

Dark Side Intelligence™

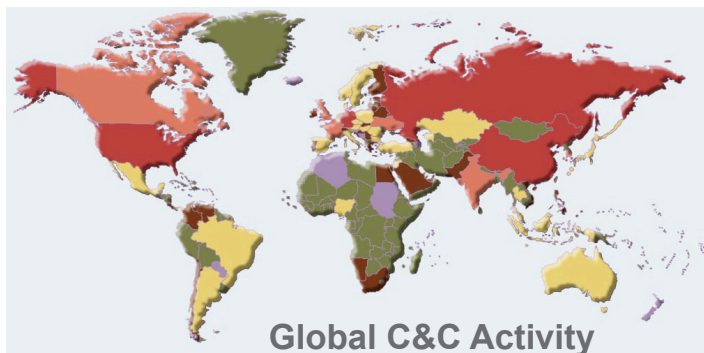
“Stopping Malware At Its Source”

Botnets are the #1 Internet threat and have propelled the global community to new levels of security awareness. These malicious networks, controlled by cybercriminals, are responsible for malware distribution, spam, phishing, information theft, and DDoS attacks. Traditional anti-malware solutions and their conventional detection methods have failed to keep pace with this new malicious technology. The proliferation of zombie computers and their associated command and control (C&C) servers has compromised the integrity of the Internet.

Umbra Data provides Dark Side Intelligence™ about Botnet activity that renders C&C's harmless and disrupts the Botnet lifecycle. Umbra Data offers its cloud-based solution in a variety of ways with an emphasis on integrating rapidly and easily into your operational environment. C&C activity is constantly monitored and vetted. Decisive action can be taken by you — anytime, anywhere.

The most comprehensive source of active Botnet data in existence

Now you can respond to the ever-changing C&C threat landscape with actionable data and clear insight into the addresses, protocols, and malicious actions associated with active Botnets.



Umbra Data is the leading provider of Botnet Command & Control threat intelligence

Dark Side Intelligence™

- Variety of data formats provide for seamless integration — each subscription is tailored to meet your unique operation requirements
- Umbra Data Validation Engine (UDVE) employs a 27-step vetting process to create an accurate threat assessment and reputation database
 - » **Block List** identifies purely malicious sites backed up with an SLA that assures no collateral damage
 - » **Alert List** warns of malicious activity occurring on a site where known good activity has also been identified
 - » **Monitor List** predicts where C&C's will emerge next by using advanced data mining and correlation techniques to identify new threats as soon as they appear
- Built-in reports for condition analysis and performance metrics

Customer Benefits

- Effective threat protection for your users and customers
- Reduced expenses associated with support and abuse teams
- Fewer security resources devoted to aggregation and vetting from multiple threat sources
- Reduced operating and capital costs
- Improved peer reputation