Analysing Malware Traffic

Alföldi Mátyás

November 1, 2020

Contents

Introduction

- LAN segment range: 10.72.33.0/24 (10.72.33.0 through 10.72.33.255)
- Domain: omegacast.net
- Domain controller: 10.72.33.10 - Omegacast-DC
- LAN segment gateway: 10.72.33.1
- LAN segment broadcast address: 10.72.33.255

Incident Report

Indication of Compromise:

- Alerts:
  - ET CNC Feodo Tracker alerts
  - Unusual Port usage (59681 -¿ 8080)
  - ETPRO TROJAN* alerts
  - ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected* alerts
  - OpenSSL Demo CA/External IP Address Lookup
  - SURICATA SMTP invalid reply (In connection with the previous alerts, this could indicate data exfiltration)
- Forensic Analyst Report:
  - Scheduled task creation(starts a launcher.bat file)/registry modification
  - doc file with malicious macro, sent as an invoice. https://www.virustotal.com/gui/file/2beec2edda2346042fdfa829caaa7403e7842e786b9b9e89baaf4cd5e45d189a
  - Creation of pseudorandom path in the users home directory
  - Malicious PE artifacts found:
    - https://www.virustotal.com/gui/file/b13aecd25a8f1a681033437ba831e13c01098c1cdfe721d24c9e2e80fe98c918
    - https://www.virustotal.com/gui/file/34873d81dc7a0468d941294a1c62f9bb9e110d0f333f55de2da41ac6ead400d7

Infected Host Info:

- MAC address: 0c:d2:92:4b:25:a7
- IP address: 10.72.33.165
- Host name: DESKTOP-5I7XDSY
- User account name: byron.ostrander