

A Damballa Case Study:

BotArmies and the Multinational Corporation

Damballa Solution At-A-Glance

- A multinational corporation discovered that it had a significant problem with active compromises using its systems to leak confidential information and launch attacks against other companies.
- This organization had well-defined and highly regarded network security infrastructure and staff. And yet, targeted attacks, like Trojans and bots, had penetrated these defenses easily and invisibly.
- Damballa's global intelligence services and hardware sensors now identify targeted attack traffic inside the network perimeter, including the ability to locate individually compromised systems and the attackers who control them.
- The client uses Damballa to rapidly identify and remediate compromises from targeted attacks on its networks. In addition, the ability to disrupt command-and-control communications gives the client the time it needs to plan proactive remediation efforts that do not disrupt normal daily operations.

Challenge

A major international manufacturing company had invested significant sums of money developing a sophisticated, well-trained network security staff and security infrastructure to match. Like other multinational corporations, the company realized that enterprise networks spanning multiple continents are complex, dynamic entities. Users, systems and applications are added, deleted and changed at a dizzying pace. This system also had to support documentation requirements for multiple overlapping governmental and data security regulations, with different regulations being applied in each country in which the company operated.

Security staff and senior management were confident that they were successful in managing the risks on their networks. They regularly passed penetration tests and security audits. Nevertheless, they were troubled by the ease with which bots and BotArmies were reputed to operate on even well-defended networks. They hired Damballa to test their assumptions and the success of their network security operations.

The Damballa Solution

Real-time information from Damballa's Global Surveillance Network immediately identified multiple compromises resulting from targeted attacks operating inside this company's networks – without having to deploy any onsite equipment. The results were startling. In the thirty days that Damballa monitored activity at the client, new compromises were detected at the rate of almost four per week, which reflected hundreds, if not thousands, of compromises that had established themselves invisibly on systems ranging from individual PCs to mission critical servers and databases.

Even worse, each of these compromises accounted for as many as 6,500 inbound and outbound connections to and from the attacker. These sessions represented individual

commands issued instructing these threats to propagate, update, or attack other systems. The compromised systems inside the network perimeter were widely dispersed, which made detection difficult, and left antivirus, antimalware and intrusion detection/intrusion prevention systems ineffective.

The client clearly had a significant problem, one that posed significant risk of losing confidential information, financial loss and significant legal and shareholder liability. In addition, its ability to document and prove regulatory compliance was now open to question. This malicious activity had been taking place in spite of what was, by all accounts, a very thorough and professional security infrastructure and top-tier staff.

Results

Damballa now provides protection against targeted attacks to the client on a 24x7 basis. In addition, Damballa placed special appliances at key locations inside the enterprise and at major access points across the network perimeter. The client uses this real-time information to identify which systems are compromised, even those compromised with zero-day exploits, and quickly determine whether the system needs to be remediated or quarantined and reimaged.

The client now has the ability to monitor communications between these compromises and the attackers, and disrupt those command-and-control links, which effectively neutralizes the bot. All actions are fully documented within Damballa's customer portal, which greatly improved the client's ability to prove compliance with all network security regulations.

This client's new compromise rate has dropped dramatically since the Damballa solution has been in operation. Even better, Damballa's information services and hardware appliances have proven to be very cost-effective, and operate without additional head-count, slowing normal operations or requiring substantial time and attention from staff.

The client has moved from having a large and largely unknown security problem to the confidence that they can proactively manage the risk embodied by targeted attacks. Senior management and security staff are very satisfied with the results.

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.