



FOR IMMEDIATE RELEASE

Damballa's Failsafe Solution Provides Next Generation of Targeted Threat Identification and Protection

Failsafe 2.0 Offers Broader Coverage Through Multi-perspective Analysis of Targeted Threat Activity

ATLANTA – July 14, 2008 – Damballa, Inc., the only Internet security company focused exclusively on targeted threats such as BotArmies, today announced the release of the Failsafe 2.0 appliance. Failsafe utilizes Internet cloud participation to provide immediate identification, protection and feedback on targeted attack activity and similar compromises within an enterprise. Damballa further augments this offering with actionable intelligence for faster remediation and minimized risk to online corporate assets.

According to Gartner research¹, “The most damaging incidents are targeted attacks, which tend to use custom-crafted malware in multistage attacks.” Moreover, “Targeted attacks are a much higher risk to the bottom line, and are generally launched by more sophisticated and motivated attackers.” Gartner further stated, “A key tenet of Internet security systems must be the capability to separate and filter out random attacks to ensure a rapid response to targeted attacks.”

“In our experience working with large enterprises, we discover, on average, that 3-5% of enterprise assets are compromised – even in the presence of the best and most up-to-date security. That’s a huge gap that’s not being addressed by traditional security technologies,” said Bill Guerry, VP of Product Management and Marketing for Damballa. “Damballa closes that gap for our customers by focusing on the one constant with targeted attacks – the need for remote control. Separating that constant, something we call command-and-control, from the background noise of the Internet is challenging. But it empowers our customers to anticipate an attacker’s next move and thus effectively isolate and remediate any issues before expensive damage can happen.”

Placed at key Internet access points and network intersections, Failsafe identifies internal activity from targeted attacks, notifies in real-time when a new compromise is detected, and defends the enterprise from malicious activity.

Failsafe 2.0 includes:

- **Virtually no false positives due to evidence capture** – Legacy technologies such as antivirus (AV) or intrusion prevention systems (IPS) typically rely on a very small sample of overall enterprise network traffic to trigger an action. Since they react to as little as a single file or a handful of packets, they are very prone to false positives. Damballa concentrates on

¹ John Pescatore, Vice President and Distinguished Analyst, Gartner, Inc., *Gartner's Threat Forecast Timeline*, June 4, 2008.



the communications between compromised systems and actual command-and-control (CnC) nodes on the Internet. As a result, each Failsafe appliance can positively identify compromised hosts with very little chance of a false positive.

- **The ability to identify the compromise of “One”** – Targeted threats come in all shapes and sizes. While the popular media focuses on the largest and most prolific spamming armies, it is often the army of one that is most threatening to the enterprise. Failsafe 2.0 identifies malware armies of all sizes within an enterprise. By selectively sampling network traffic to separate “low and slow” attacks from the merely suspicious activity, Damballa uncovers even single compromises that threaten network data integrity.
- **Real-time intelligence on the activity of the army** – Damballa’s technology includes built-in intelligence that understands the crimes targeted attacks are commanded to perpetrate. We focus on the critical communications between CnC and compromised hosts that must take place. This allows our customers to address the threat before any criminal activity is actual perpetrated.
- **Actionable information to prevent compromises** – Damballa’s Failsafe 2.0 solution tracks assets throughout the compromise lifecycle. As a result, Damballa monitors suspicious host activity that carries a high probability of a future compromise. Customers use this information to stop compromises from occurring.

Damballa offers enhanced reporting of compromised assets, as well as targeted reporting for specific threats that are important to a customer’s particular enterprise. This threat severity model provides customer-specific risk ratings per compromise and per client, with details that include:

- Number of compromises
- Compromise activity level
- Binary update frequency
- Binary capabilities

For more information on Failsafe 2.0 and other Damballa solutions, please visit www.damballa.com or call 404-961-7400.

Damballa’s solutions provide comprehensive, real-time visibility into targeted attack activity both inside the enterprise and across the Internet. Damballa’s insight often predicts attacks before they arrive, or before they can damage corporate assets. In addition, Damballa gives customers the ability to disrupt and resolve targeted attack compromises so that remediation can take place in a planned, orderly manner.

About Damballa, Inc.

Damballa protects businesses from targeted attacks used for organized, online crime. Its unique, global approach rapidly isolates the command-and-control needed to launch multi-network attacks. Damballa’s signatureless solutions improve security both inside and outside the network perimeter, to stop threats other technologies miss and restore control to legitimate owners. Damballa identifies the severity and intent of targeted attacks such as BotArmies, even when malware can’t be detected. Its products and services provide a critical window for orderly remediation, and integrate easily into existing infrastructure



without requiring additional headcount or complexity. Damballa is privately held, and is headquartered in Atlanta, Georgia.

###

CONTACT:

Ashley Vandiver

Damballa, Inc.

ashleyv@damballa.com

Mobile: (404) 432-8657

Office: (404) 961-7404