CameraSwarm: 14,500 cameras taken over, most of them in Ukraine

Over thirty-five days one operator compromised more than fourteen thousand Dahua cameras and intercoms, installed permanent backdoor accounts and sent the images out through Telegram. The firm that found it assesses the access was being built to hand on.

INCIDENT DETAILS · 5WH

Who A single Russian-speaking operator per Hunt.io, with Cyrillic comments in the tooling and staging on a rented Amsterdam server. No state nexus established.
What Covert compromise of 14,530-plus Dahua cameras, intercoms and recorders, with snapshots sent to Telegram and backdoor accounts installed on 1,923 devices.
Where Concentrated in Ukraine, then Russia and other former Soviet networks. Early scanning touched Mexican and Vietnamese ranges.
When 17 June to 22 July 2026; vendor notified 10 Aug, published 18 Aug.
Why Not established. Hunt.io assesses at moderate confidence that the access was built for onward sale.
How Brute-forcing from 12,324 addresses, two 2021 authentication-bypass flaws, and abuse of the maker's cloud relay.

IMPACT

- Privacy: a covert visual surveillance capability over some 14,500 cameras, including door intercoms pointed at people entering buildings.
- Conflict: the heaviest concentration is inside a war zone, though the recovered material shows no military reconnaissance purpose.
- Durability: backdoor accounts survive a password change, so the true remaining compromise is unknowable from outside.
- Onward risk: if built for handover, the end user is unknown and the capability outlives the campaign.

SEQUENCE OF EVENTS

2021 The two authentication-bypass flaws were published
17 Jun-22 Jul 2026 The 35-day campaign
18 Aug 2026 Hunt.io publishes after notifying the vendor

1. Broad scanning narrows to former Soviet networks
2. Brute-forcing from 12,324 source addresses
3. 1,923 devices reached through 2021 flaws; 283 via cloud relay
4. Backdoor accounts make the access permanent
5. Snapshots exfiltrated through Telegram

ASSESSMENT, LESSONS, AND RECOMMENDATIONS

- The concentration in Ukraine is suggestive and is not evidence of purpose.
- Access built for resale outlives the campaign - the backdoors remain for whoever acquires them.
- Persistent accounts defeat the remedy most owners will apply, which is a password change.
- Five-year-old vulnerabilities still working is an estate-ownership failure, not a research gap.