RedSpam – Cloud Based Security

The countermeasures detailed in this document are the various techniques RedSpam use to identify and filter the undesirable traffic. The undesirable attack traffic may come in large quantities with the intent of using brute force to overwhelm the victim system or it could come shaped in a well crafted way, designed to disrupt normal service performance. RedSpam mitigations are designed to allow desirable traffic through to the destination while lowering the impact of undesirable traffic. RedSpam use various “countermeasures” to target and remove as much of the attack traffic as possible, and to allow our client’s service to continue operating.

Description	Common names	Countermeasures
Flood Attacks		
• Flood of traffic for a specific protocol or application port • Can be designed to look like normal traffic or just floods of IP traffic • Reflection attacks • May be spoofed or non spoofed	Ping Attack, Smurf Attack, reflection attacks, UDP flood, Stream, dc++, blackenergy	Global Exception List, Geo-IP validation, Per client Black/White List, Countermeasure driven Blacklist, Geo-IP Filtering, Global Botnet Filter.
Fragmentation Attacks		
• A flood of TCP or UDP fragments are sent to a victim overwhelming the victim’s ability to reassemble the streams and severely reducing performance • Fragments may also be malformed in some way • May be a result of a network mis-configuration	Teardrop, Targa3, Jolt2, Nestea	Global Exception List, Geo-IP validation, Per client Black/White List, Countermeasure driven Blacklist, Geo-IP Filtering, Global Botnet Filter.
TCP Stack Flood Attacks		
• TCP stack flood attacks are attacks designed to exploit TCP state limitations within security and web infrastructure • May be spoofed or non spoofed	TCP SYN, TCP FIN, TCP RST, TCP SYN-ACK, TCP URG-PSH, TCP Flags	Global Exception List, Geo-IP validation, Per client Black/White List, Countermeasure driven Blacklist, Geo-IP Filtering, Global Botnet Filter, Zombie Management & Control, TCP SYN Authentication.
Connection Attacks		
Connection attacks maintain a large number of half-open or fully open idle TCP connections. Exhausting a host or security devices state table	TCP Idle attack, CC attack	Global Exception List, Geo-IP validation, Per client Black/White List, Countermeasure driven Blacklist, Geo-IP Filtering, Global Botnet Filter, Zombie Management and Control, TCP SYN Authentication, TCP Connection Reset.
Application Attacks		
Application attacks are designed to exploit a performance issue within an application or service	HTTP GET floods, SIP Invite floods, DNS amplification attacks	Global Exception List, Geo-IP validation, Per client Black/White List, Countermeasure driven Blacklist, Geo-IP Filtering, Global Botnet Filter, Zombie Management and Control, TCP SYN Authentication, HTTP Authentication, HTTP Object Rate Limiting, HTTP Request Rate Limiting, Malformed HTTP, HTTP Header Regex Filtering, TCP Connection Reset, DNS Proxy, Malformed DNS, DNS Authentication, Regular Expression Filter, Bandwidth Enforcement, Protocol Enforcement, Traffic shaping, Malformed SIP, SIP Source Rate Limiting
Vulnerability Exploit Attacks		
Vulnerability exploit are designed to exploit a flaw in an application or operating system.	Most Worms and Trojans, Land, Xmas Tree, Ping of Death, Targa3, Kiss of Death, Nuke	Global Exception List, Geo-IP validation, Per client Black/White List, Countermeasure driven Blacklist, Geo-IP Filtering, Global Botnet Filter, Zombie Management and Control, TCP SYN Authentication, HTTP Object Rate Limiting, HTTP Request Rate Limiting, Malformed HTTP, HTTP Header Regex Filtering, DNS Proxy, Malformed DNS, DNS Authentication, Regular Expression Filter

RED SPAM

FEATURES & BENEFITS

DEDICATION

We are dedicated solely to defending organisations from the damage caused by DDoS attacks.

TECHNOLOGY

RedSpam's solution is based on a combination of world class hardware and software solutions combined with our own mitigation technologies encompassed within a single management framework to offer you a world class protection service.

RESILIENCE

Each PoP is located in safe and secure data centre environment, managed by some of the world's leading data centre providers.

LOCATION

Our scrubbing centres are located in central London and London Docklands, ensuring minimal latency and flexible peering for the EMEA market.

INNOVATION

Our continual monitoring of traffic and mitigation of attacks enables our experts to identify ever changing attacks, improving mitigation solutions to the most complex attacks.

FLEXIBILITY AND AFFORDABILITY

Fixed cost with no additional overage or hidden extras irrelevant of the size or duration of an attack.

SIMPLICITY

The needs of organisations differ and we have therefore designed a range of service packages priced to meet a range of budgets making the protection accessible to all.

ISP AGNOSTIC

RedSpam are truly ISP and hosting company agnostic, no matter who you choose for your hosting or bandwidth.

'**Countermeasures**' are defence mechanisms that are designed to stop different types of attack traffic. Some attacks are effectively blocked by a single countermeasure, while other attacks are best handled by a combination of several countermeasures. All countermeasures together provide a strong in depth approach to attack mitigation.

Countermeasure	Technology	Description
Global Exception List	Router ACL, Arbor	The Global Exception List is a single traffic filter that is applied to all traffic destined for RedSpam clients.
Geo-IP validation	RedSpam IP Validation Engine	RedSpam developed packet filtering appliance that validates an IP packet has not been spoofed outside of a geographic region
Per client Black / White List	Router ACL, Arbor	Configurable filter lists based on threat analysis and feedback from Customer systems
Countermeasure driven blacklist	Router ACL, Arbor	Packet filter to discard IP packets on an event driven basis.
Geo-IP Filtering	Arbor	Discard packets based on their geo-graphic source location, based on customer requirements
Zombie Management & Control	Arbor	Rate limiting and control from suspected zombie hosts
TCP SYN Authentication	Arbor	A mechanism for validating that clients are attempting to build and maintain correct TCP state
HTTP Authentication	Arbor	A challenge mechanism to ensure a client is behaving as expected from a HTTP perspective
HTTP Object Rate limiting	Arbor	Limits the number of HTTP objects a host can request.
HTTP Request Rate limiting	Arbor	Limits the number of HTTP requests any client can generate
Malformed HTTP	Arbor	Validates HTTP requests are formatted correctly
HTTP Header Regex Filtering	Arbor	Filtering traffic based of regex pattern matching in the HTTP header
TCP Connection Reset	Arbor	Clears open, idle TCP connections
Malformed DNS	Arbor	Validates DNS requests are formatted correctly
DNS Authentication	Arbor	A mechanism to protect against DNS request attacks that request information for randomized names or use spoofed source addresses
Regular Expression Filter	Arbor	TCP/UDP Payload filtering
Bandwidth Enforcement	Arbor	Dynamically drops traffic sourced from subnets whom historically have generated no traffic to the protected hosts
Protocol Enforcement	Arbor	Dynamically drops traffic using protocols that protected hosts have not historically been utilising
Traffic Shaping	Router ACL's, Arbor	Rate limit traffic forwarded to a customers infrastructure
Malformed SIP	Arbor	Validates SIP packets are formatted correctly
SIP Source Rate Limiting	Arbor	Limits the rate SIP requests are received from a host

RED SPAM