

# RedSpam DDoS Introduction

## What is a DDoS Attack?

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access vital information.

► \$150

This is enough to buy a week-long DDoS attack on the black market with a money back guarantee to disable online assets

► More than 2,000

This is the number of DDoS attacks launched on any given day with varying size and severity

► 1/3

Of all downtime incidents are attributed to DDoS attacks

## INTRODUCTION TO REDSPAM:

RedSpam delivers market leading cloud based and cloud/ on-premise hybrid DDoS detection and mitigation services. These services deliver comprehensive protection for your organisations website and online assets. Delivering a highly reliable and cost-effective solution that guarantees business continuity in the face of an attack.

Our **Monitor, Manage and Mitigate approach** is based on a combination of industry-leading hardware and patent-pending software offering unparalleled protection. Attacks are quashed close to source while genuine traffic is never compromised. We deliver a robust service through early threat detection and seamless integration 3-way mitigation.

## WHY WORK WITH US:

RedSpam's 24/7 365 'lights on' Security Operations Centre (SOC) continues to successfully mitigate multi-layer DDoS attacks in even the most demanding of environments. Our dedicated team has many years of experience dealing with targeted attacks ranging from volumetric to sophisticated application layer attacks.

We can deploy over 30 different DDoS mitigation techniques tailoring the service dependent on each different client and threat level.

## Key Benefits:

- ⊕ Same-day fixed price quotations for the protection level required
- ⊕ Best of breed mitigation solutions, with custom built in house tools
- ⊕ Mitigation methods tailored to suit the needs of individual customers
- ⊕ 'Emergency services' for customers requiring protection using DNS redirection

**KEY BENEFITS:**

- Focuses on the customer edge.
- Ensures application availability
- Provides immediate protection from threats
- Provides complete DDoS protection within a single user interface.
- Provides advanced DDoS blocking.
- Prevents volumetric DDoS attacks by signalling upstream ISPs
- Prevents emerging botnet and application-layer attacks.
- Provides real-time and historical traffic forensics and reports.

**WHO WE WORK WITH:**

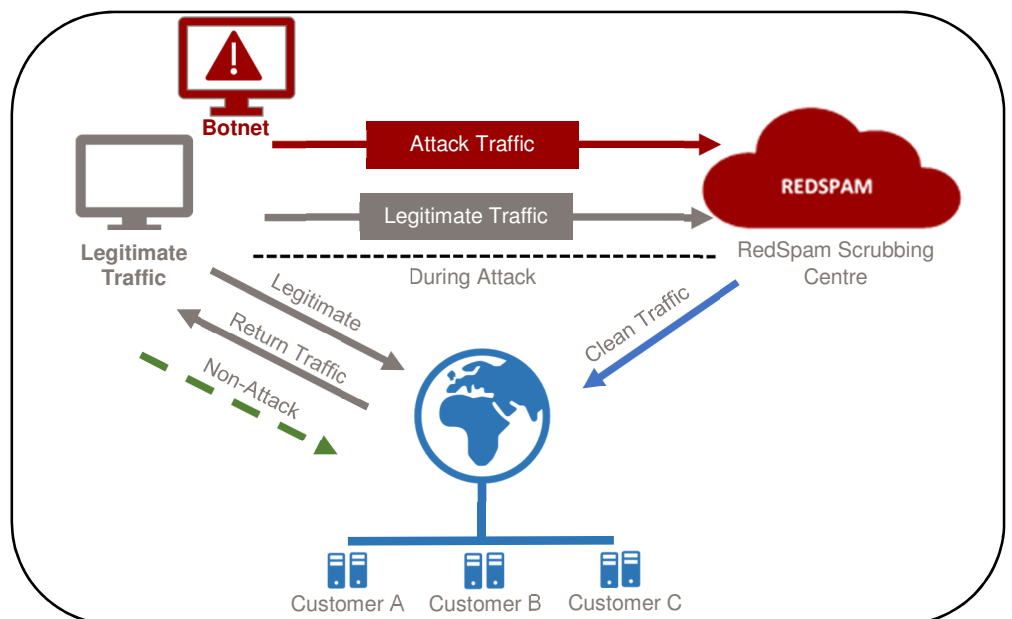
Our clients belong to a range of different sectors but all having one thing in common that their financial survival depends upon being able to effectively defend their IT assets.


**HOW WE KEEP YOUR DIGITAL ASSETS SAFE:**

The first stage, when working with a new customer, is to build up a profile of what normal traffic patterns look like. This helps to improve the speed with which we can identify when attack is underway. Analysing traffic anomalies compared to normal patterns and instantly rerouting all traffic to a clearing house where it is scrubbed clean before being routed back to the customer.

To detect when an attack is underway and to classify activity we use a combination of both signature analysis and dynamic profiling. Helping to ensure all bogus traffic is blocked at source and online assets are unaffected.

The diagram below highlights how RedSpam is able to rapidly redirect potentially hazardous traffic while normal traffic is able to remain unaffected:

**Threat Redirection Map:**

**REDSPAM:**

RedSpam provide fully managed global 24x7x365 DDoS protection and mitigation solutions that prevent targeted malicious attacks from reaching your customers' infrastructure. RedSpam offer a breadth of solutions, services and technologies and a wealth of experience that helps protect and secure your business.