



**FOR IMMEDIATE RELEASE**

Media Contacts:	Joel Deitch	Bill Keeler/Tiffany Archambault
	Damballa Inc.	Schwartz Communications
	404-961-7402	781-684-0770
	<a href="mailto:jdeitch@damballa.com">jdeitch@damballa.com</a>	<a href="mailto:damballa@schwartz-pr.com">damballa@schwartz-pr.com</a>

**Damballa Terminates Botnets and Crimeware Threats  
That Compromise Fortune 1000 Enterprises**

*New Technology Severs Communications to and from Botnets  
and Advanced Persistent Threat Controllers in Real-Time*

**ATLANTA—March 1, 2010—**[Damballa](#), the company that enables organizations to take back command-and-control from botnets and other remote-control threats, today launched real-time [Active Threat Termination](#) technology. Damballa's Failsafe 4.0 severs criminal remote control over enterprise computers. This new release detects and terminates botnets, advanced persistent threats (APTs) and other crimeware activity that relies on network-based Command-and-Control (CnC) to commit fraud, steal confidential information and use compromised systems for criminal attacks against other organizations. This Active Threat Termination technology identifies and stops malicious network activity without disrupting employee productivity or legitimate communications.

“At Damballa, we invest in understanding not just the threats, but the methods, infrastructure and criminals behind them,” said Val Rahmani, CEO, Damballa. “We know that the threat is much greater than spam or theft of credit card numbers. It is industrial espionage, brand degradation, fiduciary liability and financial loss. That's why we're excited to deliver this unique ability to identify and terminate these threats.”

Positioned at strategic Internet access points and network intersections, Damballa's industry-leading detection and Active Threat Termination technology cannot be detected by crimeware seeking to evade discovery. It proactively identifies compromised systems and internal activity typical of botnets and other remote control threats without requiring malware signatures for each individual malware infestation. It performs this high level of protection without affecting normal network operations or slowing network performance.

Damballa knows that enterprise systems are and will continue to be compromised, even for organizations with sophisticated network defenses. Damballa's focus on Command-and-Control utilizes advanced machine learning techniques to identify the patterns used by criminal operators, enabling swift detection of emerging threats before corporate

machines are used for harmful criminal activity. Damballa also integrates easily with event management and forensics applications, which helps existing security investments operate more efficiently and effectively.

“Damballa not only detects the enterprise assets that are under the control of cyber criminals, but then cuts off malicious communications and alerts the customer to the breach,” said Stephen Newman, director of product management, Damballa. “By severing a criminal’s ability to infiltrate and operate undetected inside an enterprise in real-time, Damballa gives IT administrators the advanced detection and termination technology they need to take back command and control of their networks.”

### **Product Availability**

Failsafe 4.0 is available immediately. For more information, contact [info@damballa.com](mailto:info@damballa.com) or call 404-961-7400.

### **Advanced Persistent Threat Audit for Fortune 1000 Companies**

The typical Fortune 1000 company has between 5-10 percent of its systems under botnet control. Damballa is ready to deliver an on-site audit designed to uncover botnets, APTs and other remotely controlled threats active inside the enterprise. Each audit identifies security breaches and makes recommendations for organizations seeking to aggressively stop these threats. Visit Damballa at <http://landing.damballa.com/APTaudit.html> for more information.

### **RSA Conference Demonstrations**

Damballa will demonstrate its industry-leading detection and Active Threat Termination technology next week at the RSA Conference. Media and analysts interested in Failsafe 4.0 should contact Bill Keeler or Tiffany Archambault of Schwartz Communications at (781) 684-0770 or [damballa@schwartz-pr.com](mailto:damballa@schwartz-pr.com). Contact Damballa directly at <http://www.damballa.com>, or visit Damballa at RSA Booth #728.

### **About Damballa, Inc.**

Damballa stops crimeware threats that exploit enterprise networks for illegal activity by finding and disrupting the hidden communications channels used to control internal servers and hosts. This concentrated focus on malicious remote control delivers fast, accurate insight into advanced network threats, including termination of criminal activity and remediation guidance. Damballa’s technology integrates easily with existing infrastructure for cost-effective protection against dangerous security breaches that evade other solutions. The result is smarter, more flexible network security that stops current and future threats, prevents fiduciary breaches and enhances regulatory compliance. Damballa’s customers include major banks, Internet service providers, government agencies, educational organizations, manufacturers and other organizations concerned with taking back the command-and-control of their networks. Privately held, Damballa is headquartered in Atlanta, GA.

###