



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

Damballa Research Paper Reveals How Political Cyber Activism Is an Increasing Threat to Businesses around the Globe

A Growing Number of Groups Are Asking Members to Deliberately Install Botnet Agents on Their Networks to Launch Online Protests

ATLANTA—April 21, 2010—[Damballa](#), the only network security company that enables organizations to take back command-and-control (CnC) from botnets and other remote-control criminal threats, today announced the availability of its newest research paper titled “The Opt-in Botnet Generation: Social Networks, Cyber Attacks, Hacktivism and Centrally-Controlled Protesting.” The paper can be downloaded at http://www.damballa.com/downloads/r_pubs/Opt-In_Botnets.pdf.

Authored by Gunter Ollmann, vice president of research for Damballa, the paper details the rapid adoption of opt-in botnets within social networking applications and Web 2.0 technologies by cyber criminals and protestors. These tools have become a powerful platform for launching crippling botnet cyber attacks against any type of business or government from anywhere in the world, and Fortune 1000 companies run the risk of becoming unknowing enablers of the attacks. The paper further examines the evolutionary path of opt-in botnets, including how tactics have changed, why anyone would willingly choose to join a botnet, and what activist botnets mean to organizations that find themselves both victims and enablers of a botnet-driven attack.

In addition to online attacks by criminal operators intent on committing crimes of ID theft and fraud, the number of non-violent attacks of ‘hacktivism’ focused on denial of service attacks, Web site defacements, and the redirection or hijacking of DNS configuration settings is also increasing. Hacktivism describes the nonviolent use of illegal or legally ambiguous cyber-attack tools in pursuit of political ends.

“The threat landscape is changing and gives criminals a quick and dirty way to centralize command-and-control capabilities on most any network leaving Fortune 1000 companies more vulnerable,” said Ollmann. “Tools and tactics that have proven invaluable for

launching political protests around the globe are being reinvented, reoriented, and subsequently attacking non-political targets. Businesses are now in the cyber-protesting cross-hairs of their customers – both past and present.”

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 computer systems. By detecting malicious remote control, Damballa solutions identify advanced network threats, terminate criminal activity in real-time and provide remediation guidance. Damballa customers include major banks, Internet service providers, government agencies, educational organizations, manufacturers and other companies typically targeted by organized cybercrime. Privately held, Damballa is headquartered in Atlanta, GA.

###