ICS EXPOSURES

ATG Under Attack by Iran

This report follows CNN's 15 May 2026 report that US officials suspect **Iran-linked operators** of breaching internet-facing Automatic Tank Gauges (ATGs) at US gas stations. Censys finds **6,502 ATG services on 6,057 hosts*** still reachable on the public internet today. **Every ATG service indexed in Censys is reachable without authentication**. The protocol has no login. A single unauthenticated `I20100` command returns the station's brand, street address, phone number, and live tank readings on **60.1%** of these services.

** excludes hosts where any service is labeled `HONEYPOT`.*

EXECUTIVE SUMMARY

- **6,502 ATG services** on **6,057 hosts** in 65+ countries, May 2026. Honeypots excluded.
- **3,907 services (60.1%) leak a full `I20100` in-tank inventory**: station brand, name, address, sometimes a phone number, and live volume / ullage / water-bottom readings.
- **United States: 4,224 hosts (70%)**. Puerto Rico is second at 350 hosts, of which **347 sit on a single ISP (COQUI-NET / DATACOM CARIBE)**. Top US ASNs are residential and small-business broadband and cellular ISPs: Verizon Wireless / CELLCO-PART (667), Comcast / CMCS (373), CYBERA Inc. (281), Charter / CHARTER-20115 (241), AT&T (208), UUNET / Verizon Business (171). Comcast and Charter each appear under multiple ASNs in the long tail.
- Notable brands found running ATG: **Shell (602)**, Mobil (184), BP (78), Texaco (68), Puma (52, LatAm), Marathon (47), Exxon (41), Sunoco (37), Gulf (32), Citgo (31), Chevron (23), Valero (23).
- Per CNN (15 May 2026), US officials suspect **Iran-linked operators** behind a recent run of ATG intrusions across US gas stations. Attackers reached devices "*sitting online and unprotected by passwords*" and altered on-display readings. Investigators emphasize they could not change physical fuel levels, but the same access, by protocol design, could let a leak go undetected.

THREAT ACTIVITY

Per CNN (15 May 2026), US officials suspect Iran-linked operators behind recent intrusions against unprotected, internet-facing ATGs at US gas stations. Attackers reached devices "*sitting online and unprotected by passwords*" and altered on-display readings. Physical fuel levels were not changed, but the same access channel would permit masking a real leak.

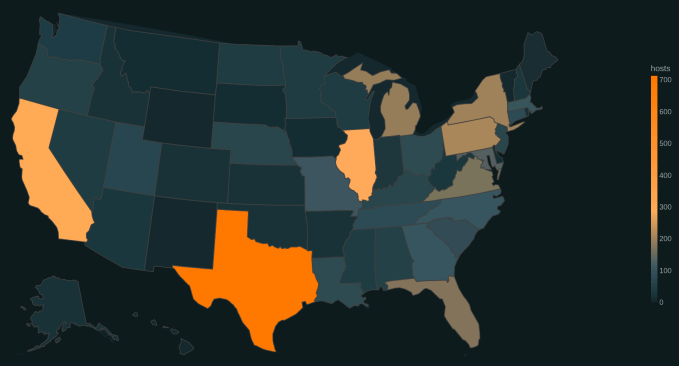
3,907 of those 6,502 exposed services don't just respond. They openly broadcast the station's **brand, street address, and on-site phone number**. For a targeted adversary, the reconnaissance is already done.

WHAT THE PROTOCOL LEAKS

The ATG protocol-level `I20100` response is a printer-formatted in-tank inventory report that begins with the station's brand and street address before the tank table: "*SHELL 135102 / 90 E.HWY 246 / BUELLTON, CA*", "*MOBIL RIO HONDO / Comerío, Puerto Rico*", "*Friendly Shell / Lexington, KY*".

Shell-branded consoles alone account for 602 reachable hosts, more than the next ten major chains in this enumeration combined. Mobil follows at 184, BP at 78, Texaco at 68, Marathon at 47, Exxon at 41.

GEOGRAPHY



US ATG hosts by state. Texas's outsized share partly reflects Verizon Wireless's BGP egress (Euless, TX).

Top US states: Texas (713), California (312), Illinois (287), Pennsylvania (212), New York (199).

Beyond the US: Puerto Rico (350; 347 on COQUI-NET / DATACOM CARIBE), Brazil (273), Australia (175), Uruguay (102), Canada (100), Spain (95).