iPrism Outbound Anti-Botnet Protection

Originally identified in 2006-2007, Botnets are a class of criminal malware designed and built to infect computers and networks, steal valuable data, and control victims' computers in order to commit other cybercrimes. According to experts, today's botnets are sophisticated, money-making machines that not only hijack data and compromise business networks, they are the backbone of a entire criminal ecosystem with the capability of putting all businesses and institutions at risk.

iPrism Botnet Threat Index

iPrism Web Security leverages a comprehensive botnet threat index to prevent bots from being activated, which occurs when they contact command and control centers outside your network. Once a bot has been detected and blocked, users are alerted via email and Real-Time Monitor so they can later remediate compromised endpoints without worrying about the immediate threat of financial loss resulting from data leakage or other damaging malicious and illegal activities. iPrism on-box reporting can show compliance with regulations that protect users' identities and data.

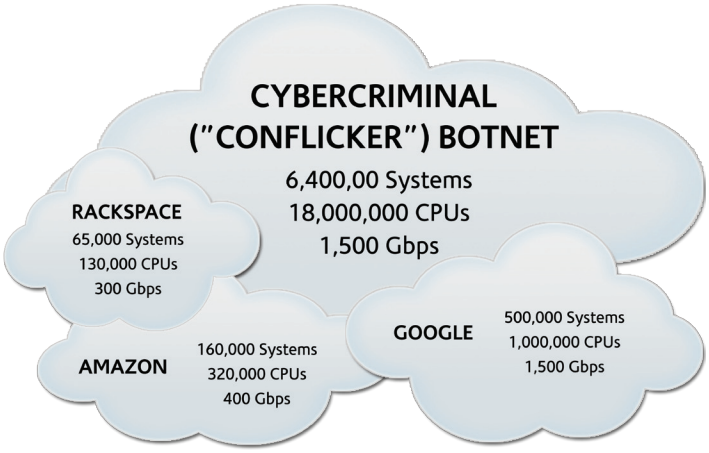
Botnets are a Pervasive Danger

Bots are autonomous applications that are often, but not always, malicious in nature. Cybercriminals create bots for financial gain, forming vast networks of these applications that can infect networks and do massive damage before they are detected. It is estimated that as many as 25% of computers connected to the Internet may be infected by botnets. These infected systems are often referred to as "zombies". Once a bot 'phones home' to one of thousands of command and control hosts, it becomes one of millions forming a botnet. They subsequently receive instructions to conduct malicious activities such as replicating themselves, sending new malware or allowing data leakage.

Not a New Market Problem

Botnets are not new but the damaging impact has only expanded as more sophisticated technologies become available. Whether created by using botnet tool kits that criminals can rent, or built as customized attacks aimed at specific target companies or institutions, botnets are frustrating IT security vendors because existing solutions have failed to prove 100% effective , even among Fortune 500 companies. And as this diagram depicting the conflicker botnet illustrates, botnets can be massive when compared with even the largest legitimate cloud networks.

Traditional methods for stopping botnets such as signature, heuristic & behavioral techniques on the endpoint, across the network, or at the gateway are estimated to be no more than 50% effective today. In the case of customized botnet attacks, these traditional approaches are totally ineffective.



Malicious Botnets can Dewarf other Cloud-Based Networks

Customer Impact

Botnets are pervasive and can have a devastating effect on businesses, including:

- The financial loss, including regulatory non-compliance fines and litigation, associated with the theft of sensitive customer/client/patient data or intellectual property leakage
- Damage to eReputation from phishing sites or proxy nets
- The hassle and cost of having to take preventive measure in the case of click fraud, DDoS and SPAM
- The cost of procuring and implementing multiple solutions to detect or prevent compromised endpoints as recommended by many IT security vendors
- The costs associated with acquiring expensive startup anti-botnet appliances

EdgeWave™

Technology Overview

iPrism

iPrism Web Security Delivers Unique and Effective Botnet Protection

iPrism Web Security leverages a comprehensive botnet threat index to bring an additional layer of defense to your gateway security and one that is more effective than others on the market. By enforcing the comprehensive botnet threat index, which is continuously updated, iPrism Web Security is able to block any attempt at an outbound connection to command and control centers outside your network, and instantly mitigate botnet threats. This approach offers significant advantages over any botnet defense our competitors are able to offer:

- The botnet threat index is continuously updated, based on four feeds from three industry-leading sources: Abuse.ch, ShadowServer and Cyber-TA. iPrism leverages these continuous updates to respond to new botnet threats immediately.
- The botnet threat index is a proven service with no known false-positives and its experts constantly update their feed sources and correlation engine to mitigate false positives from blocking legitimate traffic.
- The botnet threat index is cloud-based and synchronized hourly through EdgeWave's Circumvention Defense Network. This intelligence of thousands of known, active malicious botnet hosts are sent to your on-premises iPrism where enforcement occurs and botnets are stopped.
- iPrism Web Security enforces the botnet threat index by inspecting outbound traffic and monitoring and blocking bot-related malware attempting to "phone home"

Why iPrism Botnet Protection is Better

iPrism stops emerging botnet threats at their source, by preventing existing or newly compromised endpoints from breaching your network and causing damage from data leakage and other malicious or illegal activities. Only iPrism leverages a comprehensive botnet threat index in this unique and effective way, assuring defense that:

- Incurs no known false positives
- Does not require tweaking rules such as reputation score thresholds
- Adds 5-10% catch rates to your existing AV, anti-malware defense
- Mitigates financially damaging data leakage and regulatory non-compliance problems
- Assures the preservation and non-repudiation of logged records
- Performs without adding any network latency

EdgeWave Secure Content Management Solutions

EdgeWave™ develops and markets innovative Secure Content Management (SCM) solutions including iPrism Web Security and the ePrism Email Security Suite with next-generation solutions for Email Filtering, Continuity, Data Loss Protection, Encryption and Archive. EdgeWave innovative technologies deliver comprehensive protection with unrivalled ease of deployment and the lowest TCO on the market. The company's award winning solutions can be delivered as hosted, on-premises, and hybrid services.

Contact Us
1-800-782-3762
www.edgewave.com

Corporate Office
15333 Avenue of Science, San Diego, CA 92128

Phone: 858-676-2277 Fax: 858-676-2299
Toll Free: 800-782-3762 Email: info@edgewave.com

EW-TO-DS-01/12