Aviv Nataf

Security Researcher | Android Malware Reverse Engineering
nataf12386@gmail.com ·https://github.com/an1604 ·https://www.linkedin.com/in/aviv-nataf-757aa1247

Summary

I'm an Android malware researcher and tech lead. Day to day I take apart banking trojans, spyware, droppers and toll-fraud apps, including Flutter, Unity/il2cpp and React Native targets, and turn the results into IOCs, signatures and YARA rules. I also build the tooling around that work: a dynamic-analysis orchestrator with AI triage, deobfuscators, and detection automation. I came to security from a B.Sc. in Computer Science with a strong Python and ML background, and I mentor other researchers and run onboarding for new ones.

Experience

Android Malware Research Tech Lead
Alice (formerly ActiveFence) · Israel
Dec 2025 – Present

- Promoted to Tech Lead on research performance; mentor researchers across the malware research department.
- Own the onboarding program for new malware researchers and run regular department-wide technical sessions.
- Built a Python orchestrator that spins up a fresh dynamic-analysis environment per APK, with automatic execution, traffic and screenshot capture, and AI-assisted triage.
- Shipped two deobfuscators and scaled detection across multiple malware campaigns through automation and signatures.

Android Malware Researcher
Alice (formerly ActiveFence) · Israel
Jul 2025 – Dec 2025

- Reverse-engineered banking trojans, spyware, droppers, backdoors, toll-fraud and riskware with JADX, Ghidra, Frida and radare2, accelerating analysis with AI agents.
- Analysed cross-platform malware (Flutter, Unity/il2cpp, React Native/Hermes); defeated packers, string and file encryption, anti-debugging and native code.
- Analysed C2 traffic and produced IOC reports, detection signatures and YARA rules.

Software Engineer (Student Position)
Jit Security · Tel Aviv
Feb 2025 – Mar 2025

- Built Dockerized security applications and CI/CD pipelines deploying to AWS ECR.
- Wrote test-driven Python for security scanners and integrated scanning into customer CI workflows.

Programming Instructor
Sunspark College · Israel
2022 – 2024

- Taught Python, Java and Visual Basic to classes of 20 to 30 students.

Intern
Colman Dev Club · Rishon LeZion
2022 – 2023

- Built web projects with a student development team.

Education

B.Sc. Computer Science, The College of Management (Colman), Rishon LeZion(Mar 2022 – Mar 2025)

Selected projects

Deceptify
AI social-engineering simulator built as my degree final project: deepfake and voice-clone content plus a RAG agent that runs simulated attacks over Zoom and Telegram, to train organisations against modern phishing.
Python Flask PyTorch Hugging Face RAG
For education and authorised testing only.
Source on GitHub (https://github.com/an1604/Deceptify)

WebGoat OWASP Top 10 Solutions
Solutions and write-ups for the OWASP Top 10 lessons in WebGoat, with proof of each exploit.
OWASP Web security
Source on GitHub (https://github.com/an1604/WebGoat-Solutions-)

The Office
Autonomous dating-app assistant on an Android emulator (adb + uiautomator2), with an ML + LLM profile-scoring pipeline and a Telegram human-in-the-loop bot.
Python asyncio Android emulator uiautomator2 scikit-learn LangChain PostgreSQL pgvector aiogram
Private project

htb-sh
Pentest CLI generating ready-to-run scripts, plus local labs reproducing HTB AI Red Teamer exercises: garak scans, LLMmap fingerprinting and a prompt-injection defense evaluator.
Python YAML CLI garak Ollama
The AI red-team labs run locally and are not yet in the public repository.
Source on GitHub (https://github.com/an1604/htb-sh)

JoBot
Multi-agent job-search automation across LinkedIn, Glassdoor, Drushim and Logon, shipped as a hardened native build with licensing, per-module encryption, obfuscation and tamper detection.
Python Flask LangChain Playwright Cython Docker Sentry
The hardened build is private; the repository shows the early version.
Source on GitHub (https://github.com/an1604/JoBot)

GitLeaksController
Python wrapper that runs Gitleaks locally or in Docker and returns structured secret-scanning results.
Python Gitleaks Docker
Source on GitHub (https://github.com/an1604/GitLeaksController)

DevSecOps CI/CD with GitLab
GitLab pipeline that builds and scans WebGoat and reports findings to DefectDojo.
GitLab CI Docker DefectDojo
Source on GitHub (https://github.com/an1604/CI-CD-pipeline-gitlab)

ANAC 2024 Negotiation Agent
Automated negotiation agent strategies researched and implemented for the ANAC 2024 competition.
Python
Source on GitHub (https://github.com/an1604/ANAC)

Skills

Reverse engineering: IDA Pro, Ghidra, JADX, Frida, frida-trace, radare2, apktool, Burp Suite, Kali Linux, APK/DEX and native .so analysis, Unpacking and deobfuscation, Dynamic instrumentation
ML and AI: PyTorch, scikit-learn, Hugging Face, LangChain, NumPy, Pandas, pgvector, OpenAI, Anthropic and Ollama APIs, Fine-tuning, RAG, Multimodal LLMs, Clustering
Languages: Python, Java, C, C++, C#, JavaScript
Automation and infrastructure: Playwright, Selenium, Docker, CI/CD, Git, GitHub, PostgreSQL, MongoDB, SQL, Redis, Node.js, Flask

Achievements and certifications

- Oracle & Colman Hackathon, 3rd place — Data science and big data on the cloud for agriculture.
- ANAC 2024 — Researched and implemented negotiation agent strategies in Python for the Automated Negotiating Agents Competition.
- Cybersecurity and Ethical Hacking — Udemy
- OWASP Top 10 (WebGoat assignments) — Hands-on web security lessons
- Deep Learning — Udemy
- Machine Learning — Udemy

Languages

English (fluent), Hebrew (proficient)