

## Trust Betrayed

### *What to Do When a Targeted Attack Turns Your Networks against You*

#### **Executive Summary**

Targeted attacks such as BotArmies are big business. Each one of these compromised machines represents a system that is trusted, but is outside of its IT Department's control. In short, the trusted relationships between computers and businesses that corporations depend upon has been turned into a hidden and very profitable tool of betrayal. Damballa delivers the global intelligence on targeted threats that businesses require to manage this new threat. This information helps existing network security infrastructure work more effectively, as well as improves overall regulatory compliance.

#### **Introduction – The Numbers Don't Lie**

Targeted attacks – once the the future of Internet crime – are here. According to Gartner, targeted attacks aim to, "to achieve a specific impact against specific enterprises" and do so via malware that easily evades signature-based defenses or by hijacking critical network systems. BotArmies represent one of the fastest growing, most profitable examples of this organized, criminal online activity.

*BotMasters who sell the use of their hidden spam networks for thousands of dollars per day. A Zero-Day attack for Windows Vista offered for \$50,000 – even before Vista was formally released. Sophisticated business models in which "affiliates" are paid based on the number of systems they compromise with bots.*

Clearly, placing malicious programs on trusted computers and organizing them into hidden, decentralized distributed computing networks has become a big business. With so much money at stake, stealth is critical to a the attacker's success. That is why targeted attacks and their resulting compromises can now operate without being discovered by antivirus, antispyware, intrusion detection/intrusion prevention and network behavior systems.

*Try-before-you-buy malware. Lease a BotArmy as a managed service. Confidential information, ranging from proprietary trade secrets to personal information to credit card numbers selling at a discount, since so much is available.*

A typical BotArmy may involve hundreds of thousands – even millions – of bots, spread across hundreds of networks and businesses. However, it's often the smaller BotArmies, the ones focused on a specific corporate target or type of online fraud, that are hardest to find or stop.

*Pump-and dump stock manipulation plots that use spam to profit from inflated share prices of innocent companies – then crush those companies when the stock price later plummets. BotMasters who use blackmail to remove the BotArmies they've already placed on corporate networks.*

---

New compromises appear every day. And affected systems continue to produce normal, even critical work, which complicates remediation on those occasions when bots can actually be found. Corporations trust these systems because they have no reason not to – even while these compromised assets use corporate resources to quietly steal confidential information and attack other networks.

Targeted attacks therefore bring up three very difficult challenges that frustrate traditional network security defenses. First, how does a company find and eliminate attacks and compromises that know how to hide, and how to block the command-and-control communications? Next, how does an organization determine the severity and intent of compromise, which is just as important as detecting the presence of malware? Finally, how can staff create a safe window of opportunity to remediate these systems without disrupting normal operations?

Damballa delivers the global intelligence on targeted threats and insight into the activity that businesses need to identify compromises on their networks, understand how those compromises affect overall risk and effectively combat the threat. This information helps existing network security infrastructure work more effectively, as well as improves overall regulatory compliance. This white paper details the benefits of Damballa, and shows how Damballa's services integrate into and improve overall network management policies and procedures. This powerful combination helps businesses restore the trust that these targeted threats betray.

### **Smart, Disciplined and In Control**

Targeted attacks are successful because they convince hosts, networks and IT staff that there's nothing to be worried about. This process happens because attackers know that security staff places too much trust in signature-based, LAN-focused security devices.

For example, most bots appear as low-level threats. Their code doesn't match known viruses, worms or Trojan horses. Their activity is mostly trivial – monitoring tracking cookies, serving ads to Web browsers, etc. Bots can look like legitimate applications, or insert themselves into programs or the operating system itself.

These bots are also *polymorphic*, which means they can change their code upon command. At a preset time, they reach out across the Internet to a specific Web address. If there's an answer, they receive new code and incorporate it into their structure. Some malware updates as often as every half hour. That capability makes them much more agile than signature-based defenses, which inevitably have a delay of hours or days between the emergence of new bot code and the publication of a signature database that can detect that code.

Targeted threats also know how to operate without generating large amounts of network traffic. They talk to their update locations or receive attack instructions at infrequent intervals using normal Web ports. As a result, network behavior-based defenses see this activity as part of the normal background noise that any enterprise network generates on a daily basis. There's nothing unusual to generate an alarm.

Finally, attackers have so many compromised machines within any given BotArmy that a few can be sacrificed without damaging overall effectiveness. This ability to distribute the risk across the breadth of the Internet makes it much easier for these criminals to remain anonymous and undiscovered. It also increases the likelihood that an organization will find some compromises and feel that the problem is under control, when many others have escaped detection.

### **A Truly Global Perspective**

Every BotArmy has a weakness, no matter how well it was designed or how successfully it hides from network security. At some point, each bot must go outside the network perimeter to change its code and/or receive attack instructions from the BotMaster. There are a limited number of places that BotMasters can use to place those commands or that bots can use to call for direction, even if those places change constantly, just like the bots themselves.

In other words, BotArmies leave tell-tale traces of their activity on the Internet itself, even if they remain well-hidden on corporate networks. Enterprise defenses, by definition, can only see what happens inside the network perimeter. Damballa operates across the full breadth of the Internet, just like the BotArmies do. As a result, Damballa can rapidly identify when and where BotArmies are active, and even trace that traffic back to individual compromised systems or the BotMaster himself.

This powerful network of sensors, operating at key locations across the Internet and around the world, works in conjunction with highly tuned collection, correlation and analysis engines to generate a real-time, world-wide understanding of where individual bots are located, how those bots are organized, which BotMasters control which BotArmies, and the critical command-and-control links that make a BotArmy possible.

### **Damballa Benefits**

It is this global perspective that makes Damballa a unique and uniquely powerful security solution. No other security provider sees bots as part of – quite literally – a bigger picture. As a result, Damballa delivers the fastest, most accurate and most complete information available for identifying and isolating targeted threats. Consider the following Damballa benefits:

***Rapid Identification of Compromised Systems*** – Damballa identifies local IP and MAC addresses that attempt to connect to known command-and-control servers anywhere on the Internet. Damballa also connects compromised host activity with Active Directory domains and individual computer names. Damballa quickly recognizes external targeted attacks that attempt to communicate with internal resources. Administrators learn what's compromised in real-time, even if other defenses do not detect the threat. There's no guesswork, and staff knows immediately if the exploit can be removed, or if the system needs to be reimaged.

***Focused, Actionable Data*** – Damballa's information is updated in real-time, on a 24x7x365 basis. There is no delay between the emergence of a new targeted threats and Damballa's recognition of that threat's activity on the Internet. These reports

deliver the information security administrators need, when they need it, in an easy-to-use format with detailed drill-down for additional information.

***Command-and-Control Disruption*** – Damballa’s ability to monitor activity from individually compromised machines, anywhere across the Internet, helps administrators isolate and quarantine individually compromised hosts. By disrupting command-and-control, they are effectively neutered. Coordinated attacks from inside the network perimeter become impossible, and there is no risk of exfiltrating confidential data.

***Finds Threats that Other Solutions Miss*** – Damballa does not rely on signatures to identify bots, nor does it rely solely on network behavior profiles, router flow or other internal resources as the core of its targeted attack intelligence. This very different approach means that the techniques attackers use to evade antivirus, intrusion detection/intrusion prevention, network behavior and other security technologies can’t hide from Damballa.

***Integrates Easily with Existing Security Infrastructure*** – Damballa’s solutions integrate easily with existing security infrastructure. When combined with Damballa’s KnowledgeBase – the most comprehensive targeted attack resource on the market – this information gives administrators the insight they need to find threats that otherwise would be go undetected. Equally importantly, Damballa helps ensure that existing investments in network security work smarter and more effectively.

## **Conclusion**

Targeted attacks such as BotArmies represent something new – the maturation of the Internet as a highly profitable tool for hidden, highly organized criminal activity. In fact, the best evidence for how widespread online profiteering based on BotArmies has become is the increasingly effective efforts that online criminals undertake to keep their malicious activity a secret. The result of these efforts is that businesses literally can’t trust their own computers. Compromised machines may act normally, but they perpetrate online fraud every day with a very low likelihood of anyone except the BotMaster knowing what they are doing.

The online criminals who control these BotArmies are smart, savvy and thoroughly amoral. They are very skilled at what they do, well-funded and understand exactly how traditional network security defenses work. That’s why targeted attacks are compromising so many machines inside corporate networks and around the Internet. It takes a different approach to anticipate this new type of threat. Damballa’s represents just such an advance.

Damballa delivers information on targeted attacks that no other security solution can provide. These powerful resources help disrupt command-and-control communications, locate compromised machines and prioritize remediation efforts. Better yet, Damballa is fast, accurate and very cost-effective. It even helps existing infrastructure become truly bot-aware, without adding complexity or requiring additional staff.

Compromises from targeted attacks seek to betray the trust that enterprise networks rely upon to deliver highly efficient, highly interconnected communications. Damballa's global insight and practical, real-world solutions restores that trust by uncovering these hidden threats and stopping online criminal activity.

**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.*