Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

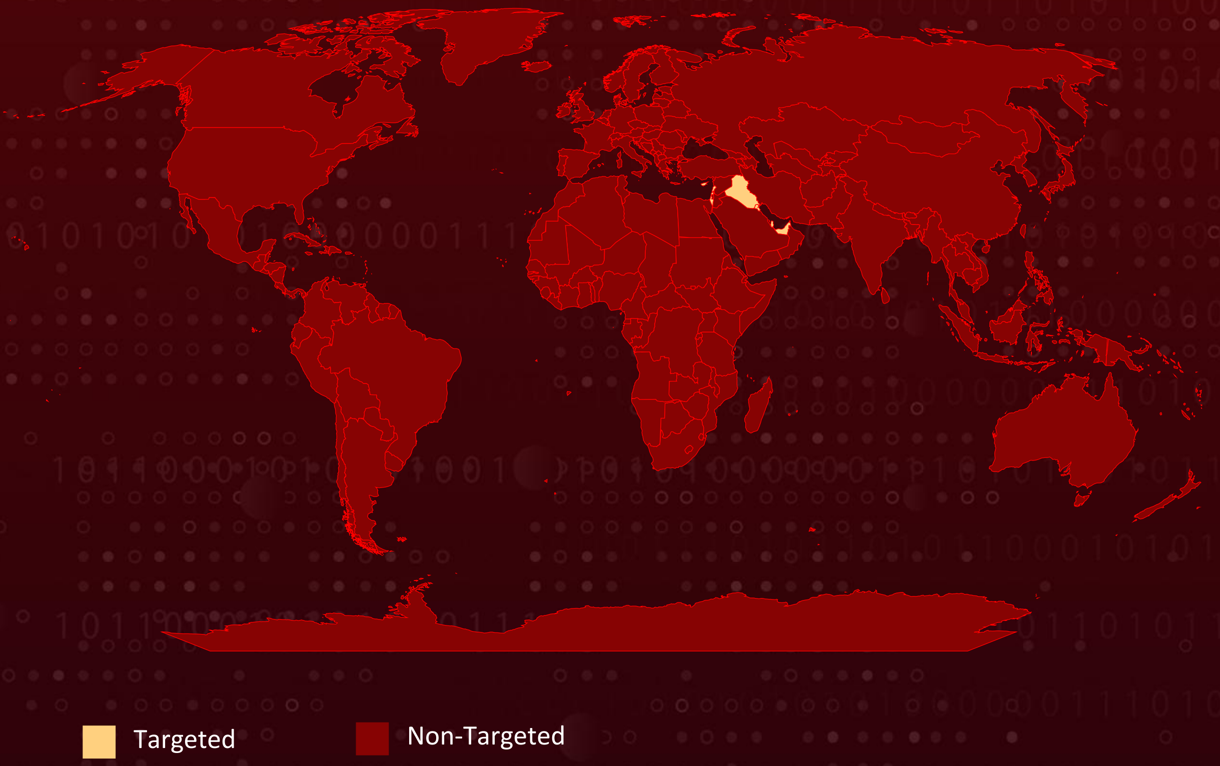
Targeting the Lens: Iranian Cyber Operations Against IP Cameras in the Middle East

Date of Publication	Admiralty Code	TA Number
March 19, 2026	A1	TA2026076

Summary

First Seen: January 14, 2026
Targeted Countries: Israel, Qatar, Bahrain, Kuwait, UAE, Lebanon, Cyprus, Iraq
Targeted Industries: Internet-connected surveillance infrastructure across all sectors
Threat Actor: Multiple Iran-nexus threat actors (infrastructure consistent with IRGC- and MOIS-affiliated operations)
Attack: A significant escalation in cyberattacks since late February 2026, targeting internet-facing IP surveillance cameras across multiple countries in the Middle East, including Israel, Qatar, Bahrain, Kuwait, the United Arab Emirates, Cyprus, and Lebanon. The activity originates from infrastructure attributed to multiple Iran-nexus threat actors and is assessed to be directly linked to physical military operations, specifically for pre-strike reconnaissance, battle damage assessment (BDA), and post-strike target correction during missile campaigns. Earlier, more targeted waves of the same activity were also detected on January 14–15, 2026, coinciding with Iran's temporary airspace closure amid heightened tensions and expectations of a potential U.S. military strike.

Attack Regions



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2017-7921	Hikvision Multiple Products Improper Authentication Vulnerability	Hikvision Multiple Products	✗	✓	✓
CVE-2021-36260	Hikvision Multiple Products Improper Input Validation Vulnerability	Hikvision Multiple Products	✗	✓	✓
CVE-2023-6895	Hikvision Intercom Broadcasting System Command Injection Vulnerability	Hikvision Intercom Broadcasting System	✗	✗	✓
CVE-2025-34067	HIKVISION Integrated Security Management Platform Remote Command Execution Vulnerability	HIKVISION Integrated Security Management Platform	✗	✗	✓
CVE-2021-33044	Dahua IP Camera Authentication Bypass Vulnerability	Dahua IP Camera	✗	✓	✓

Attack Details

#1

Since late February 2026, multiple Iran-nexus threat actors have significantly escalated exploitation attempts against internet-facing IP surveillance cameras across Israel, Qatar, Bahrain, Kuwait, the UAE, Lebanon, and Cyprus, countries also experiencing Iranian-linked missile activity. The attackers operate through layered anonymization infrastructure combining commercial VPN exit nodes (Mullvad, ProtonVPN, Surfshark, NordVPN) with virtual private servers (VPS) to enable rapid IP rotation and complicate attribution. No specific named APT group has been publicly identified; however, infrastructure patterns are consistent with both IRGC and MOIS-affiliated operations.

#2 The campaign exclusively targets two major camera manufacturers, exploiting five vulnerabilities: CVE-2017-7921 (improper authentication), CVE-2021-36260 (command injection enabling unauthenticated RCE), CVE-2023-6895 (OS command injection in intercom systems), CVE-2025-34067 (unauthenticated RCE in integrated security management platform), and CVE-2021-33044 (authentication bypass in a second manufacturer's products). No other camera vendors were targeted. Patches are available for all the five CVEs, but many devices remain unpatched and internet-exposed.

#3 Compromised cameras provide real-time ISR capabilities supporting battle damage assessment, target verification, and strike correction during missile operations. During the June 2025 Israel-Iran conflict, a street camera was reportedly compromised immediately before a ballistic missile struck the site it was monitoring. The current campaign shows exploitation spikes correlating with geopolitical events: January 14–15 (Iran airspace closure and anti-regime protests), January 24 (CENTCOM commander visit to Israel), early February (growing U.S. strike concerns), and the most significant surge beginning February 28 coinciding with Operation Epic Fury, with additional Lebanon-focused activity on March 1.

#4 This consistent correlation between scanning activity and geopolitical escalation reinforces the assessment that tracking exploitation attempts against surveillance infrastructure from attributed threat actor networks can serve as a valuable early warning indicator of potential follow-on kinetic military operations.

Recommendations

Apply Critical Firmware Patches Without Delay: Prioritize patching the five actively exploited CVEs, CVE-2017-7921, CVE-2021-36260, CVE-2023-6895, CVE-2025-34067, and CVE-2021-33044, across all deployed camera and NVR assets. Immediately decommission or replace any end-of-life devices that no longer receive firmware security updates from the manufacturer.

Eliminate Direct Internet Exposure of Surveillance Devices: Remove all direct WAN access, port forwarding, and public-facing configurations from IP cameras and NVRs immediately. Place all surveillance devices behind VPN tunnels or zero-trust access gateways to prevent unauthorized remote access. Conduct an external attack surface audit to identify any unknown or forgotten camera endpoints exposed to the internet.

Enforce Strong Authentication and Credential Hygiene: Change all default, factory-set, and weak passwords on every camera, NVR, and management platform across the environment. Enforce unique, complex credentials per device and disable any anonymous or guest access features. Where supported, enable multi-factor authentication on centralized camera management consoles and administrative interfaces.

Segment and Isolate Surveillance Networks: Deploy all cameras and NVRs on dedicated VLANs with strict access control lists preventing any lateral movement to corporate, IT, or operational technology (OT) networks. Restrict outbound traffic from camera network segments to only required firmware update servers and authorized cloud endpoints. Block all unnecessary protocols and ports, and ensure surveillance traffic cannot reach sensitive internal systems even if a device is compromised.

Implement Behavioral Monitoring and Anomaly Detection: Monitor for repeated authentication failures, brute-force login attempts, and unexpected remote access sessions targeting surveillance devices. Alert on any cameras or NVRs initiating unusual outbound connections, particularly to commercial VPN IP ranges or unfamiliar VPS infrastructure. Prioritize continuous vulnerability scanning, network traffic analysis, and device behavior baselines as the primary detection strategy.

Block Reconnaissance Patterns Matching This Campaign's Infrastructure: The attackers operate through a combination of commercial VPN exit nodes (Mullvad, ProtonVPN, Surfshark, NordVPN) and VPS infrastructure to scan and exploit camera devices. Configure firewall and IDS/IPS rules to flag or block inbound connection attempts from known commercial VPN IP ranges targeting camera ports, particularly port 80, 443, 554 (RTSP), and 37777 (Dahua default). Correlate any detected scanning spikes against these ports with geopolitical developments, as this campaign has demonstrated a clear pattern of intensifying during periods of regional escalation.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1590: Gather Victim Network Information	T1590.005: IP Addresses
	T1592: Gather Victim Host Information	T1592.001: Hardware
Resource Development	T1583: Acquire Infrastructure	T1583.003: Virtual Private Server
	T1588: Obtain Capabilities	T1588.005: Exploits
Initial Access	T1190: Exploit Public-Facing Application	
	T1133: External Remote Services	
Execution	T1059: Command and Scripting Interpreter	
Defense Evasion	T1090: Proxy	T1090.003: Multi-hop Proxy
Collection	T1125: Video Capture	

Patch Links

CVE-2017-7921: http://www.hikvision.com/us/about_10805.html

CVE-2021-36260: https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/

CVE-2023-6895: https://www.hikvision.com/en/support/download/software/

CVE-2025-34067: https://www.hikvision.com/europe/support/cybersecurity/security-advisory/clarification-on-hikvision-software---fastjson-vulnerability--cv/

CVE-2021-33044: https://www.dahuasecurity.com/download-center/firmware

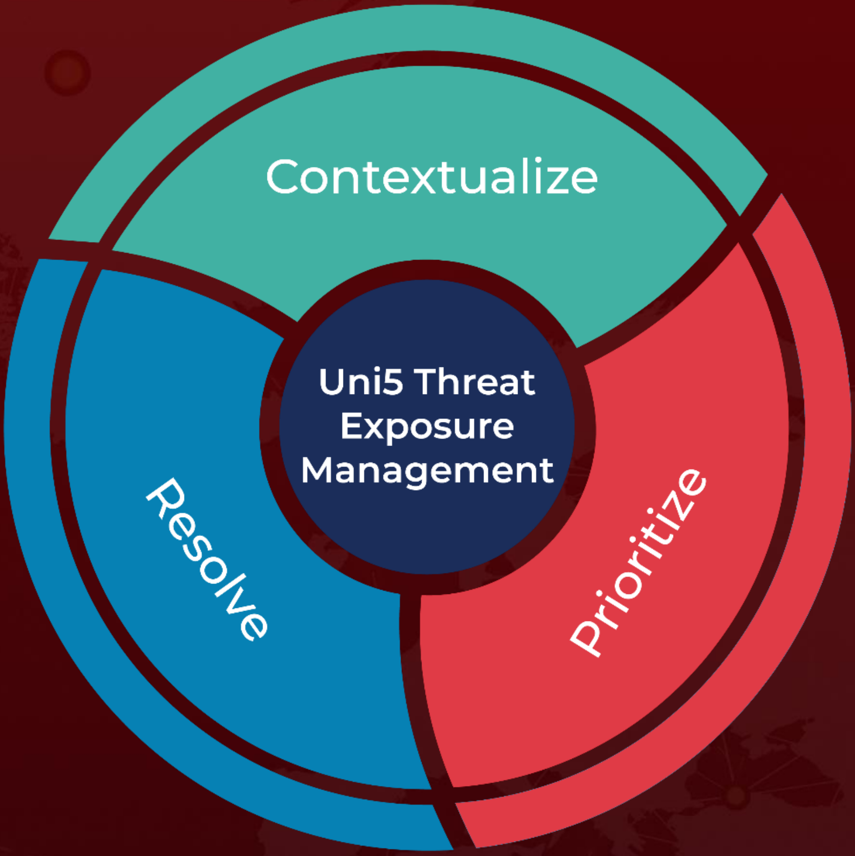
References

https://research.checkpoint.com/2026/interplay-between-iranian-targeting-of-ip-cameras-and-physical-warfare-in-the-middle-east/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 19, 2026 • 04:30 AM

More at www.hivepro.com