Analysing Malware Traffic

Alföldi Mátyás

March 17, 2021

Contents

Introduction

- LAN segment range: 10.2.8.0/24 (10.2.8.0 through 10.2.8.255)
- Domain: ascolimited.com
- Domain controller: 10.2.8.2 - AscoLimited-DC
- LAN segment gateway: 10.2.8.1
- LAN segment broadcast address: 10.2.8.255

Executive Summary

Bill Cook got infected with multiple malware at around 16:00 UTC on 2021-02-08.

Details

- User: bill.cook
- PC: DESKTOP-MGVG60Z
- MAC: 00:12:79:41:c2:aa

IoCs

Cobalt Strike:

- https://www.virustotal.com/gui/file/e519c1e99f21fbc6754e2ed9ef38a12684d506617229b4ca87fcff86f6838250/detection
- 8.208.10.147(roanokemortgages.com)
- 198.211.10.238 (also possible data exfiltration through http POST)

Ficker Stealer/Zudochka:

- 185.100.65.29
- 8.208.10.147(roanokemortgages.com)
- https://www.virustotal.com/gui/file/94e60de577c84625da69f785ffe7e24c889bfa6923dc7b017c21e8a313e4e8e1/detection

Hancitor:

- 45.124.85.55(tonmatdoanminh.com) (source of malicious doc.)
- 213.5.229.12 (Possible data exfiltration through http POST)
- api.ipify.org lookup