Analysing Malware Traffic

Alföldi Mátyás

May 29, 2020

Contents

Introduction **2**

Interesting Alerts **3**

Pcap Analysis **4**

0.1 Communication with the Trickbot C&C servers 4

0.1.1 182.141.27.238 4

0.1.2 45.148.120.153 4

0.1.3 51.254.164.244 4

0.1.4 190.214.13.2 4

0.1.5 185.180.198.50 4

0.1.6 64.44.133.131 4

0.1.7 203.176.135.102 4

Introduction

Source: http://www.malware-traffic-analysis.net/2020/03/14/index.html
Basic info:
LAN segment data:

- LAN segment range: 10.3.11.0/24 (10.3.11.0 through 10.3.11.255)
- Domain: mondogreek.com
- Domain controller: 10.3.11.3 - Mondogreek-DC
- LAN segment gateway: 10.3.11.1
- LAN segment broadcast address: 10.3.11.255

Interesting Alerts

Looking through the alerts the first that struck me is the following:

- ET POLICY exe download via HTTP

The payload contains bolton-tech.com and there is a get for YAS20.exe. A quick google search gave me the urlhaus.abuse.ch link which mentions that a malware was hosted there together with a virustotal link to it. Opening the link various av products recognize it as either a backdoor or a dropper. The next interesting alerts are the following:

- ET CNC Feodo Tracker Reported C&C Server group $n, n \in N$

Looking at the IP addresses they are Trickbot C&C servers, the IP addresses to which connection is established are the following:

- 185.141.27.238
- 45.148.120.153
- 51.254.164.244
- 190.214.13.2
- 185.180.198.50
- 64.44.133.131
- 203.176.135.102

Next alerts show that the malware initiates a connection to 64.44.133.131 and another executable is downloaded.
We can be sure that it is the malware itself, since the User-Agent WinHTTP loader/1.0 is associated with it.
(A quick lookup confirms that this is another Trickbot C&C server.) Continuing the search an http request occurs to the C&C server 203.176.135.102, which might also be data exfiltration, since part of the content looks the following way: website—user—password. Data exfiltration seems to continue later on to this C&C server. Meanwhile another executable is downloaded from 64.44.133.131.

Pcap Analysis

Looking at the pcap file I can see that there are 2 hosts and only 10.3.11.194 is the one that gets infected, so filtering for communications containing that IP will remove some noise. (The user using it is otis.witherspoon.)

0.1 Communication with the Trickbot C&C servers

0.1.1 182.141.27.238

The host sends out Syn packets and after 3 syn-s the C&C server sends an RST,ACK.(The 3way handshake is never established, since after a few Syn packets the server always sends an RST.)

0.1.2 45.148.120.153

With this there is mostly tls communication, so the only way to actually try this out is to set up the key storage on windows and import the file into wireshark, then run the malware sample.

0.1.3 51.254.164.244

Same as above.

0.1.4 190.214.13.2

Same as above.

0.1.5 185.180.198.50

Same as with 182.141.27.238

0.1.6 64.44.133.131

Here we can see something interesting. The infected host asks for a png, but it turns out that it is an executable actually that it sends. (MZ and This program cannot be run in Dos mode string found in it.) Afterwards another executable is downloaded when get request goes out for a picture.

0.1.7 203.176.135.102

This is the one for data exfiltration. The order in which data is exfiltrated:

1. Accounts/passwords from different browsers
2. Process list and various system information (Possibly for further attacks)