Analysing Malware Traffic

Alföldi Mátyás

October 6, 2020

Contents

Introduction

Source: https://www.malware-traffic-analysis.net/2020/09/25/index.html

- LAN segment range: 10.0.0.0/24 (10.0.0.0 through 10.0.0.255)
- Domain: pascalpig.com
- Domain controller: 10.0.0.10 - Pascalpig-DC
- LAN segment gateway: 10.0.0.1
- LAN segment broadcast address: 10.0.0.255

Incident Report

Basic info about the infected host

- Ip: 10.0.0.179
- Name: DESKTOP-M1JC4XX (From kerberos comm.)
- User: ronaldo.paccione (From kerberos comm.)

Malware info:

- Source: 198.12.66.108
- Executable name: jojo.exe
- md5: AD6564701054B692BCF47B5FEB6324A2
- virustotal: https://www.virustotal.com/gui/file/1e4b7d7868d25071db67da87392fd5dafab344a9fa6dc040f7afb0699152fc13

Starting process of the malware infection:

- Based on knowing that WinHttpRequest was called and the single HTTP Get can be seen in the packet, it all started from a macro, probably from a word document.

Possible C2s:

- 37.120.174.218 (Lets Encrypt Free SSL Cert used)

Further indication of compromise:

- api.ipify.org usage
- SMTP communication with 185.61.152.63
  - The infected host logs in with the user am9qb0BiaWczLmljdQ== (base64-d jojo@big3.icu)
  - it sends an email to itself, since RCPT TO is jojo@big3.icu too
  - The subject has the user and the host name, and various data is exfiltrated, including usernames/passwords.
  - Later on also a large encrypted block gets sent. (Further analysis of the malware needed for more info)
  - The alrert also signals that this is related to AgentTesla