Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks

Document ID: 13634

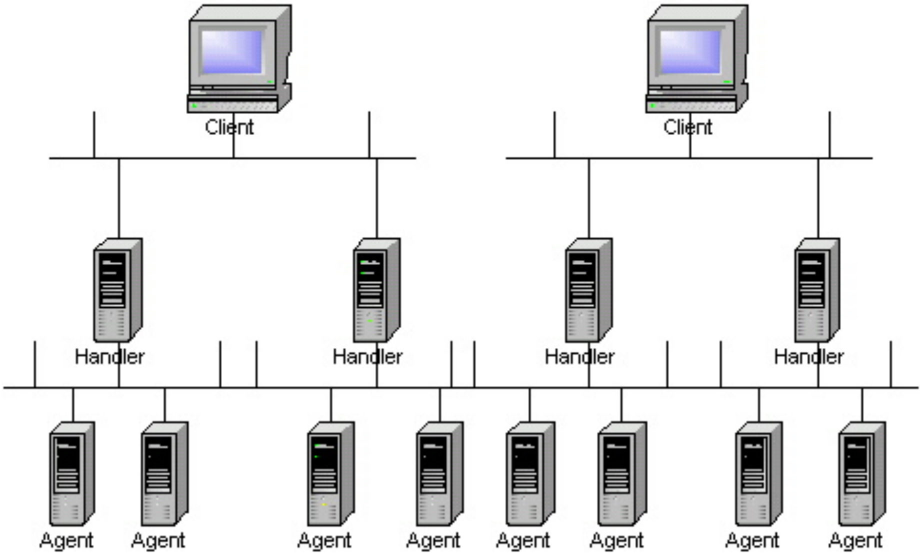
Contents

Introduction

This white paper contains information in order to help you understand how Distributed Denial of Service (DDoS) attacks are orchestrated, recognize programs used to facilitate DDoS attacks, apply measures to prevent the attacks, gather forensic information if you suspect an attack, and learn more about host security.

Understanding the Basics of DDoS Attacks

Refer to this illustration:



Behind a **Client** is a person that orchestrate an attack. A **Handler** is a compromised host with a special program running on it. Each handler is capable of controlling multiple agents. An **Agent** is a compromised host that runs a special program. Each agent is responsible for generating a stream of packets that is directed toward the intended victim.

Attackers have been known to use these four programs to launch DDoS attacks:

1. Trinoo
2. TFN
3. TFN2K
4. Stacheldraht