Cloud-based network telescope for Internet background radiation collection

Joseph O'Hara

April, 2019

Abstract

Botnets are collections of individual computers that have been taken over by an adversary in order to assemble a number of devices that can be controlled to cause disruption to services in the Internet. Distribution mechanisms for botnets scan IP address ranges of the Internet in order to find vulnerable computers that can be infected and added to existing networks. Researchers monitor blocks of IP addresses to detect scanning activities and other abnormal activities in the Internet; collectively referred to as Internet Background Radiation. A tool such as a network telescope, is used to monitor unused IP address ranges that are not hosting services and are not expected to receive legitimate network traffic.

This research proposes a novel network telescope design that is based on a diverse pool of IP addresses controlled by cloud computing providers. In contrast, traditional network telescope deployments that make use of a homogeneous, compact range of IP addresses, a diverse set of IP addresses offers the advantage that the assumed 'geographical' location of the IP addresses can be spread around the world. Also, in contrast to a block of IP addresses that may be identified as a trap and avoided by an attacker, a diverse set of IP addresses is more difficult to distinguish and avoid by possible attackers.

The data collected from this novel system was compared against data collected from a larger traditional network telescope monitoring a contiguous region of IP addresses for the same period. This research focused on the ability of the systems to detect the presence of a particular botnet. While it has been known that both larger and more diverse IP address ranges improve the performance of network telescopes, this research finds that the diversity of IP addresses is significantly more important.