Data Mining methods for malware detection

Daniel Boța
Faculty of Mathematics and Computer Science, Babeș-Bolyai University
dbota@cs.ubbcluj.ro

New malicious programs, known as malware, are created every day. In the last decade, the occurrence rate and the amount of malware have become very high. The classical approach, meaning signature-based detection, can not keep up with this overwhelming wave of new and sophisticated malicious codes and can not detect the new previously unseen malware for which there are no signatures. In this regard, we need fast and reliable detection methods that are able to detect them.

The inability of traditional methods to catch these new breed of malicious codes has shifted the focus of malware detection research to find more generalized and scalable methods that can detect malicious behavior as a process instead of a single static signature. Thus, the application of Data Mining methods for malware detection has shown good results compared to other approaches.

In this report, we investigate various Data Mining methods used for malicious executable detection.

References


