Reverse Engineering ARM based Mirai Botnet

Published: 2025-02-14 · Archived: 2026-04-05 13:55:22 UTC

Sha256: 29b78bb68ae1a4a1463e28775c00d66b70c848964803b20a91c068ffc10a5d0c Dive into the fascinating world of reverse engineering an ARM-based Mirai Botnet in this detailed walkthrough! In this video, I unpack and analyze a real malware sample—from understanding UPX packing techniques to dissecting its ARM-based syscall (SVC) instructions, persistence strategies, and more. If you've ever wondered how attackers transform exposed IoT devices into powerful botnets, this is the perfect deep-dive for you. Looking to take your cybersecurity expertise to the next level? Check out TrainSec and explore the Knowledge Library—an ever-growing collection of in-depth resources, courses, and community discussions designed to help security pros excel in reverse engineering, malware analysis, incident response, and more. Stay ahead of cyber threats, master new techniques, and join a community committed to excellence in cybersecurity. Subscribe, like, and keep learning! Key Topics Covered:

- UPX packing & unpacking
- ARM-based syscall (SVC) insights
- Persistence mechanisms (cron jobs & hidden files)
- Analysis of network communication (GET & POST requests)

Resources & Links:

- TrainSec courses: https://TrainSec.net
- Follow me on X (Twitter) for more security insights.

Enjoy the video, and continue to push the boundaries of what's possible in the cybersecurity field!
