



**FOR IMMEDIATE RELEASE**

**Damballa Discovers “Kraken” BotArmy -- Twice as Big as Storm;  
Evades Over 80% of Installed Antivirus Software**

*Company Debuts Solutions for Combating Targeted Threats at RSA 2008*

**RSA 2008, SAN FRANCISCO – April 7, 2008** – Damballa, Inc., the only Internet security company focused specifically on targeted threats such as BotArmies, announced today that the company has identified and is actively tracking a BotArmy larger than Storm. This new BotArmy, named “Kraken”, is twice as big as Storm, with over 400,000 distinct victims observed daily as compared to Storm’s 200,000 victims. Kraken has gone undetected by over 80% of computers with antivirus software installed.

“Kraken is the largest army we’ve seen to date and has an unprecedented presence in enterprise networks. We’ve observed evidence of Kraken-based compromises in at least 50 of the Fortune 500,” said Paul Royal, Principal Researcher at Damballa. Using trend data, Damballa predicts Kraken will continue to grow, reaching at least 600,000 unique victims per day by mid-April with a proportional increase in compromises in enterprise networks. Individual victims in the Kraken BotArmy have been observed sending as many as 500,000 pieces of spam in a single day.

Until Kraken, Storm was widely recognized as the largest BotArmy in history. Storm’s inception by most sources dates back to January 2007. Kraken was first observed in winter 2007, but investigation into its origins suggests the existence of early variants as far back as late 2006. The BotArmy is stealthy, robust and includes redundancy mechanisms that allow the BotMaster to recover his victims in case one or more of the primary command and control (CnC) servers are disabled. Kraken also uses encrypted communications to frustrate attempts at identification and understanding. Damballa research indicates that the primary CnC servers are hosted in Russia, France and the United States.

Damballa believes Kraken uses a propagation technique based on social engineering, which is the same technique used by Storm and many other targeted attacks. The Kraken malware automatically updates itself and has the flexibility to be used as a general purpose bot for data theft or attack activity. Kraken presents itself as an image file, tricking unsuspecting users into compromising themselves when they attempt to view the fake image. To date, Kraken’s primary behavior is spamming, which includes messages offering high interest loans, gambling enticements, male enhancement techniques, pharmacy advertisements, fake watches for purchase, etc.



Damballa will begin posting a subset of Kraken-compromised unique IP addresses starting Tuesday, April 15<sup>th</sup> on the company's Web site at [www.damballa.com](http://www.damballa.com) to provide the public an opportunity to review the data collected by Damballa from this new army. For more information on Kraken and regular updates on its progress, please contact Ashley Vandiver at 404-432-8657.

Damballa is showcasing technology at RSA 2008 in San Francisco that provides deeper understanding of and protection against targeted attacks than is possible with signature-based host, LAN or gateway security technologies. These solutions provide comprehensive, real-time visibility into targeted attack rallying activity both inside the enterprise and across the Internet, which 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 attacks such as BotArmy 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. Our 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.

[avandiver@damballa.com](mailto:avandiver@damballa.com)

Mobile: (404) 432-8657

Office: (404) 961-7404