/mobile criminal activities that run attacks by misusing the application and network resources or by exploiting zero-minute application vulnerabilities. It then automatically creates a real-time signature that characterizes the attack pattern accurately to filter out malicious activity - without blocking legitimate user traffic.

Radware is currently working with organizations from around the world to minimize network downtime and resource risk associated with the increase of smartphone usage in the enterprise. To protect network applications, Radware offers its award-winning DefensePro® real-time network attack prevention device that includes a set of security modules--DoS (Denial of Service) protection, NBA and IPS (Intrusion Prevention System)--to fully protect networks against known and emerging network security threats. DefensePro employs multiple detection and prevention engines including signature detection, protocol and traffic anomaly detection, heuristics and behavioral analysis.

The competitive advantage of DefensePro is its patent protected behavioral based real-time signatures technology that detects and mitigates emerging network attacks in real time such as zero-minute attacks, DoS/DDoS (Distributed Denial of Service) attacks, application misuse attacks, network and application scanning, and malware spread - all without the need for human intervention and without blocking legitimate user traffic.

Source URL (retrieved on *05/05/2015 - 12:21pm*):
http://www.wirelessdesignmag.com/news/2010/08/securing-network-assets-when-exposed-mobile-internet