An Analysis of Malicious ASes in the Internet

Thousands of new Autonomous Systems (ASes) are emerging every year with most of them being malicious. Malicious ASes are primarily fully dedicated to facilitate Cybercrime. Legitimate but abused ASes are the ASes which unwillingly host malicious activities because the machines that they host are abused. It’s very hard to differentiate between malicious ASes and abused ASes.

Analyzing the current malicious ASes would provide key information which can be used to build a new reputation system or to support any existing reputation system that can detect malicious ASes from Internet. In this project, we have analyzed frequency of ASes appearing in top 100 malicious ASes list, stability of malicious ASes neighbor set, country distribution of malicious ASes and abused ASes, how malicious ASes and legitimate but abused ASes are interconnected.