Identification of Suspicious Moas Conflicts

Border Gateway Protocol, and hence the Internet is susceptible to various prefix related attacks. The Internet is composed of numerous Autonomous systems (AS) which is a collection of connected IP prefixes under one administrative control and having specific routing policies. Multiple Origin AS (MOAS) conflicts take place when more than one AS announce the specific IP prefix. MOAS can occur due to some fixed number of valid reasons such as misconfigurations, multi-homing or it can even occur due to intentional attacks. Such attacks may result in unavailability of services or users as traffic may get redirected from the intended destination. While solutions are available to detect MOAS conflicts and reasons behind such conflicts can be either valid or illicit, it is important to categorize them. Utilizing the RIPE raw data, we present a system and methodology to detect MOAS conflicts, analyse and classify them as suspicious or non-suspicious.