Pitfalls and Limits of Dynamic Malware Analysis

Dr. Tamas K LENGYEL,
Intel (USA)
tamas@tklengyel.com

Abstract

The presentation will cover a historic overview of the development of dynamic malware analysis systems, motivations behind it and the solutions developed over the years. The presentation will cover modern techniques to analyze malware using hypervisors, limitations of hypervisor introspection and modern sandbox evasion techniques used by malware. The presentation will conclude with a deep view into inherent computational limits of malware analysis and detail the problem with encoding assumptions about malware behavior that can be used to subvert the analysis process.