Denial of Service and Distributed Denial of Service Attacks have significantly shackled the development of computer networks and the internet, and masked their innumerable benefits behind many hours of service unavailability. These attacks are fostered, especially in their distributed variant, by networks of compromised machines (known as botnets, that is, a network of bots) that are taken over by a hacker / attacker, and coordinated in such a way as to channel overwhelming loads of malicious or useless traffic towards resource-providing / request-servicing servers. In the long run, a sufficient load of these traffic, overwhelm target servers and constitute them unable to service the requests of legitimate users that have subscribed legally to use these resources. This army of compromised systems have also been recently linked to various malicious and nefarious activities that have been taking place on computer networks and the internet in recent times; such activities relate to malware injection / infiltration, fraud, espionage, amongst others. This paper reviews the operations and
coordination of botnets and the interactions that take place within the botnet during such malicious activities. New, valuable insights are provided towards the detection of such malicious networks through the introduction of the reverse life cycle of botnets.

References


Index Terms

Computer Science
Information Systems

Keywords

Botnets, Cybercrimes, Information Security, Malware.