Nerden tot een uurtje of vier

Datum:
22 februari 2022
Document nummer:
2022/003/DOC-CY

Inleiding

Uit de analyse van de SIGINT hits en de implant artefacten hebben we pannenkoekenpalazzo.nl kunnen identificeren als C2 server. We hebben een tap aangesloten en de data stroomt binnen. We willen in ieder geval graag weten hoe de actor communiceert met deze server.

Challenge

PCAP

2 vlaggen

We hebben de volgende vragen voor je:

- Vanaf welk upstream IP adres maakt de actor verbinding met de server?
- Hoe heet de CTO van Electron B.V.?
- Wie heeft het Electron B.V. Tafelvoetbal Extravaganza toernooi gewonnen?
- Wat probeerde de CEO te beschermen?