Analysing Malware Traffic

Alföldi Mátyás

June 14, 2020

Contents

Introduction

Source: https://www.malware-traffic-analysis.net/2020/06/12/index.html
Basic info:
LAN segment data:

- LAN segment range: 10.6.12.0/24 (10.6.12.0 through 10.6.12.255)
- Domain: frank-n-ted.com
- Domain controller: 10.6.12.12 - Frank-n-Ted-DC
- LAN segment gateway: 10.6.12.1
- LAN segment broadcast address: 10.6.12.255

Analysis

0.1 Network devices on the subnet

The subnet is 10.6.12.0/24

- 10.6.12.12
  - Seems to be a Windows machine based on IP/TCP header
- 10.6.12.157
  - Windows machine. Based on the User Agent win 10
  - Hostname: DESKTOP-86J4BX
  - User: ted.brokowski
- 10.6.12.203
  - Also a windows machine. Based on the User Agent also a win 10
  - Hostname: LAPTOP-5WKHX9YG
  - User: frank.brokowski

0.2 Possibly Malicous Files Downloaded

0.2.1 invoice-86495.doc

This one isn't detected, further checking will be needed to determine if it is really harmless.

0.2.2 june11.dll

https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
It has a relatively high detection rate, so it is most certainly malicious, although the exact type can't be said for sure based on what the AV vendors detect, but possibly a Zbot.

0.3 Suspicious connections

There are quite a few Http requests to 5.101.51.151 (snnmnkxdhflwgth-qismb.com), which is reported to be malicious(C2).
Its post.php seems to be used for communication.
Also there is the connection between 10.6.12.203 and 205.185.125.104.
The first is a get to /pQBtWj and afterwards we can see the downloading of the june11.dll.

0.4 How did the infection take place

What I can say for sure, is that 10.6.12.157 opened the .doc file, and afterwards 10.6.12.203 connected to the malicious ip, where it downloaded the dll, will have to see if these events have anything related.
A strong indication that 10.6.12.157 was infected first is what seems like suspicious SMB communication.
Right after the negotiation and session setup, it tries to access the DC-s IPC share.
Although this all happened even before the .doc file was downloaded.