

Damballa's In-The-Cloud Security Model

Enterprise Protection Moves beyond the Network Perimeter

Abstract

In spite of substantial investments in firewalls, antivirus/antispymware, intrusion prevention and other network security infrastructure, enterprise organizations remain plagued by targeted attacks that easily evade even sophisticated and layered defense-in-depth solutions. These targeted attacks are stealthy and smart, quickly adjusting to stay one step ahead of security management. It's like an invisible man let loose in the enterprise. Experienced managers have a feeling that something's wrong, but no one can see or identify the source of the damage. Damballa, Inc.'s In-The-Cloud security model represents a different approach that begins in the Internet itself, and then extends back into enterprise network security architecture. This strategy represents a powerful, innovative advance that is extremely effective at defeating Internet-based targeted attacks, such as BotArmies, that other solutions miss.

Introduction

As the old saying goes, never bring a knife to a gunfight. And yet, that's what many enterprises do when it comes to targeted attacks. These organizations rely on signature-, network, or behavior-based security defenses to keep compromised systems from leaking confidential information. However, these tactics have proven increasingly unable to contain the threat.

According to Gartner, targeted attacks such as BotArmies aim:

"to achieve a specific impact against specific enterprises, and are the growth area in Internet attacks. Targeted attacks have three major goals:

- Denial of service: disrupting business operations
- Theft of service: obtaining use of the business product or service without paying for it
- Information compromise: stealing, destroying or modifying business-critical information"

The professional criminal organizations behind these threats know their enemy. That's why the malware behind targeted attacks easily continues to evade enterprise defenses.

Targeted attacks require a different approach that supplements traditional defense-in-depth (DiD) strategy and closes the Zero-Day window between the release of a targeted attack exploit and the availability of a signature- or behavior-based solution. Damballa's innovation is to begin the threat identification process in the Internet cloud itself, then extend security back into the enterprise. By doing so, security infrastructure gains the ability to see broad-based patterns of attack that can't be seen on a network-by-network basis. This paper describes how Damballa provides powerful, cost-effective in-the-cloud (ITC) network security that dramatically improves an enterprise's ability to protect itself from targeted attacks.

The Threat Landscape – Evolved

That targeted attacks slip past signature- and behavior-based defenses is a frustrating, inescapable fact of life for network security managers. Conservative by nature, these administrators become immediately suspicious when their dashboards indicate no active threats. This too-easy all's-well is at direct odds with their experience, and with the many headlines they read. Consider the following:

- A recent Verizon Business Security survey found that 31% of data security breaches were due to malicious code. Custom malicious code was used in 25% of the data breaches, and 61% of overall attacks were targeted in some way
- A Japanese company suffered an estimated 300 million yen loss (approximately \$2.8 million USD) due to a BotArmy-driven Distributed Denial of Service (DDoS) extortion scheme (Daily Yomiuri Online)
- The estimated cost to rent a 10,000 member BotArmy in Russia has dropped to as little as \$300 per day – and the bots can be reconfigured on-the-fly for whatever purposes the customer requires

The news isn't any better from a technical perspective. Targeted attacks are pervasive:

- 11% of the Internet is compromised (Damballa), with compromised enterprise asset rates estimated between 4% and 10% (Gartner)
- >80% of all spam originates from compromised hosts (MessageLabs)
- >60% of all Windows PCs are found to run malware (Microsoft)
- >80% of all malware contains a keystroke logger (McAfee)
- 75% of enterprises will be compromised with malware that evades traditional perimeter and host defenses (Gartner)

They are persistent:

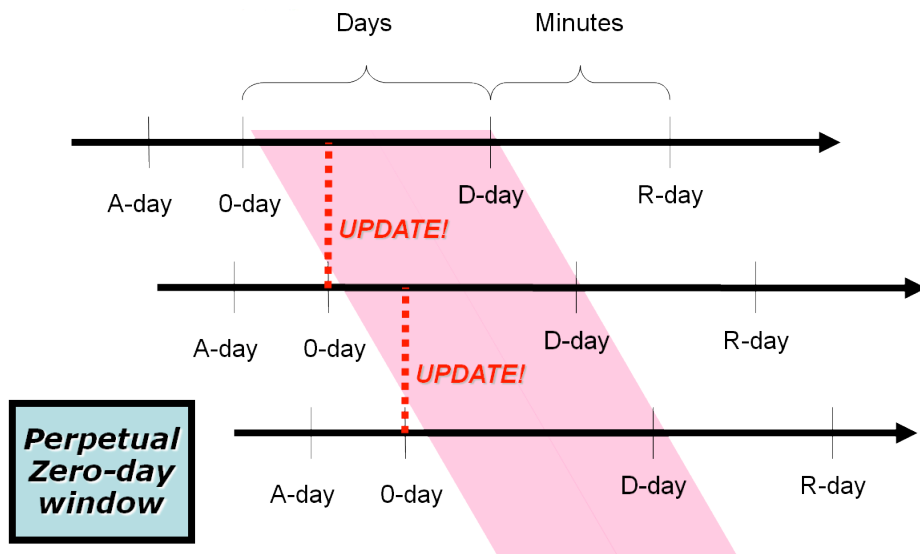
- 40% of malware in Damballa's database escapes detection by major antivirus and intrusion detection/intrusion prevention products
- 80% of newly authored malware defeats AV (AusCERT)
- Over 23% of tested systems using signature-based, updated protection were compromised by malware loaded into memory (Panda)

And they are expensive, with an average cost of remediation alone that runs 50-100 times greater than a virus attack (Gartner).

The reason for targeted attacks' success is easy to understand. Traditional DiD requires frequent signature updates to address new threats. And yet, Damballa tracks BotArmies with over 10,000 distinct pieces of malware. This malware can update itself automatically as often as every 30 minutes – far faster than even the best antivirus or intrusion prevention vendors can issue updates.

Traditional DiD also assumes that communications run predominately through designated ingress and egress points across the network perimeter. But these barriers are increasingly permeable. Mobile workers, trusted relationships with partners, misconfigured or unpatched systems, incompatible policies and procedures due to mergers and acquisitions – all conspire to create a huge window of vulnerability.

Security solutions that only monitor limited access points can't see the broader patterns of organization and intent that targeted attacks represent.



Targeted attack malware changes far faster than signature-based defenses. "0-day" is when malware adapts. "D-day" is when new signatures are available. This time lag means that businesses have a perpetual window of vulnerability to targeted attacks.

Consider an enterprise network with 100,000 devices on the network. Based on Damballa's experience within its current customer base, typical targeted attack penetrations run between 3% and 5% of all devices. Using the following conservative assumptions, the cost of targeted attacks quickly adds up:

Remediation

Assets	100,000	100,000
Compromise Rate	3% (low estimate)	5% (high estimate)
Compromised Assets	3,000	5,000
Cost to remediate per asset (low)	\$500	\$500
Total cost of remediation (low)	\$1,500,000	\$2,500,000
Cost to remediate per asset (high)	\$1,000	\$1,000
Total cost of remediation (high)	\$3,000,000	\$5,000,000

Data Theft (Per Year)

Data exfiltrated per day	100K (low estimate)	500K (high estimate)
Total exfiltration	109.5GB	912.5GB
Average document size	50K	100K
Total documents exfiltrated	2,190,000	9,125,000
Pages per document	2	2.5
Total pages exfiltrated	4,380,000	22,812,500
Value per document	\$50	\$150
Total value exfiltrated	\$109,500,000	\$1,368,750,000

The key point is that **these are largely hidden losses** that often don't show up until well after the fact and are very difficult to trace back to the source. The targeted assets behind the loss operate without the awareness of the users of the compromised systems, or even of IT or security staff. Although remediation takes time and money, it's clearly a better value than allowing losses of this size to continue.

Damballa's In-The-Cloud Alternative

These comparisons are not intended to minimize the very important role that firewalls, AV and IDS/IPS continue to provide in defending the enterprise against attack and misuse. These protection solutions are both necessary and very effective at what they are designed to do. Rather, targeted attacks represent a new and very different strategy for online criminal activity, above and beyond what was possible even one or two years ago. As such, they require an equally new and different type of response.

What is needed – and what most organizations do not realize is possible – is the ability to protect without the need to identify new malware or update behavioral profiles. In other words, to enhance existing security models by focusing on a key element that all targeted attacks must share, but that traditional DiD technologies cannot see or utilize. The best place to begin this process is to give enterprise network security the ability to operate not just on or inside the network perimeter, but across the Internet cloud itself.

That's Damballa's In-The-Cloud security. It operates where the enemy does – across the Internet itself – and then extends protection back within the enterprise. As such, Damballa can take the enemy's strength – an Internet-based, highly distributed, rapidly evolving threat – and subtly turn that strength against the attacker.

Damballa's ITC security is based on the premise that all targeted attacks require one element in order to be successful – Command-and-Control (CnC) communications. That one constant exists independently of everything else – intent, malware, army size, and location or type of compromised systems. Tracking this rallying activity in real-time regardless of port or protocol is the game-changing advantage that comes with an ITC-based approach to protection.

In-The-Cloud Security	Signature or Behavior-Based Security
<ul style="list-style-type: none"> Recognizes and responds as soon as attack activity appears on the Internet 	<ul style="list-style-type: none"> Must wait until new signature updates are available and installed, or until an attack trips behavior profiles
<ul style="list-style-type: none"> Protects against small, highly customized malware and attacks 	<ul style="list-style-type: none"> Works best for large, generic threats for which one signature or profile can be applied to large number of customers
<ul style="list-style-type: none"> Prioritizes threat analysis based on the specific needs of each enterprise client 	<ul style="list-style-type: none"> Provides generic information only
<ul style="list-style-type: none"> Provides detailed insight into targeted attacks inside the enterprise, across the network perimeter and across the Internet 	<ul style="list-style-type: none"> Only sees attacks inside the enterprise or at the network perimeter
<ul style="list-style-type: none"> Rapid conversion of research to real-world protection 	<ul style="list-style-type: none"> Must wait for new product for latest level of protection
<ul style="list-style-type: none"> Lower operating costs through centralized data analysis infrastructure. Damballa provides and maintains research, hardware and software, plus hires and trains data analysis staff 	<ul style="list-style-type: none"> Each level of defense requires its own hardware and software that must be integrated and maintained. Internal expertise on these systems is hard to find and expensive to retain.

Damballa ITC Protection: How It Works

Damballa's ITC security solutions concentrate first and foremost on targeted attack CnC. Protection begins with a **Global Surveillance Network**. This worldwide system of sensors and data feeds applies a variety of known techniques, powerful extensions of known techniques and proprietary new technologies to rapidly and accurately isolate targeted attack CnC from normal Internet traffic.

In addition, **Failsafe** appliances reside inside the network perimeter to deliver more granular insight into communications between internal systems and external malicious or suspicious CnC locations. The combined statistical network data from the Global Surveillance Network and Failsafe appliances is forwarded to Damballa's Analysis Center for both automated and manual analysis.

Damballa links these elements together via a **real-time data link** that connects each Failsafe appliance and the **Damballa Analysis Center**. This secure tunnel delivers distinct advantages for combating targeted attacks:

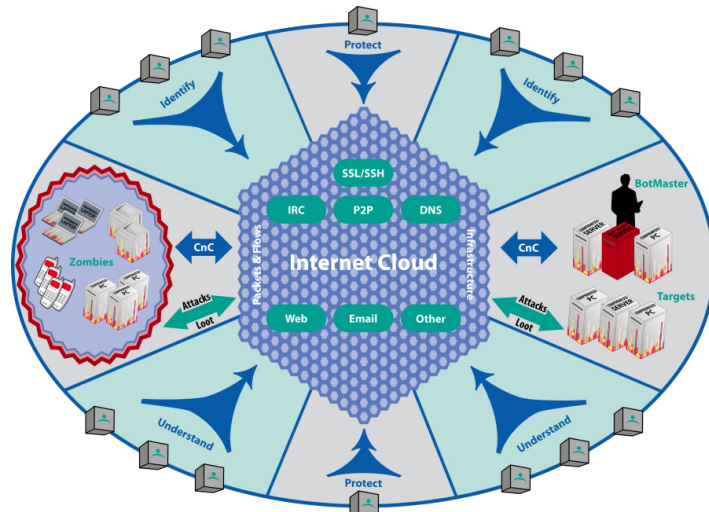
- Immediate insight into communications between internal IP addresses and known malicious domains
- Automated and human analysis of suspicious but unconfirmed activity, or communications with suspicious domains, using the most up-to-minute intelligence available
- Rapid identification and isolation of even very small, very focused targeted attacks, including attacks that rely on only a few compromised assets to exfiltrate specific corporate data

This link dramatically increases visibility into targeted attacks. Damballa uses statistical summaries of network communications flows to concentrate on isolating malicious CnC, rather than inspecting packet contents for detailed – and potentially sensitive – information. No critical internal corporate data leaves the premises.

Once CnC has been illuminated, Damballa then identifies individual compromised systems within the enterprise. Since the make-up, severity and intent of the attack has already been determined, Damballa can also often provide detailed information on the malware in use, its rate of update and proper steps for remediation.

Damballa's technology is not agent-based, which means there is no host-based software to install. The Global Surveillance Network operates independently of the enterprise, and Failsafe appliances work out-of-line to minimize the impact on network performance, which makes Damballa's solutions all but invisible to attackers.

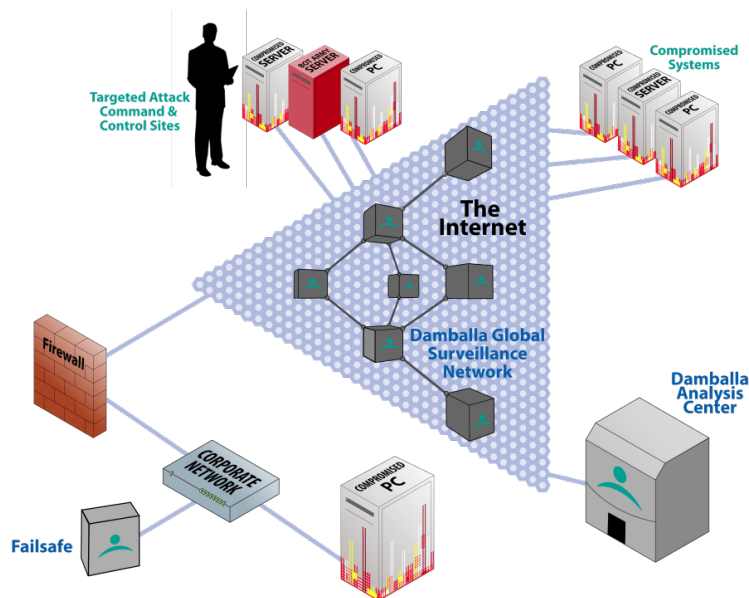
This powerful combination of Internet-based and internal enterprise targeted attack analysis delivers comprehensive insight into the targeted attacks that signature- and behavior-based solutions simply can't see. Damballa's technology operates with very few false positives, and protection works as well for small, highly customized attacks as it does for large, more generic BotArmies such as Kraken or Storm.



Damballa links global Internet visibility with local communications analysis to deliver comprehensive insight into targeted attacks.

Damballa's customers receive detailed information on targeted attack activity via a Web-based portal. This analysis includes:

- Detailed identification of targeted threats, suspicious internal behavior and global attack trends/behaviors
- Real-time information on internal resources connecting to known malicious or suspicious CnC centers across the Internet
- Rapid, accurate identification of malware entering the enterprise from the Internet – especially malware that existing defenses are unlikely to identify
- Actionable information that drives risk assessment/prioritization and remediation activities
- The ability to anticipate, recognize and respond to nascent attacks before their size becomes unmanageable, and to limit the data exfiltrated by already-active targeted attacks



Damballa's In-The-Cloud Security Solution

Real World Results

Of course, the real test of Damballa's ITC model is how it works in the real world. All of the following organizations employed up-to-date security technology, and employed DiD best practices. And yet, each discovered a significant challenge from targeted attacks once they employed Damballa's ITC approach.

Case Study #1

A Fortune 100 manufacturing company suspected that they were the victim of targeted attacks, but the current security system couldn't identify any concrete evidence of compromise. Damballa found:

- >700 compromised hosts
- >10 new BotArmies
- >300 suspicious hosts

This alarming amount of targeted attack penetration came from a single Damballa production deployment location, covering less than one-fifth of the overall enterprise network. None of these compromises were detected by existing security infrastructure.

Malware capabilities included:

- Keystroke logging
- User lock out
- Screen scraping
- Password exfiltration
- Update capability
- Stealthy access point for propagation

Case Study #2

In another example, Damballa's Global Surveillance Network tracked compromised user sessions for an enterprise-class online retailer. Damballa discovered:

- 4,500 compromised user sessions observed per day (average)
- >500 compromised online sessions involving payment per day (average)

The information stolen included:

- Login and payment credentials
- Credit card information
- Other personal information

This insight came without use of Damballa Failsafe appliances and created considerable concern for the retailer, even without the additional value that would come from a fuller deployment.

Case Study #3

A Global 100 manufacturer used Damballa to track targeted attack activity across approximately 30,000 systems as part of a broader network security evaluation. In only 30 days and in only a portion of their network, Damballa uncovered:

- 39 distinct compromised hosts
- >25 distinct BotArmies

These results covered both large, well-publicized BotArmies and a highly targeted malware army focused on specific trade secrets and intellectual property. The data were so astounding that the company immediately began to reassess its overall security strategy and its specific tactics for dealing with targeted attacks.

Conclusion

Damballa's In-The-Cloud approach to combating targeted attacks is a smarter, nimbler, and significantly more effective way to stop targeted attacks. These solutions allow Damballa's customers to see globally across the Internet to identify and understand threats that other solutions miss. Clients gain critical insight into the scale, severity and intent of each threat to act locally in a measured, intelligent manner.

The benefits of Damballa's ITC security solutions are direct and readily apparent:

- Real-time protection against targeted attacks that other solutions miss
- Closure of the perpetual Zero-Day exposure (no time delay waiting for new signature databases)
- A flexible solution that stands alone, or acts as a powerful security accelerator for existing security infrastructure
- A cost-effective platform that requires minimal infrastructure to purchase, manage or support
- Tailored reporting and alerting with a level of expertise that would be very difficult and expensive to develop in-house

Damballa's unique insight comes from focusing solely on this rapidly growing – and evolving – class of threats. By extending network security from the Internet cloud itself back into the enterprise, Damballa empowers its clients to recognize and react rapidly to a wide range of targeted attacks. The end result is a significant reduction in data and business losses that currently remain hidden due to the limitations of traditional network security infrastructure.

About Damballa, Inc.

Damballa protects businesses from targeted attacks used for organized, online crime by using the Internet cloud to identify and isolate threats that evade other technologies. Our unique, global approach monitors the Command-and-Control (CnC) needed to launch these attacks as well as compromised systems, which enables immediate identification and mitigation of malicious activity. Global 1000 corporations, large Internet service providers, OEM partners and government agencies use Damballa's signatureless solutions and industry-leading research to reinforce existing security infrastructure and stop hidden Internet attacks. The result is dramatically improved security both inside and outside the network perimeter. Damballa is privately held and headquartered in Atlanta, Georgia.

Copyright © 2008, Damballa, Inc. All rights reserved worldwide.

This page contains the most current trademarks for Damballa, Inc., which include Damballa, the Damballa logo and Harvester. The absence of a name or logo on this page does not constitute a waiver of any and all intellectual property rights that Damballa, Inc. has established in any of its products, services, names, or logos. All other marks are the property of their respective owners in their corresponding jurisdictions, and are used here in an editorial context, without intent of infringement.