Thesara VPS – Incident Response zapisnik (miner kit /var/tmp)

> **Svrha dokumenta:** sažeti što je pronađeno i zaključeno, koje su postavke/pretpostavke, gdje su dokazi spremljeni, te ostaviti "starter" komande i checkliste da se ovo može nastaviti bilo kada bez ponovnog kopanja od nule.

Kontekst okruženja

- **Server:** `vps-thesaraspace-plusvps-com`
- **Aplikacija:** Thesara
- **Repo/putanja:** `/srv/thesara/app`
- **API app:** `/srv/thesara/app/apps/api`
- **WEB app:** `/srv/thesara/app/apps/web`
- **Domena:** `thesara.space`
- **Proxy:** `nginx/1.24.0 (Ubuntu)`
- **Servisi (systemd):**
- `thesara-api.service` (Node) → sluša na `:8788`
- `thesara-web.service` (Next.js) → sluša na `127.0.0.1:3000`
- **Vrijeme / TZ:** CET (+01)

1) Primarni incident: miner "watcher" kit u `/var/tmp`

Pronađeni fajlovi (original lokacija)

U `/var/tmp` su pronađeni: - `watcher.js` - `config.js` - `proc.js` - `utils.js` - `network.js`

Svi su bili owner `amir:amir` i timestamp oko **2025-12-18 06:38–06:39**.

Sadržaj / namjena (iz pregleda fajlova)

- `watcher.js` je beskonačna petlja koja provjerava status procesa i starta ga.
- `config.js` eksplicitno referencira:
- `xmrig-6.24.0`
- URL: `https://github.com/xmrig/xmrig/releases/download/v6.24.0/xmrig-6.24.0-linux-static-x64.tar.gz`
- pool: `pool.hashvault.pro:443`
- wallet ID: `8556M2fMqE8Dg1U3pERP9rJ64jaa6MMha5SY5ovWQ7XiYjxdKquPQ7Z4afpEeXUtfJVBLGvLncGxtKMugv61S9nFGMHNA`
- `--donate-level 0`
- `proc.js` koristi `ps`, `pkill -9`, i `spawn(..., { detached: true })`.
- `network.js` radi `https.get` download uz redirect handling.

Zaključak: ovo je standardni crypto-miner loader/watchdog kit (XMRig + pool).

2) Quarantine i integritet dokaza

Quarantine lokacija

- Kreirano: `/root/ioc-quarantine`
- Kopije:
- `/root/ioc-quarantine/var-tmp/{watcher.js,config.js,proc.js,utils.js,network.js}`

SHA256 hash-evi (dokaz integriteta)

- `network.js` → `5d0754450ec088fad437942e49bf73654137f38bb8491b20f49d286fae30a83c`
- `config.js` → `656018c0c1a7d0542677a88bba272f390bb41ad18697387a65855b4f1d36275b`
- `proc.js` → `67b732f0426f7ee8c3507cc47a6357a9f7c07aac858296d44032aa72aefcfa64`
- `utils.js` → `75e24069d6f103b7efc580cfaaa0d4c8be219397beececbf277e9a3719d3d10c`
- `watcher.js` → `e399b20bc38a7143d76d0d37ddb96242a324e824d128b95cc3c401e8b1a516a8`

3) Trenutno stanje procesa i mreže

- Provjereno: nema `xmrig` procesa (IOC process check)
- Provjereno: nema tipičnih pool konekcija (`:3333/:4444/:5555` itd.)

4) Trajnost (persistence) – nalazi

Cron i systemd timers

- `crontab` za root i amir: **prazno**
- `/etc/cron.*`: standardne sistemske stvari (certbot, sysstat, logrotate, dpkg backup, ...)
- `systemctl list-timers`: standardni timers (sysstat, logrotate, certbot, ...)

rc.local

- `/etc/rc.local` ne postoji.

Systemd / user systemd

- Pretrage po IOC stringovima (watcher/xmrig/hashvault/c3pool/...) kroz `/etc/systemd`, `/lib/systemd`, `/usr/lib/systemd` nisu našle persistence reference.

Zaključak: nema jasnog persistence mehanizma uočljivog kroz cron/timers/systemd profile.

5) Aplikacijski servisni problem koji je usput riješen (Prisma)

Simptom

API failao na: - `Error: Cannot find module '.prisma/client/default'`

Root cause (najvjerojatnije)

U PNPM monorepu, runtime nije mogao resolvati prisma artefakte iz očekivane lokacije zbog node module resolucije iz `apps/api/dist`.

Fix koji je primijenjen

U `thesara-api.service` dodano: - `Environment=NODE_PATH=/srv/thesara/app/node_modules`

Nakon toga: - `thesara-api` se diže i sluša na `0.0.0.0:8788` - Health endpoint radi: `https://thesara.space/api/health` → 200

6) WEB servis status

- `thesara-web` (Next.js) radi na `127.0.0.1:3000`
- `https://thesara.space/` vraća 200

7) SSH hardening i autentikacija

Konfiguracija (efektivno)

`sshd -T` pokazuje: - `permitrootlogin no` - `passwordauthentication no` - `pubkeyauthentication yes`

Problem koji je uočen u fajlovima

- `/etc/ssh/sshd_config` je imao `PermitRootLogin yes`, ali override u `sshd_config.d/*` je rezultirao efektivno `no`.

Zaključak: brute-force preko password SSH-a nije vjerojatni vektor.

8) Logovi: što je viđeno oko 06:38

auth.log

Pretraga `2025-12-18T06:3|06:4` nije dala događaje (osim kasnijih `sudo` provjera u 15:42).

Nginx access log (ključni trag)

U intervalu **06:37–06:39** pojavio se IP: - `121.196.157.221`

I radi **seriju POST zahtjeva na** `/` (root), sa statusom **303**, s različitim user-agentima (Linux Chrome/118, Windows Chrome/120), referrer `https://thesara.space/`.

Primjeri: - `06:37:47` POST / → 303 - `06:38:15` POST / → 303 - više POST-ova do `06:39:24`

U istom periodu: - UptimeRobot HEAD / (normalno) - Googlebot GET / (normalno)

Zaključak: postoji jaka vremenska korelacija između: - `POST /` burst s IP `121.196.157.221` - nastanka miner koda u `/var/tmp` oko **06:38**

To sugerira vektor kroz **web aplikaciju / Next.js route / middleware / server action / custom handler** (ili neku backend rutu koja se mapira na `/` i radi redirect), a ne kroz SSH.

9) Dodatni artefakti i "noise"

/srv/thesara/storage

- `rg` s vrlo širokim patternom davao puno "false positive" (npr. riječ `match` u node_modules).
- Kada je korišten striktni IOC pattern + exclude node_modules + exclude sourcemap:
- `rg` je vratio **0** hitova.

Zaključak: storage/bundle sadržaj izgleda kao normalan build/output (barem po strikt IOC kriterijima).

10) Glavna radna hipoteza (trenutno)

1) Netko (ili bot) je pogodio endpoint (ili slabost) na web aplikaciji (vjerojatno `/` POST flow). 2) Eksploatacija je dovela do izvršenja koda pod korisnikom `amir` (jer su fajlovi owner `amir`). 3) Dropan je miner kit u `/var/tmp` (watcher/config/proc/utils/network), ali binary nije nužno uspio biti downloadan ili je obrisan. 4) Ne vidimo persistence kroz cron/systemd, niti aktivan mining proces sada.

Bitno: činjenica da je owner `amir` ne znači da je `amir` osobno pokrenuo to — može biti da servis/web runtime radi kao `amir`.

"Starter" komande i postavke (za nastavak bilo kada)

A) Brzi status servisa i portova

```
sudo systemctl status thesara-api --no-pager -l | head -n 80
sudo systemctl status thesara-web --no-pager -l | head -n 80
sudo ss -ltnp | rg -n ':8788|:3000|node'
```

```
curl -sS -I https://thesara.space/api/health | head -n 20
curl -sS -I https://thesara.space/ | head -n 20
```

B) IOC pretrage (strogo, bez node_modules i map)

```
PAT_STRICT='xmrig|kdevtmpfsi|kinsing|/var/tmp/\.font|/tmp/runnv|alive\.sh|
lived\.sh|pool\.hashvault|hashvault\.pro|c3pool|moneroocean|cryptonight|/tmp/
\.XIN-unix|/var/tmp/xmrig'

sudo rg -n -S --no-messages
  -g'!**/node_modules/**' -g'!**/*.map'
  "$PAT_STRICT" /srv /etc /home /root 2>/dev/null | head -n 200
```

C) /var/tmp provjera

```
sudo find /var/tmp -maxdepth 1 -type f -printf '%M %u:%g %s %TY-%Tm-%Td %TH:%TM
%f\n' | sort
stat -c '%a %A %U:%G %n' /var/tmp
```

D) Nginx log fokus (incident window)

```
sudo sh -lc "zgrep -h '18/Dec/2025:06:3' /var/log/nginx/access.log* 2>/dev/null
| tail -n 200"
sudo sh -lc "zgrep -h '18/Dec/2025:06:4' /var/log/nginx/access.log* 2>/dev/null
| tail -n 200"

sudo sh -lc "zgrep -h '2025/12/18 06:3|2025/12/18 06:4' /var/log/nginx/
error.log* 2>/dev/null | tail -n 200"
```

E) Auth/SSH (format je ISO)

```
sudo sh -lc "zgrep -h -n '2025-12-18T06:3|2025-12-18T06:4' /var/log/auth.log*
2>/dev/null | tail -n 200"

sudo sh -lc "zgrep -h -n 'Accepted |Failed |Invalid user' /var/log/auth.log* 2>/
dev/null | tail -n 200"

last -ai | head -n 80
sudo lastlog | rg -n 'amir|root' || true
```

Otvorena pitanja

1) **Koji dio aplikacije prima** `POST /` **i vraća 303?** (Next.js action/middleware/custom server?) 2) Je li `POST /` normalan dio aplikacije (login, form submit), ili abnormalan/bot? 3) Je li bilo request body-a ili parametara koji ukazuju na RCE / injection? (potrebni puni access logovi + upstream logovi) 4) Je li `thesara-web` ili `thesara-api` (ili worker) u tom trenutku imao mogućnost pisanja u `/var/tmp` (vjerojatno da) i pozivanja child_process/exec/spawn?

Preporučeni sljedeći koraci (plan)

1) Sigurnosna stabilizacija (odmah)

- Rotirati SSH ključeve za `amir` (i ukloniti stare iz `~/.ssh/authorized_keys`).
- Provjeriti i rotirati sve app tajne koje bi kompromitacija mogla dodirnuti (npr. `.env.production`, Firebase SA JSON, DB creds, Redis, sl.).
- Dodati privremeni `nginx` block za IP `121.196.157.221` dok se ne potvrdi legitimnost.

2) Forenzika vektora (najkritičnije)

- Izvući kompletne linije `POST /` zahtjeva (idealno i request body ako se logira; ako ne, pojačati logging privremeno).
- Usporediti timestampove `06:38` s:
- `journalctl -u thesara-web` i `journalctl -u thesara-api` u tom prozoru
- aplikacijskim logovima (Next/API) ako postoje.
- U kodu tražiti: `child_process`, `execSync`, `spawn`, `eval`, dinamičke `require/import()` i sve što može dropati fajlove.

3) Hardening aplikacijskog runtime-a

- Pokrenuti web i api servise s ograničenjima:
- `NoNewPrivileges=true`
- `PrivateTmp=true` (ako je izvedivo)
- `ProtectSystem=strict` + whitelisting write pathova
- `ReadWritePaths=` samo gdje treba
- `ProtectHome=true`
- Ograničiti outbound egress (barem blokirati mining/pool destinacije) putem firewall-a ili egress policy.

4) Cleanup

- Nakon što su artefakti sigurno u quarantine: obrisati dropane fajlove iz `/var/tmp`.
- Provjeriti permisije `/var/tmp` (treba biti `1777` sticky).

Dodaci: “Known bad” IOC lista

- `xmrig`, `xmrig-6.24.0`, `kal.tar.gz`
- `pool.hashvault.pro` / `hashvault.pro`
- wallet: `8556M2fMqE8Dg1U3pERP9rJ64jaa6MMha5SY5ovWQ7XiYjxdKquPQ7Z4afpEeXUtfJVBLGvLncGxtKMugv61S9nFGMHNA`
- fajlovi: `/var/tmp/watcher.js`, `/var/tmp/config.js`, `/var/tmp/proc.js`, `/var/tmp/utils.js`, `/var/tmp/network.js`