



FOR IMMEDIATE RELEASE

Damballa Solutions Showcased in Leading Industry Analyst Firm's Case Study

IT Security Industry Experts Continue to Emphasize Growing Concern Over Targeted Attacks and the Importance of Early Detection

ATLANTA – October 6, 2008 – Damballa, Inc. (www.damballa.com), the Internet security company focused exclusively on targeted threats such as BotArmies, announced today that the company was referenced in a September 11, 2008 Gartner, Inc. report titled, "***Case Study: Early Detection of PCs That Have Been Compromised via Botnet Clients***," authored by John Pescatore and Adam Hils. The case study discusses the effectiveness of Damballa's solution within an industry leading, multi-national consumer products organization.

Damballa's innovative technology stops targeted threats that other technologies miss and quickly restores control over compromised hosts. From the case study, "One of the most-effective distribution mechanisms for these attacks has been through botnets, where PCs are compromised with botnet client software that is usually delivered via compromised Web sites that a user has visited. The compromised PCs can be 'rented' by any financially motivated attackers, and the initial botnet client is used to download targeted malware, such as password stealers or database harvesters." Damballa identifies the presence, severity and intent of targeted attacks that are designed to evade existing security.

It has been well noted by industry experts that traditional forms of IT security – specifically antivirus, IDS/IPS, and content filtering – are insufficient when it comes to innovative threats such as targeted attacks. As stated in the Gartner case study, "Traditional signature-based defenses are inadequate against targeted attacks and must be augmented." Also stated in the report, "Enterprise security officers shouldn't assume that compromises haven't occurred, just because their antivirus, host IPS and network IPS tools don't detect botnet-infected PCs." In addition, "Getting IT operations to acknowledge and remediate botnet-compromised endpoints is critical. It's especially difficult when IT operations are outsourced."

The types of threats covered in the case study are widespread and dangerous. Damballa typically discovers that 3-5% of enterprise assets are compromised – even in the presence of the best and most up-to-date security. According to another Gartner report from September 22, 2008, "***Hype Cycle for Infrastructure Protection, 2008***," authored by Greg Young, Kelly M. Kavanagh, John Pescatore, Adam Hils, Mark Nicolett, Neil MacDonald, Vic Wheatman, Peter Firstbrook, Jeffrey Wheatman, John Girard, Lawrence Orans, Ray Wagner, Joseph Feiman, L. Frank Kenney, Earl Perkins, "Gartner estimates that 3% to 7% of typical enterprise PCs are



compromised with a bot client, while consumer PCs are in the 5%-to-15% range.” This report also notes that, “...financially motivated, targeted attacks via bot clients are starting to cause more local damage, leading to increased attention and a need to mitigate the threats.”

To read the report, “**Case Study: Early Detection of PCs That Have Been Compromised via Botnet Clients**” by Gartner, Inc., please go to the Damballa Web site home page at www.damballa.com (no registration required).

For an ongoing discussion of targeted attacks and their impact on the enterprise, visit the Damballa blog - The Day Before Zero - at <http://blog.damballa.com>.

About Damballa, Inc.

Damballa protects businesses from targeted attacks used for organized, online crime by using the Internet cloud to identify and isolate threats that evade other technologies. Our unique, global approach monitors the Command-and-Control (CnC) needed to launch these attacks as well as compromised systems, which enables immediate identification and mitigation of malicious activity. 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 Internet attacks. The result is dramatically improved security both inside and outside the network perimeter. Damballa (www.damballa.com) is privately held and headquartered in Atlanta, Georgia.

###

CONTACT:

Ashley Vandiver
Damballa, Inc.
ashleyv@damballa.com
Mobile: (404) 432-8657
Office: (404) 961-7404