Abstract

Today's wide usage of the Internet makes malicious software (malware) and botnets a big problem. While anti-virus software is commonplace today, malware is constantly evolving to remain undetected. Passively monitoring DNS traffic on a network can present a platform for detecting malware on multiple computers at a low cost and low complexity. To explore this avenue for detecting malware we decided it was necessary to design an extensible system where the framework was separate from the actual detection methods. We wanted to divide the system into three parts, one for logging, one for handling modules for detection and one for taking action against suspect traffic. The system we implemented in C collects DNS traffic and processes it with modules that are compiled separately and can be plugged in or out during runtime. Two proof of concept modules have been implemented. One based on a blacklist and one based on geolocation of requested servers. The system is complete to the point of being ready for field testing and implementation of more advanced detection modules.