Vitalii Zaiats

Security Engineer • Reverse Engineering & Threat Intelligence

vizhakivskiy@gmail.com • Ukraine • GitHub • blog

Summary

Security engineer working at the seam of network fingerprinting, Android and native malware reverse engineering, and threat intelligence. I build tooling and detection that read the layers an attacker can't fake — the TCP/IP stack, the TLS handshake, the native code inside an app — and I disclose what I find responsibly. Independent malware research was recognized by NCSC-NL, the Dutch national CERT.

Skills

Languages: Go, Python, TypeScript, C / C++
Reverse engineering: Android APK static analysis, ELF / Go binary analysis, custom binary-protocol reconstruction, mitmproxy traffic analysis
Network fingerprinting: TCP/IP stack, JA3 / JA4 (TLS), HTTP/2 & HTTP/3, STUN / WebRTC leak detection, SOCKS5 & proxy internals, BitTorrent DHT
Detection & intelligence: Suricata / Snort signatures, IOC development, residential-proxy & botnet detection
Backend & systems: async Python (FastAPI), gRPC control planes, high-throughput SOCKS5 data planes, traffic metering & distributed rate limiting, PostgreSQL, Redis
AI / automation: LLM intent classification & reply automation, webhook data pipelines
Infrastructure: Linux, Docker, systemd, raw sockets (AF_PACKET / CAP_NET_RAW), Cloudflare, GeoIP

Experience

Software Engineer 2020 – Present
VergelijkDirect (vergelijkdirect.com) *Netherlands — remote*

- Built an AI customer-support bot for WhatsApp / Trengo: a webhook pipeline capturing ~24K messages across ~3.3K conversations, with LLM intent triage, debounced auto-replies, and clean human handoff.
- Turned real support history into a labelled intent / flow dataset (~8.6K turns) to drive the automation; handled assigned tickets and internal tooling across the platform's PHP / Laravel and Python services.

Selected Research & Projects

Residential-proxy botnet — discovery, reverse engineering & disclosure 2026
Independent research

- Reverse-engineered an Android residential-proxy malware family (Go native library) and its custom multiplexing C2 protocol from a single consented device sample; confirmed the live infrastructure end to end.
- Packaged IOCs and Suricata detection into a technical report submitted to Europol EC3 and national CERTs; the operation (~17M devices, per press) was subsequently taken down. Recognized with an NCSC-NL challenge coin.

apkscan — static APK triage pipeline 2026
Open source

- Batch-triages cracked APKs for bundled proxy / malware SDKs via manifest shape, signing-certificate clustering, and native-code / JNI analysis — fully static, samples are never executed.

Multi-layer network-fingerprinting stack 2025 – 2026
Open source

- Server-side capture fusing TCP/IP, TLS (JA3 / JA4), HTTP/2 and HTTP/3 fingerprints into one record per request; used to separate residential-proxy and automated traffic from real users.

Coordinated disclosure — IoT devices resold as proxies 2026
Independent research

- Passively fingerprinted compromised CCTV / IoT devices being sold as residential proxy exit nodes and disclosed them to NCSC-NL — without ever accessing the devices.

Education

B.Sc. Computer Science 2019 – 2023
Lviv Polytechnic National University *Lviv, Ukraine*