



FOR IMMEDIATE RELEASE

Damballa's Q2 Research: 40% of Targeted Threats Give Control of Enterprise Assets to Criminals

Antivirus Solutions Detect Fewer Than 20% of Targeted Threats When First Discovered in the Wild

ATLANTA – June 2, 2008 – Damballa, Inc., the only Internet security company focused specifically on targeted threats such as BotArmies, today announced findings from their second quarter analysis. As a key tool for organized crime, targeted threats continue to grow in sophistication with an elevated focus on the enterprise network.

“2008 is poised to be the year of the targeted attack,” said Paul Royal, Principal Researcher at Damballa. “Targeted threats are attacks that exploit relationships between people, what’s important to them and what they don’t know. We’ve seen enhancements to the structure, format, and presentation of these attacks, which make them more likely to successfully compromise corporate users in and get out of enterprise environments. Today’s targeted attacks evade traditional enterprise security mechanisms and perpetrate malicious activities, such as data exfiltration.”

In the second quarter of 2008, Damballa’s research team analyzed a corpus of targeted threats and discovered the following results:

- 40% of the overall targeted threats analyzed give control of enterprise assets to criminals. This is derived from the fact that 50% of targeted threats analyzed use HTTP for communications, which allows for easier criminal control. And of those, almost 80% will steal proxy settings to facilitate successful outbound communication.
- Over 75% of targeted attack Command and Control (CnC) sites are located in Asia, with China being the most dominant location.
- Almost half of the targeted threats analyzed were propagated using PDF files, with Word documents and PowerPoint presentations coming in second and third, respectively.

A recent analysis of antivirus solutions performed using VirusTotal shows that detections of newly discovered targeted attacks average less than 20%. These results follow similar and disturbing trends, which include armies rapidly adapting for self preservation. For example, in January 2007 a large portion of Bobax cannibalized itself to bootstrap Storm. More recently, just a few weeks after being widely discussed in the press, Kraken changed from using a custom protocol with encrypted content to one that uses plaintext HTTP.

Targeted threats no longer encompass malware executables with obvious extensions (e.g., .exe, .scr, .pif). Instead, documents such as PDFs are used to execute arbitrary and malicious code. These attacks are successful because most users believe that documents such as PDFs are harmless. Yet, simply viewing a PDF with a slightly out-of-date reader can place a computer



under the control of a malicious third party. In addition, when an attack is successful, the user is unlikely to know a compromise occurred.

The social engineering aspects of targeted attacks have also grown in sophistication. Instead of standard enticements normally found in spam, these attacks use subject lines which would be of importance to enterprise users. These include financial topics such as IRS complaints or notices, political topics that play off current events such as the Olympics in China, freeing Tibet, and human rights issues, and personal topics such as speaker invitations and scholarship offers.

“Enterprise organizations need to enhance their understanding of the danger targeted attacks pose to their environment. Defenses such as firewalls, IDS, and antivirus often fail to detect these new and increasingly frequent kinds of attacks,” said Royal.

Damballa is showcasing the company’s technology at the 2008 Gartner IT Security Summit June 2-4 in Washington, DC (Booth # 34). Damballa’s solutions provide 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 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 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. 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