Analysing Malware Traffic

Alföldi Mátyás

June 11, 2020

Contents

Introduction

Source: http://www.malware-traffic-analysis.net/2020/01/30/index.html
Basic info:
LAN segment data:

- LAN segment range: 10.5.28.0/24 (10.5.28.0 through 10.5.28.255)
- Domain: catbomber.net
- Domain controller: 10.5.28.8 - Catbomber-DC
- LAN segment gateway: 10.5.28.1
- LAN segment broadcast address: 10.5.28.255

Questions

- Based on the Trickbot infection's HTTP POST traffic, what is the IP address, host name, and user account name for the infected Windows client?
  - IP: 10.5.28.229
  - Host: CAT-BOMB-W7-PC
  - User: phillip.ghent
- What is the other user account name and other Windows client host name found in the Trickbot HTTP POST traffic?
  - User: timothy.sizemore
  - Host: CAT-BOMB-W10-PC
- What is the infected user's email password?
  - gh3ntf@st
- Two Windows executable files are sent in the network traffic. What are the SHA256 file hashes for these files?
  - cursor.png 4e76d73f3b303e481036ada80c2eeba8db2f306cbc9323748560843c80b2fed1
  - imgpaper.png 934c84524389ecfb3b1dfcb28f9697a2b52ea0ebcaa510469f0d2d9086bcc79a

Analysis

Uploading the pcap file to virustotal, gives us some helpful snort/suricata alerts.
(Which also confirm the existence of a Trickbot infection.)
Interesting DNS requests:

- wtfismyip.com
- 5efxqhk2zhgnc24l.onion
- api.ipify.org

Interesting HTTP Requests:

- http://36.89.106.69/yas33/CAT-BOMB-W7-PC_W617601.1071BE9788304FBD0C52B1EE36701166/83/
- http://36.89.106.69/yas33/CAT-BOMB-W7-PC_W617601.1071BE9788304FBD0C52B1EE36701166/81/
- http://36.89.106.69/yas33/CAT-BOMB-W7-PC_W617601.1071BE9788304FBD0C52B1EE36701166/81/
- http://36.89.106.69/yas33/CAT-BOMB-W7-PC_W617601.1071BE9788304FBD0C52B1EE36701166/81/
- http://203.176.135.102:8082/yas33/CAT-BOMB-W7-PC_W617601.1071BE9788304FBD0C52B1EE36701166/90
- http://162.216.0.163/ico/VidT6cErs
- http://162.216.0.163/ico/VidT6cErs
- http://wtfismyip.com/text
- http://icanhazip.com/
- http://162.216.0.163/images/imgpaper.png (Actually a PE file + WinHTTP loader/1.0 User Agent)
- http://162.216.0.163/images/cursor.png (Same as the above)
- http://203.176.135.102:8082/jim734/CATBOMBER-DC_W617601.6019FD9E35E11D1F54B4CABDE0F3477D/90

Looking into the pcap file one can see, that process list, general machine data, and email account/passwords are exfiltrated. Also something interesting is the Eternalblue exploitation, which can be seen between 10.5.28.229 and 10.5.28.8.