Botnet Tracking

Botnets are one of the major threats to the Internet today. This project aims to shed light on this phenomenon. Towards this goal, we established a scalable distributed data collection infrastructure to capture and track large collections of Botnets. Currently, our system is tailored to capture Botnets that use IRC to disseminate the Botmaster commands to his Bot armies. Our infrastructure collects Malware using a distributed Honeynet. The collected Malware is then analyzed to discover new IRC Botnets and extract their features to enable infiltration and longitudinal lightweight tracking. For more information, please visit the project's web page (no longer updated).