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: 10.1.75.0/24 (10.1.75.0 through 10.1.75.255)
- Gateway IP: 10.1.75.1
- Broadcast IP: 10.1.75.255
- Domain Controller (DC): PixelShine-DC at 10.1.75.4
- Domain: pixelshine.net

Questions

- State the time and date of this infection.
    - 2018-10-01 18:55
- Determine the IP address of the infected Windows client.
    - 10.1.75.167
- Determine the host name of the infected Windows client.
    - RIGSBY-WIN-PC
- Determine the MAC address of the infected Windows client.
    - Resolved: MSITechn_8b:32:9e
- Determine the Windows user account name used on the infected Windows client.
    - judson.rigsby
- Determine the SHA256 hash of the Word document downloaded by the victim.
    - 1112203340b2d66f15b09046af6e776af6604343c1e733fe419fdf86f851caa3
- Determine the SHA256 hash of the first malware binary sent to the infected Windows client.
    - 0d7a4650cdc13d9217edb05f5b5c2c5528f8984dbbe3fbc85f4a48ae51846cc3
- Determine the time the Domain Controller (DC) at 10.1.75.4 became infected.
    - 2018-10-01 19:01:51 (Eternalblue, the malformed secondary request is sent around this time)
- Determine the SHA256 hash of the second malware binary sent to the infected Windows client (same file retrieved as radiance.png and table.png).
    - 0dc9d82d2f9d9ae27a1cb6d64ec7ab73bcee16d327027dba1273cbcc33849f9f
- What are the two file hashes for executables you can retrieve from the SMB traffic using Wireshark?
    - cf99990bee6c378cbf56239b3cc88276eec348d82740f84e9d5c343751f82560 (Trickbot)

  - 28c33a9676f04274b2868c1a2c092503a57d38833f0f8b964d55458623b82b6e (Trickbot)

- Determine the two families of malware the Windows client was infected with.
  - Emotet, Trickbot

- Determine the one family of malware the DC was infected with.
  - Trickbot

- Determine the public IP address of the infected Windows client.
  - 109.238.74.213