

VOJTĚCH HRON

Offensive Security

E-mail: vojtech.hron.22@proton.me

Blog: vojtechhron.dev

GitHub: github.com/n00bDebugger-git

LinkedIn: linkedin.com/in/vojtech-hron-688457419

PROFILE

Cybersecurity student focused on red teaming and exploit development, CRYPTO holder. I find and report vulnerabilities in production devices, analyze real-world malware samples, and build the tools I need myself. In parallel I worked as a Python developer on embedded AI.

EXPERIENCE

Python Developer, embedded AI (solo) Sep 2025 – Sep 2026

- Drone development on a Pixhawk flight controller, sole developer on the project
- Deployment on Jetson Nano, person detection and SLAM

Self-hosted infrastructure (homelab) 2023 – present

- Raspberry Pi server exposed via Cloudflare Tunnel with no open ports, running a Tor onion service in parallel
- Encrypted off-site backups, scripted deployment, operation without IP address logging
- Since 2026 this infrastructure hosts vojtechhron.dev, where I publish my research

Freelance web development occasional

- Custom and WordPress websites for clients
- Working to a brief, a deadline, and a non-technical client

VULNERABILITY RESEARCH

ZTE ZXHN H267A, unauthenticated admin password disclosure Jul 2026

- Improper use of encryption in the configuration interface of an O2 ISP-provided router
- The recovered admin password gives an attacker full access to the router's admin panel
- Handled through responsible disclosure, not public yet, so no details here

D-Link DIR-825AC G1A, unauthenticated path traversal May 2026

- The web server's /concat endpoint allows reading arbitrary files on the system, including /etc/passwd and device configuration
- Root cause identified by reverse-engineering the anweb binary (MIPS)
- Published advisory with a technical breakdown and reproduction steps
vojtechhron.dev/en/article/unauthenticated-path-traversal-dir825ac

MALWARE ANALYSIS

Psyduck, PowerShell RAT Jun 2026

- Static and dynamic analysis of a sample from Malware Bazaar
- Reverse-engineered the code and mapped the techniques used
vojtechhron.dev/en/article/psyduck

Fake Cloudflare verification, macOS infostealer Apr 2026

- Campaign delivering an infostealer through a spoofed verification page
- Analysis of the captured sample and its execution chain
vojtechhron.dev/en/article/cloudflare-malware

RED TEAM

Living off the Land: LOLBAS, LOLDrivers, GTF0Bins Jul 2026

- Techniques abusing legitimate system binaries and drivers, with working PoCs
 - Written from a purple team perspective, with attention to detectability
- vojtechhron.dev/en/article/living-off-the-land

TOOLS BUILT

PERE, PE Risk Engine (Python, open source) May 2026

- CLI tool for static analysis of EXE and DLL files across Windows directories
 - Scores binaries by imports, digital signature, PE structure and entropy, and surfaces the suspicious ones first
- github.com/n00bDebugger-git/PERE

SKILLS

Languages: Python (primary), C++ (basics), C (learning)

Environment: Linux as daily driver since 2022

Areas: reverse engineering, PE format analysis, static and dynamic malware analysis, vulnerability research, red team TTPs, responsible disclosure

Tools: Nmap, Cobalt Strike, Gobuster, Ghidra

CERTIFICATIONS

Red Team Ops (CRT0), Zero-Point Security Aug 2026

EDUCATION

Secondary School of Communications and Informatics, Tábor expected 2029

- Information Technology programme (18-20-M/01)

LANGUAGES

Czech: native

English: B2 (certified at B1)

German: A2

INTERESTS

Guitar, reading, chess.