VOJTĚCH HRON

Ofenzivní bezpečnost

E-mail: vojtech.hron.22@proton.me
Blog: vojtechhron.dev
GitHub: github.com/n00bDebugger-git
LinkedIn: linkedin.com/in/vojtech-hron-688457419

PROFIL

Student kyberbezpečnosti zaměřený na red teaming a vývoj exploitů, držitel CRTO. Hledám a nahlašuji zranitelnosti v produkčních zařízeních, analyzuji reálné vzorky malwaru a chybějící nástroje si píšu sám. Souběžně jsem pracoval jako Python vývojář na embedded AI.

PRAXE

Python vývojář, embedded AI (solo) 09/2025 – 09/2026

- Vývoj dronu na řídicí jednotce Pixhawk, jediný vývojář projektu
- Nasazení na Jetson Nano, detekce osob a SLAM

Správa vlastní infrastruktury (homelab) 2023 – současnost

- Server na Raspberry Pi vystavený přes Cloudflare Tunnel bez otevřených portů, souběžně provozovaná Tor onion služba
- Šifrované zálohy mimo server, skriptované nasazování, provoz bez logování IP adres
- Od roku 2026 na této infrastruktuře hostuji web vojtechhron.dev, na kterém publikuji svůj výzkum

Tvorba webů na zakázku příležitostně

- Weby na míru a ve WordPressu pro klienty
- Práce se zadáním, termínem a netechnickým zadavatelem

VÝZKUM ZRANITELNOSTÍ

ZTE ZXHN H267A, únik administrátorského hesla bez autentizace 07/2026

- Chybné použití šifrování v konfiguračním rozhraní routeru od poskytovatele O2
- Získané administrátorské heslo umožňuje útočníkovi plný přístup do administrátorského panelu routeru
- Řešeno formou responsible disclosure, zatím není veřejné, proto neuvádím detaily

D-Link DIR-825AC G1A, path traversal bez autentizace 05/2026

- Endpoint /concat webového serveru umožňuje číst libovolné soubory v systému, včetně /etc/passwd a konfigurace zařízení
- Příčinu jsem dohledal reverzním inženýrstvím binárky anweb (MIPS)
- Publikováno advisory s technickým rozborem a postupem reprodukce
  vojtechhron.dev/cs/article/unauthenticated-path-traversal-dir825ac

ANALÝZA MALWARU

Psyduck, PowerShell RAT 06/2026

- Statická i dynamická analýza vzorku z Malware Bazaar
- Reverzní inženýrství kódu a mapování použitých technik
  vojtechhron.dev/cs/article/psyduck

Falešné Cloudflare ověření, macOS infostealer 04/2026

- Kampaň doručující infostealer přes podvrženou ověřovací stránku
- Analýza zachyceného vzorku a řetězce jeho spuštění
  vojtechhron.dev/cs/article/cloudflare-malware

RED TEAM

Living off the Land: LOLBAS, LOLDrivers, GTFOBins 07/2026

- Techniky zneužívající legitimní systémové binárky a ovladače, doplněné funkčními PoC
- Zpracováno z purple team pohledu, s ohledem na detekovatelnost
  vojtechhron.dev/cs/article/living-off-the-land

VLASTNÍ NÁSTROJE

PERE, PE Risk Engine (Python, open source) 05/2026

- CLI nástroj pro statickou analýzu EXE a DLL v adresářích Windows
- Skóruje binárky podle importů, digitálního podpisu, struktury PE a entropie a řadí podezřelé nahoru
  github.com/n00bDebugger-git/PERE

DOVEDNOSTI

Jazyky: Python (hlavní), C++ (základy), C (učím se)

Prostředí: Linux jako denní systém od roku 2022

Oblasti: reverzní inženýrství, analýza PE formátu, statická i dynamická analýza malwaru, výzkum zranitelností, red team TTPs, responsible disclosure

Nástroje: Nmap, Cobalt Strike, Gobuster, Ghidra

CERTIFIKACE

Red Team Ops (CRTO), Zero-Point Security 08/2026

VZDĚLÁNÍ

Střední škola spojů a informatiky, Tábor očekávané ukončení 2029

- Obor Informační technologie (18-20-M/01)

JAZYKY

Čeština: rodilý mluvčí

Angličtina: B2 (certifikováno na úrovni B1)

Němčina: A2

ZÁJMY

Hra na kytaru, čtení, šachy.