

# Protection from Modern Cyber Threats

## Botnets, Advanced Malware, Crimeware, and Advanced Persistent Threats

Modern cyber threats have evolved. Gone are the days of mass viruses and worms that simply caused havoc for hacker notoriety. Today's targeted attacks are executed by criminal organizations using stealthy command-and-control (CnC) infrastructures to commit industrial espionage, steal enterprise information, or attack other networks.

Sophisticated malware variants used by botnets and other persistent threats are customized, dynamic, and **engineered to bypass prevention layers and signature-based defenses**, providing criminals a conduit to breached PC endpoints, confidential data residing on them, and access to other systems in the network.

## Damballa™ Failsafe. Malware Happens, Stop the Breach.

The only constant across the millions of variants of malware, crimeware, and bot agents penetrating enterprise defenses today is the **command-and-control (CnC)** communications used to issue instructions and exfiltrate information from a compromised endpoint. Damballa™ Failsafe rapidly identifies CnC behaviors and communications to and from breached endpoints and confirms the risk of each compromise.

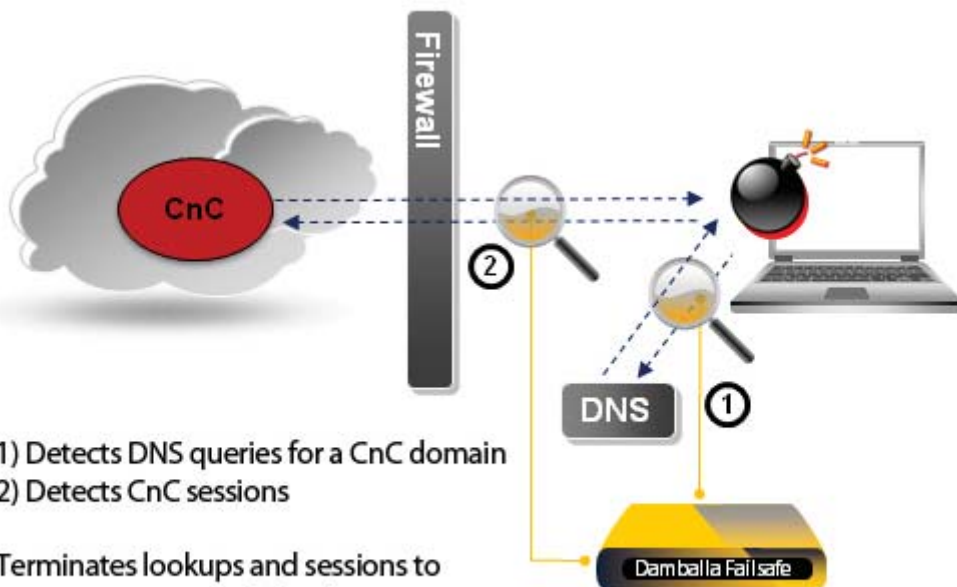
By employing multi-dimensional inspection engines, correlated intelligence, and a global reputation system, Damballa Failsafe **accurately detects known and zero-day threats** and mitigates the risk caused by these breaches by **blocking the CnC communication** from bot malware installed on compromised endpoints to criminal CnC servers.

## Fast, Accurate Detection. No Signatures Required.

Damballa Failsafe uses a system of out-of-band sensors placed in the network to passively monitor communications such as DNS queries, HTTP requests and egress transmissions for behaviors and unique fingerprints of CnC communication and correlates this data to identify compromised endpoints.

Damballa Failsafe **multiple inspection engines** detect threats by:

- Inspecting and correlating traffic patterns within the enterprise that match behavioral reputation profiles of CnC communication (eg. domain fluxing algorithm behaviors)
- Statistically analyzing enterprise DNS traffic to profile zero day CnC communication
- Capturing binaries within suspicious network communications traffic, identifying if they are malicious, and analyzing them to profile their CnC communication behavior



*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 are pleased to see Damballa focused on modern, underaddressed threats.*

Josh Corman -  
Research Director  
for Security,  
The 451 Group



### Damballa

817 W. Peachtree Street NW  
Suite 800  
Atlanta, GA 30308  
sales@damballa.com  
blog.damballa.com  
www.damballa.com  
(404) 961-7400

Working in tandem with the inspection engines is the **Damballa global reputation system**, which focuses on the infrastructure supporting CnC servers. By collecting, analyzing, and identifying CnC servers through the reputation of related domains, DNS infrastructure, network IP, and related malicious content, the Damballa global reputation system has identified and classified millions of unique CnC profiles - the largest and most accurately vetted threat knowledge bases of its kind.



## Active Threat Termination. Cut the Cord, Stop the Threat.

Active Threat Termination works in concert with Damballa™ Failsafe inspection engines as the countermeasure to a malware breach. It eliminates the criminal operators' control over a compromised endpoint by severing malicious communications to and from command-and-control servers by using two methods: preemptive termination and session termination. The ability to terminate malware CnC activity **stops the threat before they can do damage** - limiting the risk even after a breach.

Damballa Failsafe out-of-band network placement allows for termination techniques that do not impede normal network traffic, but intercedes and stops only malicious traffic so the malware itself can not communicate with its CnC infrastructure.

**Preemptive Termination** prevents malware from beginning CnC communication attempts. Damballa Failsafe identifies the DNS query for the CnC server's IP address and intercedes by acting as the DNS server and forging a DNS answer packet back to the compromised asset.

**Session Termination** identifies any CnC connection attempt and tears down the TCP session. CnC sessions initiated by malware active in an enterprise network are detected and immediately torn down by Damballa Failsafe by injecting TCP Reset packets to both the malware agent and the CnC server.

Policy control allows management of termination solutions to be enabled independently or configured to work in unison, as well as the ability to specify IP ranges to include/exclude from termination protection.

## Detailed Forensics. Rewind and Replay.

**Damballa Failsafe** provides comprehensive evidence playback for e-discovery and other forensic activities of malicious events on the network, enabling administrators to replay and see security incidents and prioritize remediation processes. Details such as evidence of communication attempts and full conversations with criminal CnC servers, identity of botnets, behaviors such as domain fluxing, specifics such as ports and protocols, and malicious binaries downloaded to hosts are all captured.

In addition, compromised asset behaviors and details are also captured, such as traffic to the installed malware (bytes in and bytes out), computer names, the connection state, and anti-virus coverage statistics. These specifics provide administrators a priority list based on asset risk profiles.

## Security Integration. Plays Well With Others.

Damballa integrates directly with **McAfee® ePO** for seamless unified host security visibility. This powerful combination delivers a network-wide view of criminal activity and the enterprise network's overall security posture.

Damballa also integrates easily and transparently into existing security workflow and management applications, such as **ArcSight's ES**M security management environment or **Lancope's StealthWatch** netflow analysis system. Damballa identifies botnet activity and compromised hosts, then passes this information to the workflow or SIEM solution.

## Contact Damballa

Find out why Fortune 500 enterprises, leading universities, internet service providers, and government agencies have chosen to deploy Damballa.

Web: [www.damballa.com](http://www.damballa.com) | Blog: [blog.damballa.com](http://blog.damballa.com) | Email: [sales@damballa.com](mailto:sales@damballa.com) | Phone: 404-961-7400

