1. Record Nr.   UNINA9910437564503321

   Titolo   Botnets / / Heli Tiirmaa-Klaar ... [et al.]

   Pubbl/distr/stampa   New York, : Springer, 2013

   ISBN   1-4471-5216-6

   Edizione   [1st ed. 2013.]

   Descrizione fisica   1 online resource (viii, 97 pages) : illustrations (some color)

   Collana   SpringerBriefs in cybersecurity, , 2193-973X

   Altri autori (Persone) Tiirmaa-KlaarHeli

   Disciplina   005.84

   Soggetti   Malware (Computer software)
                         Computer security

   Lingua di pubblicazione Inglese

   Formato   Materiale a stampa

   Livello bibliografico Monografia

   Note generali   "ISSN: 2193-973X."

   Nota di bibliografia Includes bibliographical references.

   Nota di contenuto   Foreword -- Botnets, Cybercrime and National Security -- Botnets: How
                         to Fight the Ever-growing Threat on a Technical Level.

   Sommario/riassunto   Malware poses one of the major threats to all currently operated
                         computer systems. The scale of the problem becomes obvious by
                         looking at the global economic loss caused by different kinds of
                         malware, which is estimated to be more than US$ 10 billion every year.
                         Botnets, a special kind of malware, are used to reap economic gains by
                         criminals as well as for politically motivated activities. In contrast to
                         other kinds of malware, botnets utilize a hidden communication
                         channel to receive commands from their operator and communicate
                         their current status. The ability to execute almost arbitrary commands
                         on the infected machines makes botnets a general-purpose tool to
                         perform malicious cyber-activities. Botnets provides a comprehensive
                         analysis of the topic, and comprises both technical and non-technical
                         sections written by leading cybersecurity experts. The non-technical
                         section addresses how botnet infrastructure could be exploited for
                         national security and cybercrime purposes. It approaches the subject as
                         a public policy issue and analyzes the phenomenon of botnets from
                         national security, law enforcement and regulatory policy perspectives,
                         and makes recommendations for policy-makers on different public
                         policies, highlighting the need for international response mechanisms.
                         The technical section provides insight into current botnet techniques
                         and discusses state-of-the-art countermeasures to combat the botnet

threat in detail. It includes new detection methods as well as different approaches to actively compromise running botnets.