



FOR IMMEDIATE RELEASE

3% to 5% of Enterprise Assets are Compromised by Bot-driven Targeted Attack Malware

Damballa's Failsafe Appliance Captures Five Times More Botnet Attack Activity Inside Enterprise Networks than Traditional Security Defenses¹

ATLANTA – March 2, 2008 – Damballa, Inc. today announced the release of the Failsafe 3.0 appliance. Failsafe provides real-time identification and protection against bot-driven targeted attack activity taking place inside enterprise networks. These appliances employ a multi-perspective analysis of targeted attack activity that concentrates on the communications between compromised systems and actual Command-and-Control (CnC) nodes on the Internet. As a result, Failsafe identifies compromised hosts that other technologies miss, with very little chance of a false positive.

“Our customers wanted three things: faster, more accurate recognition of botnet compromises; better information for driving remediation and forensic response; and the ability to leverage Failsafe either as a service or as a standalone product. We directly answered these needs with Failsafe 3.0. It’s a huge step forward in terms of stopping Zero-Day and targeted attacks,” said Bill Guerry, VP of Product Management and Marketing for Damballa.

Damballa is the only Internet security company focused exclusively on bot-driven targeted attacks. Their real-world research indicates 3% to 5% of enterprise assets are compromised with targeted attack/bot malware – even in the presence of the best and most up-to-date security tools. This is due in part to the fact that enterprise-grade antivirus and IDS/IPS fail to capture 20% to 70% of new threats, including targeted attacks and common Trojan attacks².

According to Gartner research³, “Signature-based malware detection is reactive and limited to catching only well-known malware. It does not have as high a detection rate against threats such as targeted hacks, custom malware and/or zero-day malware.”

These bot-driven targeted attacks are the most damaging, hardest to find network security challenge today. The malware driving these attacks has overwhelmed enterprise antivirus solutions and other signature-based defenses by morphing faster than they can respond. As a result, security administrators use Failsafe to close the delay between when new malware is released into the wild and when an antivirus or IDS/IPS engine can be updated to detect it.

A study by Damballa demonstrated that the typical gap between malware release and detection/remediation using antivirus is 54 days. The study was comprised of over 200,000

¹ Damballa, Inc. research based on real-world active deployments

² Damballa, Inc. research based on real-world active deployments

³ Peter Firstbrook, Research Director, Gartner, Inc., *Unix and Linux Servers Rarely Benefit From Signature-Based Antivirus Software*, November 13, 2008



malware samples scanned by a leading industry antivirus tool over six months. The study also revealed that:

- Almost half of the 200,000 malware samples were not detected on the day they were received
- 15% of the samples remained undetected after 180 days

“In the battle between malware and security technologies, yesterday’s signature-based solutions have lost,” said Guerry. “For 54 days not only can enterprises who rely on AV not find compromised hosts, but even if they somehow discovered a system was compromised, they would not be able to remediate it.”

Failsafe 3.0 improves customers’ ability to respond quickly and accurately to bot-driven attacks, simplify reporting and alerting, and generate faster, more effective remediation through the following new features:

- **Granular Customer Control** – Failsafe’s Management Console gives users granular control over settings, reports, cloud participation, and updates. The Management Console maintains diagnostic information and displays it in report panels so that the user can track critical components of Failsafe’s visibility over time, as well as ensure that Failsafe performs at optimal levels.
- **Easy Integration with Third-Party API** – Failsafe 3.0 simplifies report integration with existing network and security management infrastructure to maximize the utility of existing security investments. Simply point any generic database API to the Failsafe Management Console to pull data elements into existing security and network management systems.
- **Multi-perspective Malware Capture and Analysis** – Failsafe’s signatureless malware capture and analysis employs powerful machine learning algorithms and advanced knowledge of malware CnC to capture Zero-Day malware inside enterprise networks. Failsafe’s comprehensive reporting identifies the root cause of these malware downloads so that customers can proactively prevent future compromises.
- **Flexible and Effective Cloud Participation** – Failsafe 3.0 enables customers to participate in an in-the-cloud security model that maximizes threat identification and mitigation. Cloud participation captures and leverages highly suspicious domains and malicious binary executables, while protecting the client’s confidential data – even from Damballa. Damballa then processes this information to update all Failsafe devices, whether participating in-the-cloud or not.

Failsafe 3.0 is available in March 2009. For a demo of Failsafe, visit the SANS Vendor Tool Demo site at http://www.sans.org/resources/vendor_demos/.

For more information on Failsafe and other Damballa solutions, please visit www.damballa.com or call 404-961-7400. And for an assessment of how many of your enterprise systems may be



compromised by bot-driven targeted attacks, please visit the Damballa Risk Calculator at <http://www.damballa.com/overview/risk.php>.

For an ongoing conversation about targeted threats, please visit the Damballa blog, *The Day Before Zero*, at <http://blog.damballa.com/>.

About Damballa, Inc.

Damballa protects businesses from bot-driven 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 that coordinates botnet attacks to rapidly identify compromised systems and enable immediate control 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 is privately held and headquartered in Atlanta, Georgia.

###

CONTACT:

Ashley Vandiver Damballa, Inc. ashleyv@damballa.com Mobile: (404) 432-8657 Office: (404) 961-7404	Michelle Schafer Merritt Group, Inc. schafer@merrittgrp.com Mobile: (703) 403-6377 Office: (703) 390-1525
---	---