DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation - DTU Orbit

DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation

The Internet of Things (IoT) revolution has not only carried the astonishing promise to interconnect a whole generation of traditionally “dumb” devices, but also brought to the Internet the menace of billions of badly protected and easily hackable objects. Not surprisingly, this sudden flooding of fresh and insecure devices fueled older threats, such as Distributed Denial of Service (DDoS) attacks. In this paper, we first propose an updated and comprehensive taxonomy of DDoS attacks, together with a number of examples on how this classification maps to real-world attacks. Then, we outline the current situation of DDoS-enabled malwares in IoT networks, highlighting how recent data support our concerns about the growing in popularity of these malwares. Finally, we give a detailed analysis of the general framework and the operating principles of Mirai, the most disruptive DDoS-capable IoT malware seen so far.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Örebro University, University of Rome La Sapienza
Corresponding author: Dragoni, N.
Contributors: De Donno, M., Dragoni, N., Giaretta, A., Spognardi, A.
Number of pages: 30
Pages: 1-30
Publication date: 2018
Peer-reviewed: Yes

Publication information
Journal: Security and Communication Networks
Volume: 2018
ISSN (Print): 1939-0114
Ratings:
Scopus rating (2018): CiteScore 1.81 SJR 0.311 SNIP 0.862
Web of Science (2018): Impact factor 1.376
Web of Science (2018): Indexed yes
Original language: English
Electronic versions:
7178164.pdf
DOIs:
10.1155/2018/7178164
Source: FindIt
Source ID: 2396578271
Research output: Contribution to journal › Journal article – Annual report year: 2018 › Research › peer-review