Analysing Malware Traffic

Alföldi Mátyás

June 14, 2020

Contents

Introduction

Source: https://www.malware-traffic-analysis.net/2019/11/12/index.html
Basic info:
LAN segment data:

- LAN segment range: 10.11.11.0/24 (10.11.11.0 through 10.11.11.255)
- Domain: okay-boomer.info
- Domain controller: 10.11.11.11 - Okay-Boomer-DC
- LAN segment gateway: 10.11.11.1
- LAN segment broadcast address: 10.11.11.255

Questions

- What operating system and type of device is on 10.11.11.94?
  - Based on TTL=64, Don't fragment flag set, Maximum segment size of 1460, and a Window size which isn't any common, so one can safely assume that it is variable, the OS is Linux. Based on the MAC address it is related to Foxconn, so it is either a gaming console or a mobile device.
  - Based on HTTP requests it uses Chrome OS, so it is most likely a Chromebook. (Although User-Agents can usually be easily modified, but assuming that this is a company setting it isn't that likely that someone would modify it.)
- What operating system and type of device is on 10.11.11.121?
  - Based on the same values as for .94 this is also has Linux on it.
  - Looking at http requests Android 9, and it is a SAMSUNG SM-N950U
- Based on the MAC address for 10.11.11.145, who is the manufacturer or vendor?
  - Motorola
- What operating system and type of device is on 10.11.11.179?
  - OS X (looking into the http requests confirms this). It is probably a Macbook
- What version of Windows is being used on the host at 10.11.11.195?
  - It seems like Windows 10, based on http requests
- What is the user account name used to log into the Windows host at 10.11.11.200?
  - brandon.gilbert based on the CNameString in kerberos communication.
- What operating system and type of device is on 10.11.11.217?
  - It looks like a Linux device based on IP/TCP headers, but the manufacturer is apple
  - http requests show that it is an iPad
- What IP is the Windows host that downloaded a Windows executable file over HTTP?

  - 10.11.11.203 (40group.tiff)

- What is the URL that returned the Windows executable file?
  - acjabogados.com/40group.tiff
- What is the SHA256 file hash for that Windows executable file?
  - 8d5d36c8ffb0a9c81b145aa40c1ff3475702fb0b5f9e08e0577bdc405087e635
- What is the detection rate for that SHA256 hash on VirusTotal?
  - 58/72
- What public IP addresses did that Windows host attempt to connect over TCP after the executable file was downloaded?
  - 138.201.6.195 which is reported to have been a C2 server for various malware, but mostly IcedId
- What is the host name and Windows user account name used on that IP address?
  - host: TUCKER-WIN7-PC
  - user: candice.tucker