

## A Damballa Case Study:

# ISP Uses Damballa to Stop BotArmies, Improve Quality of Service and Reduce Support Costs

## Damballa Solution At-A-Glance

- A large Asian ISP suspected that significant numbers of BotArmies were operating on its systems and sending traffic across its networks.
- Damballa's BotArmy intelligence services and sensor appliances now identify active BotArmy traffic that originates on compromised systems within the ISP's infrastructure, which enables security teams to locate and remediate threats that they previously missed. The ISP's support costs associated with BotArmy activity have dropped dramatically.
- The ISP has gained the ability to isolate and block BotArmy communications that cross its networks, but originate elsewhere. The ISP's customers enjoy significant protection from BotArmy threats, and the ISP has new incremental revenue opportunities reselling its new ability to clean up bot-compromised networks.

## Challenge

A large Asian Internet Service Provider (ISP) recognized the threat that BotArmies and BotMasters posed to its commercial and residential customers. The ISP worried that BotMasters were using its infrastructure to perpetrate fraud, and that existing defenses were not capable of identifying or stopping those BotArmies. The support costs alone from damage caused by BotArmies consumed a large portion of the ISP's overall network security budget.

The ISP faced an additional problem. An ISP provides the network that customers use to transport data and communications to and from the rest of the Internet. Many of the compromised systems using this ISP's networks were outside its direct control. The bots and BotMasters generating malicious traffic might be anywhere around the world, and the ISP had no means with which to locate or stop the threat.

The ISP clearly needed to stop BotArmy compromises that used its systems for malicious activity. It also wished to develop a competitive advantage by stopping BotArmy traffic that crossed its networks, but started and stopped elsewhere on the Internet.

To bring this vision to reality, the ISP needed a bot-aware security solution that could reduce or eliminate persistent BotArmy compromises on its systems. It also needed to be fast and flexible, so that new BotArmy techniques could be blocked within the shortest time window possible. Finally, the ISP wanted to integrate this solution into its existing network security infrastructure without being forced to hire extra staff or install extra layers of complexity.

## The Damballa Solution

Damballa designed a solution for this ISP that used Damballa's Global Surveillance Network and strategically placed sensor appliances to identify BotArmy traffic

---

whenever and wherever it appeared on the ISP's networks. Damballa's technology operates within the Internet itself, rather than being limited to specific network segments or corporation. This global perspective gives Damballa the ability to rapidly identify key locations that bots and BotMasters must use to communicate with each other.

By identifying and monitoring these key BotArmy contact points in real-time, Damballa quickly separated BotArmy activity from legitimate customer traffic, and used this insight to identify the function of BotArmies, the locations of bots and BotMasters, and the specific malware involved with each compromise on the ISP's systems.

The solution also gave the ISP the ability to recognize BotArmy traffic as it traversed its networks, even if that traffic originated outside the ISP's domains. This information gives the ISP the ability to selectively block these communications, or to stop network traffic to and from known BotMaster IP addresses and BotArmy command-and-control contact points.

### **Results**

The ISP relies on Damballa for global, 24x7 insight into BotArmy activity and command-and-control communications. This information has made the ISP's other security technologies bot-aware for the first time. As a result, support costs directly attributable to BotArmy activity have dropped to a small fraction of what they were prior to the Damballa solution.

Damballa's solution does not rely on malware or attack signatures to detect bots or BotMasters. As a result, it provides protection against new and undiscovered bots that traditional security technologies miss. Nor does it require direct access to network infrastructure such as routers for flow information or other low level network detail, which greatly simplifies installation and maintenance.

Damballa's ability to identify and monitor BotArmy activity anywhere on the Internet also means that the ISP now has the ability to block or dramatically reduce BotArmy communications on its networks without disrupting service to any of its legitimate customers. Its customers benefit from this extra layer of protection, since BotArmies have far less opportunity to reach the ISP's customer's systems, and existing compromised systems have no easy way to connect with BotMasters.

### **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, BotArmy and BotMaster. 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.*