



## VISIBILITY INTO BOT-COMPROMISED HOST COMMUNICATIONS BOTH WITHIN AND LEAVING ENTERPRISE NETWORKS

If your enterprise is connected to the Internet, then you are the target of a bot-driven targeted attack. It's not a question of if or when you'll be compromised – it's a question of how bad the problem already is, and how soon before your staff can identify or minimize the damage.

The key difference between these attacks and other network security threats is that botnet attacks use malware armies, deeply organized and coordinated across the Internet, to perform criminal activities via direct, secret control over compromised enterprise assets. These Command-and-Control (CnC) communications link compromised hosts to criminally motivated external parties. Industry analysts widely acknowledge that these targeted attacks are growing rapidly, and usually involve the following:

- ▶ Denial of Service (DoS) attacks that intentionally and persistently disrupt business operations
- ▶ Theft of service attacks that steal business products or services without paying for them
- ▶ Information attacks where confidential corporate information is stolen, modified or destroyed

Online, professional criminal organizations invest heavily in botnets for one simple reason – malware armies are extremely profitable platforms for making money.

### The Challenge

3% – 5% of enterprise assets are already compromised with botnet malware regardless of up to date anti-virus signatures and other defenses. Each one of these compromised assets operates outside the control of IT and security staff, without anyone being aware of the problem. In fact, it is the exceptional stealth of these attacks and their widely dispersed nature that makes them so uniquely dangerous. Every one of these systems can leak sensitive internal information or attack other organizations at any time.

The key point is that these are largely hidden losses that often don't show up until well after the fact. The compromised assets behind the losses appear to operate normally. The relatively low level of unauthorized activity compared to overall business operations, as well as the dispersed nature of these attacks, makes it very difficult to discover them. However, the amount of data being exfiltrated every day makes the damage very real and very expensive.

Moreover, how are these bot-compromised hosts impacting other hosts within your network and which ones are worthy of further investigation and require remediation?

### Joint Solution Benefits

#### *Reduce costs, maximize staff productivity*

- ▶ A single console view of all host activity
- ▶ Accelerated incident response and remediation efforts
- ▶ Absence of regular signature updates

#### *Demonstrate Compliance*

- ▶ Deeper visibility, more effective remediation efforts and greater host accountability
- ▶ Precise attack disruption of egress CnC traffic potentially indicative of data leakage
- ▶ Alarming on unauthorized host/server access and identification of additional hosts compromised
- ▶ Detection of newly emergent previously undiscovered targeted attacks

#### *Extend the value of existing resources*

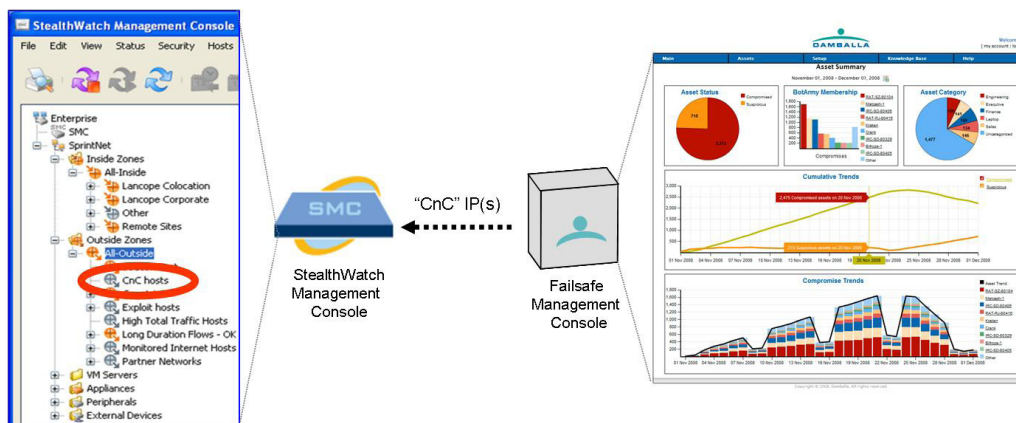
- ▶ Deeper and broader visibility into compromised enterprise assets across fully-meshed MPLS networks.

## Joint Solution

The integration between Damballa's Failsafe and Lancope's StealthWatch solution provides immediate and unprecedented visibility into compromised enterprise assets and actual bot-driven targeted attack activity taking place on the network with broader detection capabilities of malware for which no signatures exist. This integration provides visibility into all hosts that have communicated or are communicating with CnC and helps decipher whether or not these compromised and suspicious hosts are worthy of further investigation. This integration provides:

- ▶ Extremely high fidelity identification of zero-day botnet compromises and the CnC information needed to launch botnet attacks
- ▶ The ability to research and pinpoint in real-time extremely relevant internal communication patterns
- ▶ Mitigation to stop CnC traffic with no impact on the "good" traffic

## How the Failsafe and StealthWatch Solution Works



Setting up this integration can be accomplished quite easily:

- ▶ Create a "CnC" zone within StealthWatch for CnC host IP addresses
- ▶ Create a StealthWatch "soft firewall" or zone locking rule to alarm on all internal host traffic communications to the CnC hosts
- ▶ Enable StealthWatch Integration on the Failsafe Management Console and provide the appropriate configuration parameters necessary to communicate the "CnC" zone ID to the SMC
- ▶ From this point forward, Failsafe will automatically update the StealthWatch "CnC" zone whenever it positively identifies CnC traffic from a compromised host. StealthWatch will then trigger an alarm notifying the operator that further investigation of hosts that have been conversant with the bot-compromised host is warranted to verify that their host integrity remains intact.

## About Lancope, Inc.

Lancope®, Inc. is the leader in NetFlow Analysis and the provider of the StealthWatch® for flow-based anomaly detection and network performance monitoring. Delivering unified visibility across physical and virtual networks, StealthWatch eliminates network blind spots and reduces total network and security management costs.

## About Damballa, Inc.

Damballa protects businesses from bot-driven 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 that coordinates botnet attacks to rapidly identify compromised systems and enable immediate control 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.

## Lancope Headquarters

3650 Brookside Parkway  
Suite 400  
Alpharetta, GA 30022

+1.770.225.6500 (US)  
(Toll Free) 888.419.1462  
+1.770.698.8827 (International)

Website: [www.lancope.com](http://www.lancope.com)  
E-mail: [sales@lancope.com](mailto:sales@lancope.com)

©2009 Lancope, Inc. All rights reserved. Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. All other trademarks are properties of their respective owners. StealthWatch is covered by U.S. Patent Nos. 7,290,283; 7,185,368; 7,475,426 and other U.S. and foreign patents pending.

ID12042009