Cisco ASA Botnet Traffic Filter

At-A-Glance

What Is the Cisco ASA Botnet Traffic Filter?

The Cisco® ASA Botnet Traffic Filter complements existing endpoint security solutions by monitoring network ports for rogue activity and detecting infected internal endpoints sending command and control traffic back to a host on the Internet. The Botnet Traffic Filter database accurately and reliably identifies command and control traffic, as well as the domains or hosts receiving the information.

Why Is the ASA Botnet Traffic Filter Important for My Organization?

With the increase in malware, spyware, and the use of Web 2.0 applications such as Facebook and MySpace, the possibility of an endpoint being infected has increased exponentially. Cisco's defense-in-depth approach for endpoint security advocates multiple layers of protection, including long-term infection prevention systems, visibility and mitigation, and endpoint remediation.

Process	Security Product
Infection prevention	• Cisco IPS 4200 Series Sensors • Cisco IronPort® S-Series Web Security Appliance • Cisco ASA 5500 Series Content Security and Control Module (CSC-SSM)
Detection	Cisco ASA Botnet Traffic Filter
Endpoint remediation	Cisco Network Admission Control (NAC)

Cisco IPS and Cisco IronPort web security appliances are long-term infection prevention systems, and the Botnet Traffic Filter complements these solutions. It functions as a detection feature to identify infected endpoints that have bypassed the existing prevention mechanisms. Endpoint remediation technologies such as NAC can be used to quarantine infected endpoints.

Understanding Botnets and Botnet Infection

What Are Botnets?

Botnets are a collection of malicious software or "bots" covertly installed on endpoints and controlled by another entity through a communications channel such as IRC, peer-to-peer (P2P), or HTTP.

What Is the Botnet Infection Process?

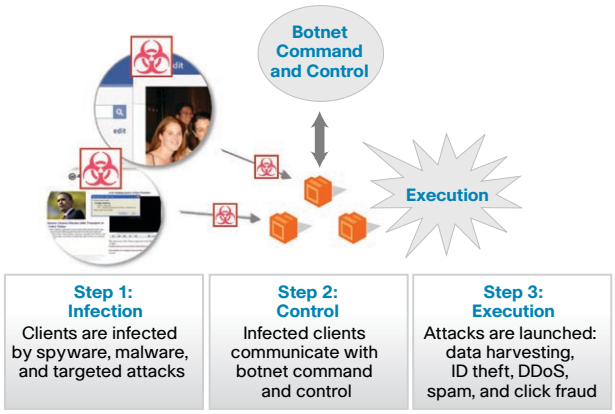
There are three components to botnet infection:

- **Step 1: Infection.** Endpoints can become infected through different means; web or email malware is the most common mechanism
- **Step 2: Control.** The infected endpoint sends "phone home" traffic back to the command and control on the Internet.
- **Step 3: Execution**. Botnet attacks are launched.

How Do Botnets Impact Organizations?

Botnet attacks can take on a variety of different forms. They have evolved from spam and denial-of-service attacks to website attacks, data harvesting, and click-fraud. The impact to organizations is typically financial, as attackers achieve significant financial gain from targeting spam attacks or bringing down websites for profit.

Figure 1. Botnet Infection Process



Cisco ASA Botnet Traffic Filter

The Cisco ASA Botnet Traffic Filter monitors phone home traffic across all ports and protocols by using an internal database that is continuously updated with results for malicious IP addresses and domain names. Visibility into the infected endpoints sending data to the command and control host allows businesses to terminate this connection via normal mechanisms such as ACLs or "shun."

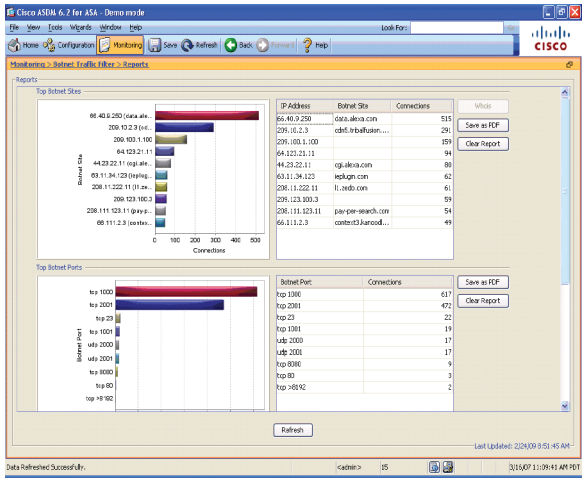
The Botnet Traffic Filter database receives periodic updates from the Cisco Security Intelligence Operations Center, which delivers the fastest and most accurate protection against threats. The Cisco SIO features:

- Largest footprint of security devices in the world (email, web, firewall, and IPS devices)
- Largest and most dynamic collection of intelligence data from Cisco devices and third-party data feeds
- Largest investment of resources dedicated to understanding the dynamic threat environment (more than 250 certifications, 100 publications, 20 books authored, and 100 security patents) and delivering continuous coverage

The Cisco ASA Botnet Traffic Filter is available with Cisco ASA Software Release 8.2 via a license.

Top Reports

The Cisco ASA Botnet Traffic Filter offers several reports to provide businesses with visibility into phone home traffic, ports, and infected endpoints.



For more information, visit: http://www.cisco.com/go/asa

C45-530437-00 04/09