



DAMBALLA

Take Back Command & Control

Damballa has found that they are in the right place at the right time. Their focus on fighting botnets turns out to be just what people are looking for post Google-Aurora.

Best of Show
RSA Conference 2010
Richard Steinnon
President, IT Harvest

Stealthy, sophisticated malware masterfully exploits the blind spots of legacy security – leaving enterprises exposed to loss and unwitting participation in deplorable forms of criminal and state-sponsored campaigns. We're pleased to see Damballa focused on modern, under-addressed threats.

Joshua Corman
Research Director/Security
The 451 Group

Damballa
817 W. Peachtree Street NW
Suite 800
Atlanta, GA 30308 USA
404-961-7400
sales@damballa.com

www.damballa.com
blog.damballa.com
Twitter: DamballaInc

If they want to break in, they will.

Law enforcement agencies readily admit that break-ins are unstoppable – we can only hope that they will catch the bad guys before our valuables have disappeared. The same can be said for today's threat to enterprise networks. *Even the leading security suite providers admit that their anti-virus solutions are no match for the advanced nature of today's criminal malware.* Never before has so much company-critical data been stored and transmitted electronically, and never before has it been so easy to steal or, worse, criminally manipulate.

Botnets. Advanced persistent threats. Next generation malware. Cyber espionage. Insider threats. Targeted attacks.

Whatever you want to call it, the bad guys want corporate financial information, logins, customer data, intellectual property, social security numbers, or to hijack enterprise networks to launch cyber attacks against other organizations. It happened to Google, Adobe, and hundreds of other companies. And, for the first time in history, Fortune 500 companies are now disclosing this threat in their SEC 10K filings, alongside other global risks to their shareholder value.

The threat has evolved; so should corporate security practices. There is only one company that has been focused on analyzing and preparing for this threat since 2006.

Damballa.

Damballa is revolutionizing network security. Today's cyber crime is orchestrated using remote control communications via the internet, also known as command-and-control (CnC).

Cut the cord and you terminate the threat. That is what Damballa does.

Working "out-of-band", so that network performance is not impacted and the bad guys can not evade our solution, Damballa sensors automatically detect and terminate the CnC communication that is required for the criminals to operate the malware or bot agents on breached enterprise assets. Once terminated, we provide the necessary forensics to track, plan and execute timely remediation.

While every other network security company continues to fight the losing battle of prevention, **Damballa is the only company that recognizes that you can't stop the criminals from breaking in, but you can keep them from doing harm.**

Led by Val Rahmani, a 28 year IBM veteran and most recently the General Manager of IBM Internet Security Systems (ISS), the Damballa team consists of world renowned experts in cyber crime and the criminal infrastructure behind these attacks. The Damballa research team is led by Gunter Ollmann, who was the Chief Security Strategist for IBM ISS and Director of the ISS X-Force Research and Development. The Damballa team includes respected industry veterans from Trend Micro, F-Secure, Secure Computing, McAfee and the U.S. intelligence community.

No one understands this threat better than Damballa, and no other company has the technology or intelligence capable of terminating these cyber attacks. If they want to break in, they will. Damballa can keep them from doing harm.

Cyber crime is orchestrated using remote control communications via the internet.

Cut the cord and you terminate the threat.