Welkom in Cyberspace

Datum:
15 februari 2022
Document nummer:
2022/001/DOC-CY

Inleiding

Op 14 februari is er na 12 maanden radiostilte weer een spoor aangetroffen van de ZUURKOOL actor. De netwerkdetectieregels voor ROOKWORST zijn afgegaan op de SIGINT stroom. Het gedetecteerde verkeer is afkomstig van de externe gateway van Electron B.V. op 192.0.2.3. Het verkeer komt overeen met beacons van de bekende ZUURKOOL implant, ROOKWORST.

Challenge

1 vlag

Een rustig begin. We hebben het inlichtingendossier gevuld met de afschalingsnota van het onderzoek naar ZUURKOOL[1], suricata regels voor de ROOKWORST implant, en 2 geselecteerde pakketten.

1 "Rapport: Afschaling onderzoek ZUURKOOL", 2021/00362/DOC-CY, 04-02-2021