



Advanced, Specialized Threat Protection for the Enterprise

“We are truly in an arms race when it comes to fighting cyber crime.

The criminals have vast resources and patience, and the sophistication of the infection tactics and associated malware continues to outpace our ability to block it or detect it. But even the criminals have to use the basics of the internet and DNS to communicate with the assets they infect. Advanced detection of malicious domain abuse could be the only way of staying ahead of this threat. Damballa is doing something special.”

*Kenneth A. Minihan
Lt. Gen, USAF (ret)
former Director,
National Security Agency*

Damballa Integration Partners



Damballa Inc.
817 W. Peachtree Street NW
Suite 800
Atlanta, GA 30308

Web: www.damballa.com
Blog: blog.damballa.com
Email: sales@damballa.com
Phone: 404-961-7400

Advanced Malware. Persistent Threats. Zero-Day Targeted Attacks. Modern cyber threats have evolved. Today’s targeted attacks are executed using stealthy malware and command-and-control infrastructure designed to steal corporate data and commit industrial espionage.

The sophisticated malware used in these attacks is engineered to bypass prevention layers and signature-based defenses, providing criminals a conduit to customer data, intellectual property, and trade secrets. Once stealthy malware has infected an endpoint device (PC, Mac, iPad, smartphone, etc.) it communicates with the criminal operator in the same manner a legitimate user would access the Internet.

This command-and-control (C&C) communication is used to issue instructions to the malware, steal data and credentials, and update/change the malware to further evade detection or to perform a more targeted task, making these stealthy threats the top priority for security teams across all industries.

According to recent research, on average corporate network breaches go unnoticed for more than 140 days before they are discovered. Rapid detection of the breach and termination of the criminal communication is critical to stopping data theft.

Damballa® Failsafe

Damballa® Failsafe is a purpose-built, specialized threat protection solution, which hunts for these hidden threats utilizing an array of patent-pending technologies. Damballa Failsafe:

- Automatically detects and analyzes suspicious executables and PDFs entering the network to uncover zero-day and unknown malware
- Rapidly identifies C&C behaviors and criminal traffic on your network
- Correlates the malware and communications evidence to immediately pinpoint live infections
- Terminates the criminal communications to stop data theft
- Delivers full forensic evidence and playback of events in sequence to provide actionable intelligence to remediate the breach

The Damballa Failsafe sensors monitor DNS, egress and proxy traffic and utilize multi-dimensional deep packet inspection engines to correlate suspicious behaviors to rapidly identify and isolate a breach.

Utilizing the industry’s most advanced cyber threat intelligence from Damballa® Labs, Damballa Failsafe accurately detects unknown and zero-day threats and mitigates the risk caused by these breaches by blocking the communication from compromised endpoints to criminal C&C servers.

Damballa Failsafe

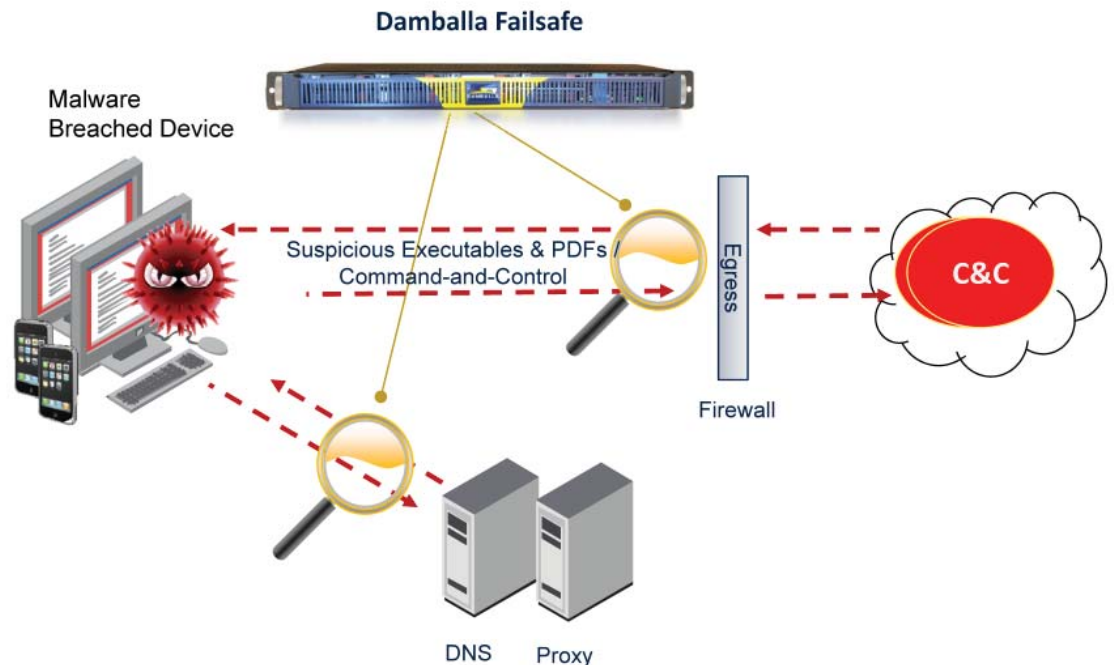
Hunting for Advanced Malware, Persistent Threats and Targeted Attacks

Fast, Accurate Detection. Damballa Failsafe uses a system of out-of-band sensors to monitor communications including firewall traffic, DNS queries, and HTTP requests. It looks for behaviors and unique indicators of suspicious files and C&C communication and correlates this information to identify the presence of malware and pinpoint infected devices.

Multiple deep packet inspection engines in Damballa Failsafe sensors detect threats utilizing:

- **Automated Malware Analysis** – detecting and capturing suspicious executables and PDFs, identifying if they are malicious, and analyzing them at Damballa Labs in real-time to profile their C&C communication behavior and provide host forensic details.
- **Behavioral Analysis** – tracking the behavior of the asset's communications - identifying if certain communications seem automated or act more like a human.
- **Profiling Communications** – analyzing network traffic to determine if the destination is suspicious, known to be C&C, has a low reputation, or is generally shady.

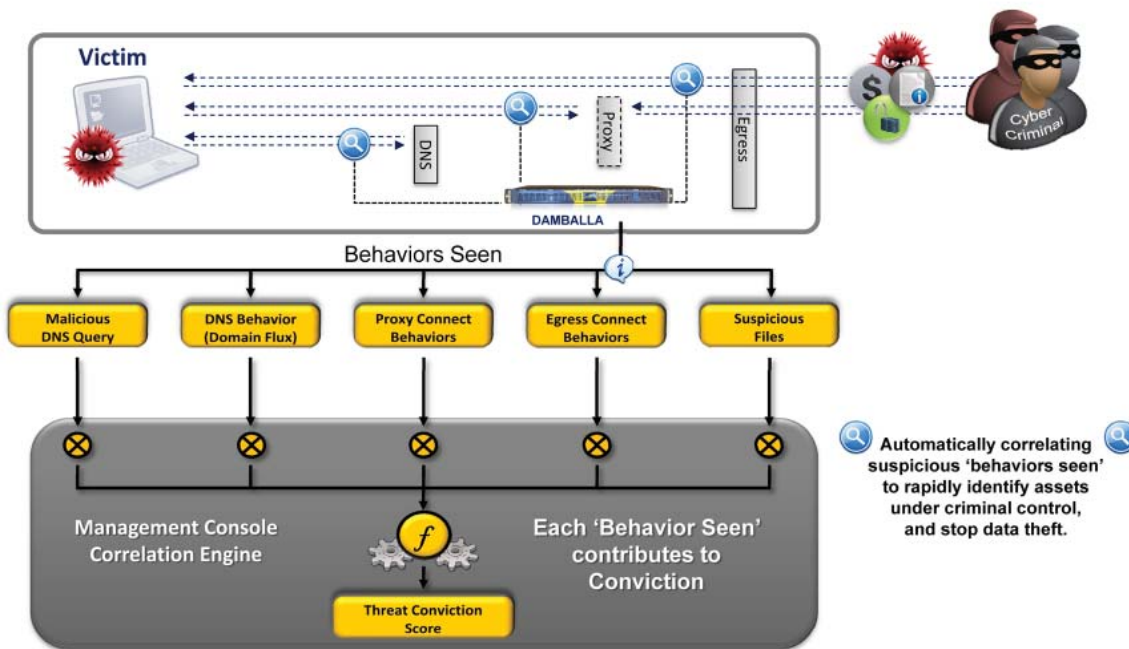
Damballa Failsafe performs full packet captures of suspicious traffic and generates forensic reports identifying changes the malware makes on victim devices, providing a complete picture of who, what, where, and why. This situational awareness provides definitive, actionable intelligence for security teams and eliminates wasted time in chasing false alarms.



Damballa Failsafe provides definitive, actionable intelligence for security teams and eliminates wasted time in chasing false alarms.

Damballa Failsafe is the only solution specifically designed to automatically detect criminal network communication behavior, analyze zero-day and targeted malware, correlate the forensic evidence to pinpoint live infections, identify the nature of the threat and the criminal operator, and terminate the communication to stop data theft.

Damballa Failsafe



Damballa Failsafe has the ability to correlate multiple behavioral indicators to rapidly and accurately pinpoint hidden infections and is unequalled in the market. Damballa now offers real-time malware analysis as additional forensic evidence that contributes to the threat conviction scores for threats identified on infected devices.

Stopping Data Theft

Active Threat Termination. When a threat is identified, Damballa Failsafe can automatically block criminal communications and eliminate the malware's ability to receive commands, send information and steal data. Termination is accomplished using two methods: preemptive termination that prevents malware C&C communication attempts and session termination, which tears down a criminal TCP session.

Factoring Risk, Confirming Infections

Damballa Failsafe rapidly and automatically identifies assets under criminal control and profiles the relative risk of each infected asset. All evidence of criminal network activity is correlated and an Asset Risk Factor is assigned to provide threat response teams a way to prioritize response efforts by identifying which assets pose the biggest relative risk to the enterprise.

Asset Risk Factor is based on a number of observations including the number and severity of the threats identified on the asset, connection success and frequency, the volume of data leaving the asset or entering the network, as well as the location, user or classification of the asset.

Threat Conviction Score is calculated for each identified threat, based on behaviors seen across the DNS, egress and proxy sensors. Identifiable criminal communication traits include DNS queries for suspicious domains, domain query behavior such as fast flux (NXDomains), egress and proxy connection attempts to C&C servers, connection behavior (automated versus user-driven), and suspicious binary downloads. A threat report also details what is known about that threat(s) identified on the device and the criminal operator(s) related to the threat(s).

Armed with this correlated evidence, organizations know with certainty which devices need immediate attention, enabling efficient prioritization of remediation efforts.



Damballa Failsafe

Advanced Cyber Threat Intelligence

Damballa Failsafe leverages the industry's leading early warning capabilities of Damballa FirstAlert to discover the C&C infrastructure used by emerging cyber threats weeks or months before the malware samples are first seen by the rest of the security industry. By using Damballa FirstAlert cyber threat intelligence, Damballa Failsafe can detect advanced malware infections in enterprise networks long before traditional preventative security solutions will have the signatures or blacklists needed to detect the infection.

The screenshot shows the Damballa Failsafe interface. At the top, there is a navigation bar with 'Dashboard', 'Assets', 'Reports', 'Policies', 'Setup', 'Threats', and 'Help'. Below this is a 'Show Table Tools' button. The main content area displays a table of threats. The first row is highlighted, showing a threat named 'WRM-SD-80226' with a risk factor of 8.7. Below this, a 'Behaviors Seen' section is expanded, showing connection attempts to 'irc.debelizombi.com', DNS queries to 'irc.debelizombi.com', and file downloads including 'W32/Virut.gen (MFR)', 'Benign File', and 'Suspicious File'. The table below lists various assets and their associated threats, including 'ATL-WORKSTATION-12', 'NYC-WORKSTATION-23', 'ATL-WORKSTATION-25', 'CHI-WORKSTATION-7', 'NYC-WORKSTATION-10', 'PHI-WORKSTATION-16', and 'PHI-WORKSTATION-11'.

Asset Name	Risk Factor	Threat	TCS	First Threat Seen	Last Threat Update	Category	Tags
NYC-LAPTOP-15	8.7	WRM-SD-80226	100	3 months	3 months	Executive	
		Behaviors Seen					
		Connection Attempts: irc.debelizombi.com (1), irc.debelizombi.com (1), irc.debelizombi.com (1), irc.debelizombi.com (1), irc.debelizombi.com (1), ...					
		DNS Queries: irc.debelizombi.com (5)					
		File Downloads: W32/Virut.gen (MFR), Benign File, Suspicious File					
ATL-WORKSTATION-12	7.1	WRM-SD-80226 Bobax-4	100 50	3 months	3 months	Executive	
NYC-WORKSTATION-23	5.1	WRM-SD-80226	100	3 months	3 months	Sales	
ATL-WORKSTATION-25	4.7	Bobax-4	62	3 months	3 months	Executive	
CHI-WORKSTATION-7	4.6	Sality-01 Bobax-2	100 50	3 months	3 months	Sales	
NYC-WORKSTATION-10	4.5	Bobax-4	100	3 months	3 months	Finance	
PHI-WORKSTATION-16	4.4	RAT-SZ-80104	10	3 months	3 months	Executive	
PHI-WORKSTATION-11	4.4	TwoRandomName (Conficker.C) Bobax-3 RAT-SZ-80104	100 60 50	3 months	3 months	Finance	

About Damballa Inc.

Pioneering the fight against cybercrime, Damballa protects enterprise, ISP and telecommunications networks from the devastating effects of targeted attacks, persistent threats, advanced malware, and other cyber threats. Damballa provides the only network security solution that detects and terminates remote-control communication used by criminals to breach networks. Patent-pending solutions from Damballa are platform and system-agnostic, protecting networks with any device type including PCs, Macs, smartphones, and mobile devices. Headquartered in Atlanta, Damballa customers include Fortune 2000 companies, government and educational organizations, and Internet and telecommunication providers.

Damballa Integration Partners



Damballa Inc.
817 W. Peachtree Street NW
Suite 800
Atlanta, GA 30308

Web: www.damballa.com
Blog: blog.damballa.com
Email: sales@damballa.com
Phone: 404-961-7400