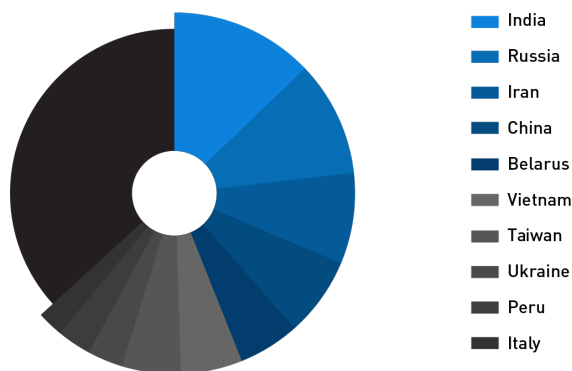


Threat InDepth IP Reputation

The continuing growth of botnets brings a new challenge for applications and systems — to ensure that the host you are transacting with really is ‘trustworthy’ and not compromised by malware.

Cyren’s Threat InDepth: IP Reputation feed provides information on hosts discovered in the last 24 hours that are infected by malware and used as ‘zombies’ by botnets. Data describing bad IP addresses and types of malicious activities detected is provided by the Cyren GlobalView™. This document describes the IP Reputation Intelligence feed and its data format.

ZOMBIE COUNTRIES



Overview

The service delivers data from the GlobalView threat intelligence network regarding identified, recently active zombie host computers. IP addresses can be compared to the known “bad IP” records in the data, and if there is a match, accompanying data describes the types and frequency of malicious activity known to have originated from that host. Cyren’s partners use the IP Reputation Intelligence feed to:

- Prevent fraudulent activities
- Decrease bot user registration
- Hinder Dynamic Denial of Service (DDoS) attacks
- Supplement Advanced Persistent Threats (APT) detection

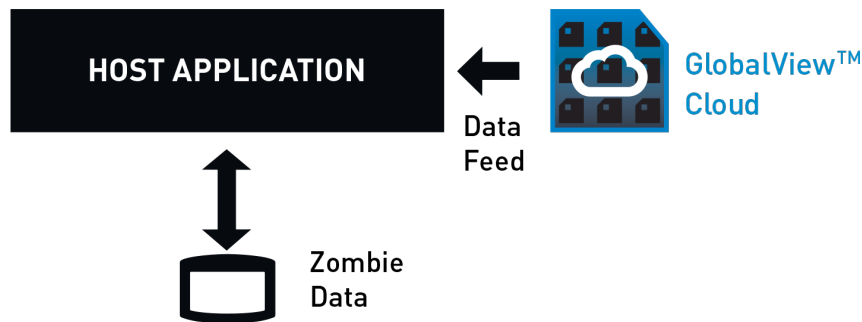
Why Use Cyren’s Threat InDepth: IP Reputation?

- **Unique Intelligence**—the IP Reputation Intelligence feed is powered by GlobalView, Cyren’s global threat intelligence platform. GlobalView examines 25+ billion transactions per day to build unique insight into current and emerging security threats.
- **The latest data**—the service lists only those infected hosts that have been active within the last 24 hours.
- **Easy to implement**—the service is designed to be up and running quickly, and is easily integrated with partner applications via SDK, or as a text data feed.
- **Partnership**—our business is built on empowering our partners with detection capabilities that lead the market, consume minimal resources, and are easy to integrate. All backed by a dedicated technical and commercial partner support model.

www.cyren.com/contact
sales@cyren.com

How It Works

Every 24 hours a full dataset of all active zombies is delivered, including types of activity. Incremental updates are provided every 10 minutes.



IP Reputation Intelligence Feed Data Format

Header	Parameter	Description
Action	+ / - / =	Add / Delete / Modify a recording
IP	IP address (Ipv4 format)	IP address of zombie with leading zeroes as needed
First-Seen	YYYY-MM-DD-HH:mm:ss	First detection time (UTC)
Last-Seen	YYYY-MM-DD-HH:mm:ss	Most recent detection time (UTC)
Intensity	unsigned number (0...10)	Active zombie intensity level. A lower number indicates relatively less malicious spam activity; a high number indicates a zombie host with a high level of spam activity
Class	text	Bad IP category: C1 = Dynamic C2 = Static
Risk	unsigned number (0...10)	Ratio between malicious and valid activity
Country	Country code (2 letters)	Country of zombie origin

About Cyren

Cyren is the global leader in information security solutions for protecting web, email, and mobile transactions. Our award-winning, patented technologies and global security platform increase the value and profitability of our partners' solutions, protecting over 1.3 billion end users in 180 countries.

Support

For additional information, or to assist you during your evaluation or integration, please contact your Cyren Technical Account Manager.