World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:04, 2014

Automatic Intelligent Analysis of Malware Behaviour

Authors : Hermann Dornhackl, Konstantin Kadletz, Robert Luh, Paul Tavolato

Abstract : In this paper we describe the use of formal methods to model malware behaviour. The modelling of harmful behaviour rests upon syntactic structures that represent malicious procedures inside malware. The malicious activities are modelled by a formal grammar, where API calls' components are the terminals and the set of API calls used in combination to achieve a goal are designated non-terminals. The combination of different non-terminals in various ways and tiers make up the attack vectors that are used by harmful software. Based on these syntactic structures a parser can be generated which takes execution traces as input for pattern recognition.

Keywords : malware behaviour, modelling, parsing, search, pattern matching
Conference Title : ICISAI 2014 : International Conference on Information Security and Artificial Intelligence
Conference Location : Venice, Italy
Conference Dates : April 14-15, 2014