1. Record Nr. UNINA9910437578803321

Autore	Yin Heng
Titolo	Automatic malware analysis : an emulator based approach / / Heng Yin, Dawn Song
Pubbl/distr/stampa	New York, : Springer, 2013
ISBN	1-283-62478-8 9786613937230 1-4614-5523-5
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (82 p.)
Collana	SpringerBriefs in computer science, , 2191-5768
Altri autori (Persone)	SongDawn
Disciplina	005.8
Soggetti	Malware (Computer software)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Introduction -- Dynamic Binary Analysis Platform -- Hidden Code Extraction -- Privacy-breaching Behavior Analysis -- Hooking Behavior Analysis -- Analysis of Trigger Conditions and Hidden Behaviors -- Concluding Remarks.
Sommario/riassunto	Malicious software (i.e., malware) has become a severe threat to interconnected computer systems for decades and has caused billions of dollars damages each year. A large volume of new malware samples are discovered daily. Even worse, malware is rapidly evolving becoming more sophisticated and evasive to strike against current malware analysis and defense systems. Automatic Malware Analysis presents a virtualized malware analysis framework that addresses common challenges in malware analysis. In regards to this new analysis framework, a series of analysis techniques for automatic malware analysis is developed. These techniques capture intrinsic characteristics of malware, and are well suited for dealing with new malware samples and attack mechanisms.