

About Damballa, Inc.

- Founded:** April 2006 with core technology from Georgia Tech
- Headquarters:** Damballa is privately held and headquartered in Atlanta, Georgia
- Funding:** Series A, \$2.5 million; Series B, \$6 million; Series C, \$8.2 million
- Focus:** Damballa closes botnet security gaps through high-fidelity detection and mitigation. Damballa also improves security by integrating easily with existing workflow and event management applications. Our products identify bot-driven threats that evade other technologies, even when malware can't be detected, by monitoring the Command-and-Control (CnC) that links individual bots together.
- Technology:** As the pioneering leader in stopping botnet breaches, Damballa knows that the only way to combat bots is to understand the full breadth of their capabilities, propagation, and Command-and-Control. This approach includes deep research and analysis into the uniquely networked and borderless nature of botnets – something very different from simple signatures or packet analysis. Damballa's powerful insight quickly identifies individual compromised machines and entire compromised networks operating internationally across corporate boundaries. This signatureless technology works in real-time to contain, mitigate and remediate these critical security breaches. The end result is dramatically improved security both inside and outside the network perimeter, and rapid restoration of control over compromised systems. Damballa has four patents pending.
- Solutions:** Damballa's Failsafe appliances automatically identify botnet activity across enterprise networks without requiring malware signatures or network behavior profiles. Failsafe operates as a standalone product with its own management console for automated capture and analysis of bot threats, and as an added-value in-the-cloud offering that transfers captured malware and network metadata to Damballa for increased granularity of analysis. Failsafe contains and mitigates botnet threats by integrating into existing security workflow and event management systems. As a result, it helps existing security investments work faster and more effectively.
- Benefits:** Real-time identification of bot-driven attacks that evade signature-based host, LAN and gateway security technologies.
- Fast, accurate identification and isolation of botnet activity inside the enterprise, even before actual malware or compromised systems have been detected.
- Accelerated containment and mitigation of botnets via easy integration with existing security workflow and event management systems.
- Customers:** Global 1000 corporations, large Internet service providers, OEM partners and government agencies use Damballa's signatureless solutions and industry-leading research to reinforce existing security infrastructure and stop hidden botnet attacks.
- Contact:** Damballa, Inc.
817 W. Peachtree St. NW, Suite A-110
Atlanta, GA 30308
404-961-7400
sales@damballa.com
www.damballa.com
blog.damballa.com