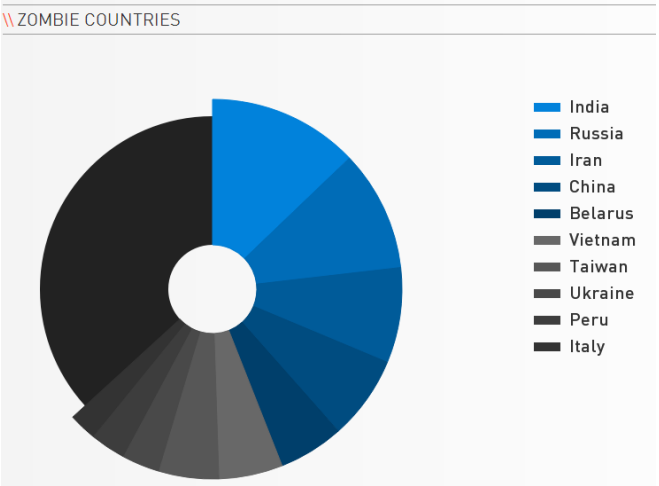
# ZOMBIE INTELLIGENCE

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

CYREN Zombie Intelligence Service 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 type of malicious activities detected is provided by the CYREN GlobalView™ Cloud platform. This document describes the Zombie Intelligence service and its data format.




## OVERVIEW

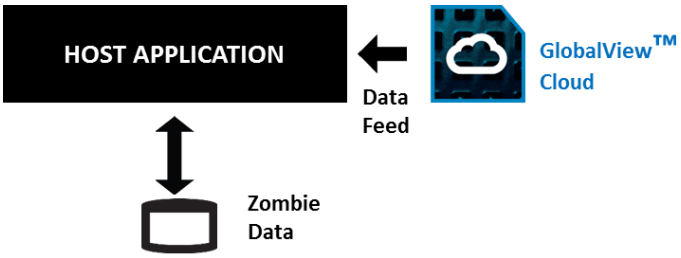
The service delivers data from the CYREN GlobalView™ Cloud threat intelligence database, regarding identified, recently active zombie host computers. IP addresses can be compared to the known 'bad IP' records in the data and if there is a match, accompanying data describes the types and frequency of malicious activity known to have originated from that host. CYREN partners use Zombie Intelligence Service data to:

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

### BENEFITS

- **Unique Intelligence -** the Zombie Intelligence Service is powered by GlobalView™ Cloud, the CYREN global threat intelligence platform. GlobalView™ Cloud examines 12+ 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

## HOW IT WORKS




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

## ZOMBIE INTELLIGENCE DATA FORMAT

| HEADER | PARAMETER | DESCRIPTION |
|---|---|---|
| Action | +/-/= | Add/Delete/Modify a record |
| 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) | Computed intensity as active zombie. Low means spam activity is low, high indicates a high spam activity zombie host |
| Flags | bitwise | Indicates the zombie is conducting malicious activities |
| Class | text | Bad IP category:<br>C1 = Dynamic<br>C2 = Static |
| Risk | unsigned number (0.. 100) | 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 550 million end users in 190 countries.

### SUPPORT

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