



DAMBALLA

Take Back Command & Control

“Damballa has found that they are in the right place at the right time. Their focus on fighting botnets turns out to be just what people are looking for post Google-Aurora.”

*Best of Show
RSA Conference 2010
Richard Steinnon
President, IT Harvest*

“Stealthy, sophisticated malware masterfully exploits the blind spots of legacy security – leaving enterprises exposed to loss and unwitting participation in deplorable forms of criminal and state-sponsored campaigns. We’re pleased to see Damballa focused on modern, under-addressed threats.”

*Joshua Corman
Research Director/Security
The 451 Group*

Damballa, Inc.

817 W. Peachtree Street NW
Suite 800
Atlanta, GA 30308 USA
404-961-7400
sales@damballa.com

www.damballa.com
blog.damballa.com
Twitter: DamballaInc

A Clear and Very Present Danger

Remote-controlled cybercrime attacks on corporate networks are the latest, and potentially most damaging, security threat to any business. Using ‘botnets’ or advanced persistent threats (APTs), criminals evade detection by traditional security solutions and steal intellectual property, corporate secrets, credit card data, and expose the corporation to criminal and state-sponsored campaigns. Google’s now-famous announcement of the Aurora attack in January triggered a stream of similar announcements from other Fortune 1000 companies. In fact, companies are beginning to list these attacks as business risks in their 10K filings.

The tools and techniques for launching these attacks are increasingly easy to acquire and the criminal operators are well funded, patient and relentless. Unlike the ‘hackers’ of yesterday who sought notoriety, these criminals are financially motivated and intentionally stealthy – the longer they remain undetected on a network the more value they can gain.

A New Solution for a New Threat

These ‘botnet’ attacks are successful because criminal operators know how to disable or evade detection by existing antivirus software and intrusion protection solutions. Simply put, criminals change the game faster than these vendors can keep up. The main difference between this new threat and the ‘viruses’ of old is the ability for the criminals to take command-and-control (CnC) of the systems within an enterprise network.

At Damballa we know it is not a matter of ‘if’, but ‘when’ an organization will be attacked and compromised. The only way to protect corporate assets is to detect, and then sever this CnC communication, rendering the botnet ‘dumb’ and ineffective. Damballa is the only company that targets and terminates this CnC activity. Born from research by recognized world experts at Georgia Tech, and perfected through installations in some of the world’s largest enterprise networks and Internet Service Providers, Damballa provides a critical layer of defense needed to protect the enterprise from these devastating attacks.

The Damballa solution:

- Detects CnC activity, terminates the threat, and provides detailed forensic evidence
- Deploys ‘out of band’ on the network, meaning that it cannot be evaded, and will not negatively impact network performance or reliability.
- Easily integrates with existing security solutions (e.g. McAfee, ArcSight, Lancope).