🔒 Security Scan — 2026-06-11 21:58

Aanleiding: Jamals verzoek "check alle bestanden op open tokens/API's in plaintext".
Scope: ~/.claude, ~/jamal-geheugen, ~/haartips-photo-gen, ~/styleme, ~/Downloads/Claude-Werk, ~/telegram-bot + poorten/processen/permissies.

✅ Gevonden & DIRECT GEFIXT

1. **Anthropic API-key (sk-ant-…) plaintext in Obsidian-plugin** `.obsidian/plugins/smart-connections/data.json` — stond bovendien in de PRIVATE GitHub-repo `haarvisie-brain-vault`. → Key uit het bestand verwijderd, gecommit en gepusht. ⚠ Key staat nog in git-HISTORIE; advies: key roteren op console.anthropic.com (en evt. BFG-historie-purge).
2. **Telegram-bottoken plaintext in** `~/.claude/scripts/health-check.py` → gepatcht naar Keychain-lookup (syntax geverifieerd).
3. **Telegram-bottoken in 2 permission-regels** in `~/.claude/settings.local.json` → regels verwijderd (JSON gevalideerd).
4. **Twee vergeten** `python -m http.server` **processen** op poort 8898/8899, luisterend op ALLE interfaces, serveerden ~/ergodirect en ~/Downloads/Claude-Werk/ergodirect-social aan het hele LAN zonder auth → gestopt.
5. `~/styleme/.env.local.backup.20260520` — overbodige kopie met Stripe SECRET key, Anthropic, Gemini, Pexels keys → verwijderd. (Pexels-key eerst veiliggesteld in Keychain.)
6. *(eerder vanavond)* **Tavily API-key plaintext in settings.json** → Keychain + wrapper-script.

⚠ Aandacht (bewuste keuzes / laag risico)

- **FileVault staat UIT** — schijf onversleuteld. Bij diefstal van de Mac Mini is alles leesbaar. Advies: aanzetten (Systeeminstellingen → Privacy & beveiliging). Jamals keuze.
- `~/styleme/.env.local` bevat live keys (o.a. Stripe secret) — is ge-gitignored en alleen lokaal; normaal voor dev, maar weet dat het er staat.
- **Mnemosyne-brug (poort 8744)** luistert op alle interfaces — bewust (MacBook/iMac verbinden), token-beveiligd. Firewall door Conductor geregeld.

- `~/.claude/channels/telegram/.env` bevat het bottoken — standaard-opslag van de Telegram-plugin, permissies 600 (alleen jasa). Acceptabel.
- Supabase-key in `supabase-keepalive.sh` is de **anon**-rol (publiek bedoeld) — laag risico, netjes zou Keychain zijn.
- styleme build-output (`.next/`) bevat de Supabase **anon**-key — by design (NEXT_PUBLIC), geen lek.

✳ OK

- SSH: key-only, gehard op 10 juni (Conductor).
- Keychain: 114 items, secrets-discipline grotendeels nageleefd.
- Obsidian-plugin-treffers in `main.js` = minified code, vals alarm.
- Browser Bridge (9223), Ollama (11434), node-services: alleen localhost.

✳ Stats

- Plaintext secrets gevonden: 6 locaties → alle 6 gefixt
- Open verdachte poorten: 2 → gestopt
- Keychain items: 114 | FileVault: UIT (advies: aan)

Vervolgacties (voor Jamal)

1. sk-ant-key van de Obsidian-plugin roteren op console.anthropic.com (en nieuwe alléén in Keychain/plugin, niet committen).
2. Overwegen: Telegram-bottoken roteren via BotFather (exposure was alleen lokaal — optioneel).
3. FileVault aanzetten.
4. Optioneel: BFG-purge van de vault-historie.