XTQ

Raport tehnic, versiune publică
Generat pe 5 noiembrie 2026

Raport de securitate a rețelei

Răspuns la alerta DIGI Infosec privind IP-ul `188.27.xx.xxx`, categoria `ssh-brute-force / botnet`, eveniment raportat pe `2026-11-02 14:58:40 UTC` (16:58:40 ora României), `src_port 59459`, `dst_ip` gol.

Concluzie: niciun dispozitiv din rețea nu prezintă semne de compromitere. Din internet nu este accesibil niciun port, nici pe IPv4, nici pe IPv6. Niciun dispozitiv pe care îl controlez nu a inițiat conexiuni SSH la ora din raport. Singura componentă care nu poate fi inspectată de client este routerul furnizat de DIGI.

1. Metodă

- **Descoperire LAN** din rețeaua internă (`192.168.1.0/24`): ping sweep, tabelă ARP, nmap (TCP connect și detecție servicii), mDNS.
- **Scanare externă IPv4** dintr-un server din datacenter (în afara rețelei DIGI): toate cele 65.535 de porturi TCP și un set de porturi UDP uzuale.
- **Scanare externă IPv6** dintr-un alt server din datacenter, către adresele IPv6 publice atribuite automat de routerul DIGI.
- **Verificări din interiorul fiecărui dispozitiv**: porturi deschise, conexiuni active, procese, servicii și sarcini programate, chei SSH, log-uri de sistem pentru intervalul raportului, integritatea binarelor.
- **UPnP:** interogare IGD pentru maparea automată a porturilor.

2. Inventarul rețelei

Dispozitiv	Adresă LAN	Sistem	Stare la ora raportului
Router DIGI TP-Link EX520 v1.0	192.168.1.1	Firmware 0.1.0 Build 240723, administrat de DIGI	Pornit
MacBook	192.168.1.130	macOS 27.0.1	Pornit
Laptop (server de lucru)	192.168.1.133	Arch Linux, kernel 7.2.9	Pornit (uptime 12 zile)
iPhone	192.168.1.134	iOS	Pornit
PC Windows	192.168.1.135	Windows 11	**Oprit** (vezi 5.4)
PlayStation 5	adresă link-local	Sistem închis Sony	Consolă de jocuri, nu rulează software terț

Nu există dispozitive IoT (camere, prize smart, electrocasnice conectate). Nu rulează niciun container Docker.

3. Expunere din internet

Test	Rezultat	
IPv4, toate cele 65.535 de porturi TCP	0 porturi deschise. 65.532 filtrate (fără răspuns), 3 închise activ de router (80, 443, 58877). Portul 22 (SSH) nu răspunde.	**Închis**
IPv4, UDP (53, 69, 123, 161, 500, 1900, 4500, 5353)	Niciun răspuns pe niciun port.	**Închis**
IPv6, MacBook (2 adrese) și laptop	Ping blocat. 49 de porturi testate, inclusiv toate porturile pe care ascultă dispozitivele în LAN: 0 deschise.	**Închis**
Port forwarding pe router	Nicio regulă configurată.	**Niciunul**
UPnP IGD	Niciun serviciu UPnP IGD în rețea, deci nicio aplicație nu poate deschide porturi automat.	**Inactiv**

Scanarea externă IPv4 a fost făcută pe IP-ul public actual al aceleiași conexiuni, după schimbarea IP-ului. Configurația routerului este aceeași.

4. Routerul DIGI

Scanarea completă a celor 65.535 de porturi TCP pe partea de LAN a găsit: DNS (53), interfața de administrare (80 și 443), **serviciul TR-069 de administrare la distanță TP-Link (8877)** și un serviciu SSL pe portul 58877. TR-069 este protocolul prin care DIGI administrează și configurează routerul de la distanță. Din internet, portul 8877 nu răspunde, iar 58877 este închis activ.

Serverul DNS raportat este `dnsmasq 2.89`, o versiune din 2023. Versiunea 2.90, lansată în februarie 2024, a corectat vulnerabilități publice: `CVE-2023-50387` (KeyTrap), `CVE-2023-50868` și `CVE-2023-28450`.

> Firmware-ul este administrat de DIGI și nu poate fi actualizat de client. Routerul este singurul echipament din rețea pe care nu îl pot inspecta: este administrat de DIGI prin TR-069, nu oferă acces la procese, nu păstrează log-uri ale conexiunilor de ieșire și nu poate fi înlocuit cu software propriu.

5. Dispozitive

5.1 MacBook

System Integrity Protection	**Activ**
Gatekeeper	**Activ**
FileVault (criptare disc)	**Activ**
XProtect (antimalware Apple)	**Actualizat, v5371**
Server SSH	**Neactiv**
Agenți și servicii de pornire	Doar aplicații cunoscute, instalate de mine (Google, Zoom, Mullvad, Steam, Riot, Synergy, Ollama și utilitare proprii)
Firewall aplicații macOS	**Dezactivat. Fără impact extern: testele IPv4 și IPv6 arată că din internet nu se ajunge la niciun port**

5.2 Laptop (Arch Linux)

Log-uri de sistem 16:50 până la 17:10, 2 noiembrie	**Nicio conexiune SSH, nicio sesiune**
Autentificări SSH din afara LAN-ului (de pe 25 octombrie)	**Niciuna**
Integritatea binarelor sistem (pacman -Qkk)	**Niciun binar modificat**
Conexiuni active	Doar către propriile servere, Cloudflare și Google
Chei SSH autorizate	2 chei, ambele ale mele
VPN WireGuard propriu	3 dispozitive proprii (PC, MacBook, telefon). Singurul care s-a conectat vreodată este PC-ul, din LAN. Portul nu e accesibil din internet
Mașini virtuale de laborator	2 VM-uri de test proprii, rețea NAT prin laptop

5.3 iPhone

Doar porturile standard Apple pentru sincronizare (62078 și 49152). Nu există aplicații SSH automate: SSH este folosit doar manual, din Termius.

5.4 PC Windows

Ultimul eveniment din log-ul de sistem înainte de raport	2 noiembrie, 00:11
Primul eveniment după raport	3 noiembrie, 00:43 (pornire sistem)
Evenimente între 16:50 și 17:10, 2 noiembrie	**0. PC-ul era oprit**
Scanare Microsoft Defender (4 noiembrie)	**Nicio amenințare**
Port 22 / server SSH la ora raportului	**Inexistent**

Singura detecție din istoricul Defender (21 octombrie) este semnalarea propriei modificări de politică făcute de proprietar la dezactivarea protecției în timp real, nu malware.

6. Analiza raportului primit

- Un atac SSH brute force înseamnă mii de încercări. Spre comparație, un server pe care îl administrez primește aproximativ 9.400 de încercări în 24 de ore, de la peste 100 de IP-uri. Raportul conține **o singură conexiune**.
- Portul sursă 59459 este un port efemer obișnuit, alocat de orice sistem de operare pentru orice conexiune de ieșire.
- Câmpul `dst_ip` este gol, așa că evenimentul nu poate fi verificat de nimeni. Tehnicianul DIGI a confirmat telefonic, pe 5 noiembrie, că nici DIGI nu are alte date și că de atunci nu au mai venit alte raportări.
- IP-ul nu apare cu activitate abuzivă pe AbuseIPDB și nici cu servicii expuse pe Shodan.

7. Limitări

Routerul DIGI nu păstrează log-uri ale conexiunilor de ieșire, așa că nimeni, nici clientul, nici DIGI, nu poate reconstitui traficul de pe 2 noiembrie la nivel de pachet. Concluziile se bazează pe starea dispozitivelor, pe log-urile lor și pe testele de expunere. Traficul mașinilor virtuale de laborator nu a fost inspectat separat.

8. Solicitări către DIGI

- Închiderea raportului ca fals pozitiv, cu confirmare scrisă că nu se iau măsuri asupra conexiunii sau a contractului.
- Dacă raportul rămâne deschis: dovezile complete (IP destinație, număr de încercări, log-uri).
- Verificarea routerului EX520 și a firmware-ului său, inclusiv actualizarea dnsmasq, sau înlocuirea echipamentului.

9. Monitorizare de acum înainte

Din 5 noiembrie 2026, laptopul rulează un monitor de conexiuni (Grafana și Loki) care loghează în timp real fiecare conexiune nouă: sursa, destinația, portul, protocolul și programul care a deschis-o. Conexiunile SSH către servere care nu îmi aparțin au un contor separat, care trebuie să stea la 0. Următorul pas este un router MikroTik care va trimite în același sistem log-urile întregii rețele.

În această versiune publică, IP-ul public a fost mascat. Adresele interne din LAN (192.168.1.x) sunt private și nu identifică pe nimeni.