Analysing Malware Traffic

Alföldi Mátyás

August 13, 2020

Contents

Introduction

Source: https://www.malware-traffic-analysis.net/2020/07/31/index.html

Analysis

- Infected host:
  - 10.7.31.101
- Infected user:
  - gregory.simmons
- Infection process:
  1. A doc file is downloaded from 191.6.208.51(e-dsm.com.br) through http get /www/ZdJCAB/
  2. Afterwards a Get request from 10.7.31.101 to 67.20.112.81 (jambino.us/tv/DYsPb/)
  3. Finally we can see possible data exfiltration to 201.235.10.215 and 104.236.52.89
- Malware hashes
  - MD5:BEE97C2CD32806D16640A8C1ED4E080F (The doc file, a downloader)
  - MD5:B7EC256BD8CDB13EC031C4595514666E (emotet)