

How to Be a Hero in the War against BotArmies

Introduction

Security professionals have a very difficult challenge. They need to protect their organizations against targeted attacks such as BotArmies, but to do that they must convince senior management that this protection is needed, cost-effective, and will not require additional headcount. Damballa's unique, powerful insight gives security professionals the knowledge they need to become heroes in the war against BotArmies. These innovative solutions dramatically improve overall security via simple, yet powerful, intelligence that extends security capabilities without straining budgets or staff.

No One Wants to Hear Bad News

After spending substantial sums of money building a network security infrastructure, security staff now discover there's a new and growing threat – BotArmies – that easily slips through these rather expensive defenses. And yet, that's exactly the message that dedicated security professionals must take to senior management.

The motivation behind this threat is easily understood. The BotMasters who create bots and forge them into BotArmies understand how successful firewalls, antivirus, anti-malware and intrusion detection/prevention systems are at their appointed tasks. They understand how these defenses work. Most importantly they understand what these defenses miss. That's why BotMasters construct their bots to evade even the most carefully constructed enterprise network defenses.

Current generations of bots masquerade as legitimate software or low-level threats that don't raise alarms or trip alerts. In other words, they do not give signature-based or packet analysis systems anything to match or identify. Bots also shape their impact on network traffic to evade behavior-based systems. As a result, bots rapidly mold themselves into trusted elements inside the network perimeter.

Then the BotMaster sends the command for the bots to launch the attack and steal confidential data. These trusted systems quietly betray their users and their administrators, usually without anyone being aware of what's happening. New systems are compromised. Confidential data such as trade secrets or credit card numbers quietly migrate to the BotMaster. Valued corporate assets have now become the launching pad to perpetrate crime. It's quiet, profitable (for the BotMasters), and nearly impossible to detect.

Silence is Not Security

The reason why BotMasters are so successful is because security infrastructure traditionally works within the host PC or the LAN to identify active and potential threats. BotArmies operate across corporate boundaries. The entire Internet is their domain, not individual LANs or systems.

Host- and LAN-based defenses cannot track hundreds of thousands of bots acting in concert across hundreds of individual networks. These tools, however valuable and

effective, can't see the broader world. They have no means to identify BotArmy activity or the command-and-control networks BotArmies rely upon to be effective. Even worse, on the rare occasions that malware is detected, they can't connect a compromise with the severity of the threat and the intent of the BotArmy's actions.

This lack of visibility is a BotMaster's best weapon. It only takes a few compromised systems to exfiltrate large amounts of data. Then the trouble begins. The corporation may be legally liable. The negative publicity alone is a nightmare, regardless of whether the business successfully passed security audits in the past. The security team's job security may well be swept aside as part of the internal recriminations. All without anyone really understanding what happened, and how to prevent a recurrence in the future.

There is a Better Way

Fortunately, security staff and network administrators can become heroes with a positive message that resonates with senior management. They can integrate BotArmy intelligence and awareness into their existing security defenses. Because bots are the root cause of many threats faced by the enterprise, existing staff can become more effective. And they can find bots that have already compromised network assets before those bots can do more damage.

Better yet, this solution is simple to deploy, works extremely well, and is very cost-effective. In other words, rather than take bad news to senior managers, smart security staff can be heroes, since a well-prepared company is much less likely to suffer financial, legal or publicity damage from bot-related attacks. All it takes is a solution that makes existing security investments work smarter.

That solution is Damballa.

Damballa Helps Security Professionals Become Heroes

Damballa is a simple, effective and affordable solution for targeted threats like BotArmies. Unlike most security technologies, Damballa doesn't force the replacement of existing infrastructure or require additional head-count. Rather, Damballa helps existing infrastructure and staff work more effectively by accurately and actively identifying BotArmy threats.

Damballa's ability to track the communications between bots and BotMasters anywhere across the Internet provides a global perspective that signature-based and LAN-focused security products simply can't deliver. This knowledge enables administrators to recognize that systems have been compromised, accurately quantify the risk those compromises represent, locate the affected systems, and plan appropriate remediation efforts.

Better yet, Damballa intelligence helps security staff identify the command-and-control communications that BotMasters must use to control their BotArmies. This information gives staff the ability to disrupt these communications, thereby minimizing the bots' ability to morph into new, more virulent forms or launch attacks. No other security solution delivers this same level of actionable information or gives administrators the ability to respond so flexibly and effectively.

Finally, Damballa's KnowledgeBase represents the most complete and accurate reference on the capabilities and techniques of targeted attacks available on the market today. The KnowledgeBase details each bot, how it propagates, how to identify it, known IP addresses used to communicate with BotMasters, severity of threat, compromise vectors and control capabilities. This highly detailed resource gives administrators the edge they need to assess BotArmy risk and develop a more structured and thorough response.

Damballa Enterprise Solutions

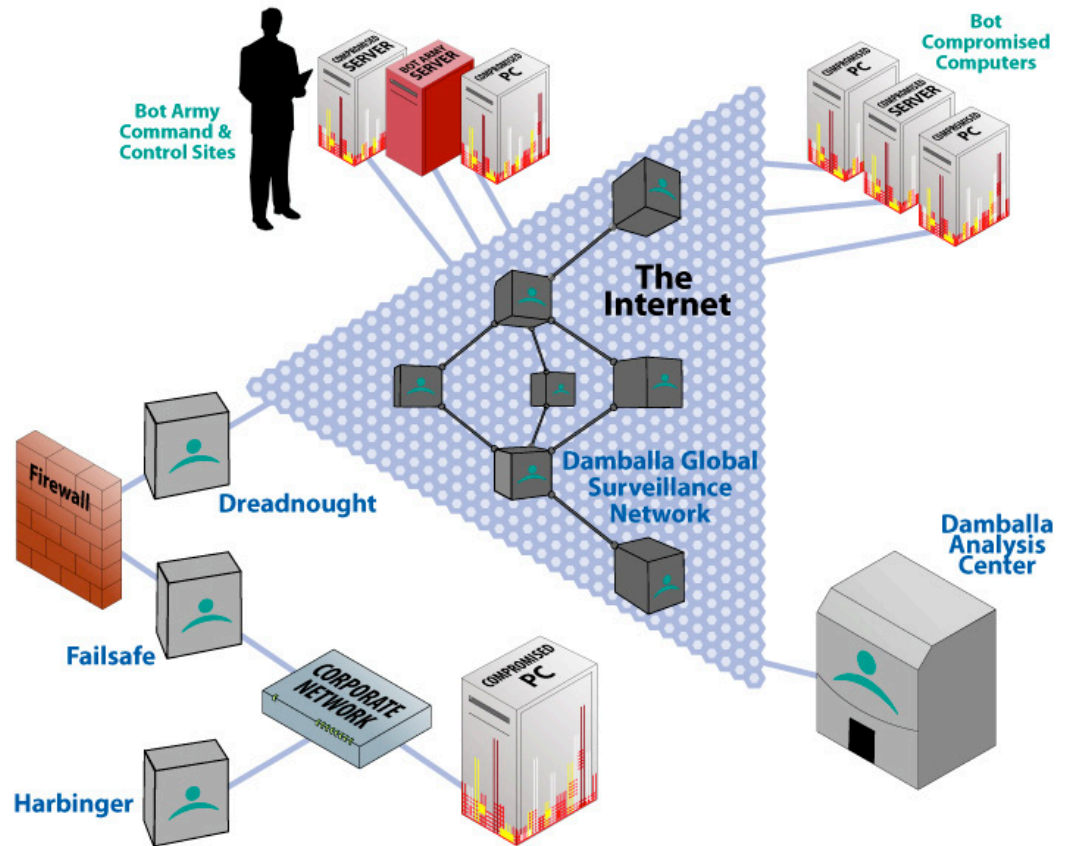
Damballa has three deployment options that work cooperatively to protect enterprise organizations. Clients receive focused, real-time information and analysis of bot compromises on their networks and broader BotArmy activity by subscribing to Damballa's Internet-based **Global Surveillance Network**. This service delivers immediate alerts when new bot compromises occur on client networks. It requires no equipment on client premises and can be fully operational within hours.

Organizations concerned about compromised machines operating inside their network, unimpeded by AV or IDS/IPS, subscribe to Damballa's **Failsafe** solution. This service utilizes Damballa appliances placed at key Internet access points and network intersections to identify internal activity from targeted attacks such as bots. Damballa notifies clients in real-time when a new compromise is detected.

Damballa's **Harbinger** appliance provides real-time, on-site insight into suspicious systems, potential BotArmy compromises and the resulting security events that these areas of concern create. Harbinger provides more than just binary answers, such as "Compromised" or "Not Compromised." Queries to Harbinger return a rich characterization of the host's compromise level and recent activity, which is useful for both operations center personnel and end-user customers.

This information allows analysts and systems to react faster and more accurately to a wider range of security risks, thus saving clients money and safeguarding corporate reputations.

When companies are concerned about compromised machines connecting to mission critical applications (e.g. VPNs, online transaction systems, ERP systems, etc.), they purchase Damballa's **Dreadnought** solution. With this service, Damballa provides real-time information on malicious systems attempting privileged connections to critical internal systems. Damballa's unique ability to identify targeted attacks operating across the Internet dramatically increases any organization's ability to enhance the security of their most critical assets.



Damballa provides insight into targeted attacks from across the Internet (Global Surveillance Network), from immediately outside the network perimeter (Dreadnought), from inside the network perimeter (Failsafe) and advanced data analysis and correlation (Harbinger and the Damballa Analysis Center).

Conclusion

BotArmies are a very real threat to enterprise security. Since traditional security infrastructure is blind to BotArmy activity, security professionals need a fast, accurate and cost-efficient means to complement existing solutions so that they can respond to this new threat. Damballa's ability to track BotArmies across corporate boundaries, anywhere on the Internet, delivers the intelligence that administrators need to meet the BotArmy threat. Further, Damballa gives security professionals the insight and confidence they need to deliver a positive message to senior management, rather than raising an alarm on a problem with no solution. BotArmies can be beaten. It doesn't have to be expensive. Damballa turns security staff into heroes who know how to solve the BotArmy problem.

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.