Incident: Unauthorized Device "mk7"

Date Detected: July 21, 2025

Time: 12:16 AM

Alert Type: New Device Detected on Network

Detection Source: GL.iNet Router (main network) + FQGuardBot (alert delivery)

Device Details:

- MAC Address: 00:3F:10:A4:79:B0
- Vendor: Shenzhen GainStrong Technology Co., Ltd.
- IP Address: 192.168.x.x
- Ports Open:
  - 22 (SSH)
  - 53 (DNS)
  - 80 (HTTP)

Response Actions:

- Device was immediately flagged and logged
- Blocked via router MAC filter
- Logged to incident file
- Nmap scan saved for review

Analyst Notes:

MAC vendor indicates a non-recognized IoT device. Spoofing suspected due to lack of user-side identification.

Follow-up scheduled to detect recurrence and enhance MAC/OUI filtering.

Status:

Blocked and removed from network routes by 12:30 AM.