Analysing Malware Traffic

Alföldi Mátyás

June 15, 2020

Contents

Introduction

Source: https://www.malware-traffic-analysis.net/2018/UISGCON/index.html
Basic info:
LAN segment data:

- IP range: 172.16.1.0/24 (172.16.1.0 through 172.16.1.255)
- Gateway IP: 172.16.1.1
- Broadcast IP: 172.16.1.255
- Domain Controller (DC): Maricheika-DC at 172.16.1.3
- Domain: maricheika.net

Questions

- State the time and date of this infection.
  - 2018-10-01 18:38
- Determine the IP address of the infected Windows client.
  - 172.16.1.125
- Determine the host name of the infected Windows client.
  - ANATOLIY-PC
- Determine the MAC address of the infected Windows client.
  - b8:97:fa:74:de:c0
- Determine the Windows user account name used on the infected Windows client.
  - anatoliy.demchuk
- Determine the SHA256 hash of the Word document downloaded by the victim.
  - e2b0c9f57dcf08c0e14456f5cb54d8e50714c8e7a3a88cf818896dc8ba1dba51
- Determine the type of malware used in the initial infection.
  - Hancitor, later on Zeus
- Determine the public IP address of the infected Windows client.
  - From the api.ipify request: 31.44.188.95