INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:35 UTC

Nation-States Are Watching Through Your Cameras: IP Camera Compromise Becomes Standard Wartime Surveillance Tactic

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0114
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Internet-connected IP cameras (multiple vendors; specific models unspecified in source reporting)
Published	2026-03-27
Discovery Source	Rss

Executive Summary

Nation-state adversaries are reported to exploit compromised internet-connected IP cameras to conduct surveillance operations, according to March 2026 threat intelligence reporting. This represents a shift from opportunistic criminal activity to deliberate state-sponsored intelligence collection infrastructure. Organizations with internet-exposed camera systems face nation-state threat exposure and must treat IP cameras as high-value targets requiring enterprise endpoint-level hardening controls.

Technical Analysis

This campaign does not exploit a single disclosed CVE. Based on historical IP camera vulnerability patterns, nation-state actors are likely systematically exploiting endemic weakness classes across multi-vendor IP camera deployments: hardcoded credentials (CWE-798), missing authentication for critical functions (CWE-306), improper authentication (CWE-287), improper access control (CWE-284), and insufficient verification of data authenticity (CWE-494). Attack surface likely includes internet-facing cameras with default or hardcoded credentials, unauthenticated RTSP/HTTP streams, and devices reachable via external remote access services (T1133). Adversaries leverage valid accounts obtained through credential abuse (T1078, T1078.001), exploit public-facing applications (T1190), capture video (T1125), collect network topology data (T1016, T1602), and exfiltrate over standard application-layer protocols (T1071.001). Impair-defenses techniques (T1562.001) may be used to disable logging or alerting on compromised devices. No vendor-issued patch addresses this campaign specifically; remediation requires configuration hardening and network

segmentation across all deployed camera hardware. Source reporting references historical research on Hikvision command injection vulnerabilities and supply-chain IoT weaknesses (CVE-2021-28372) as illustrative of the broader vulnerability class; neither is confirmed as the active exploitation vector in this campaign.

Action Checklist

1. Containment, Immediately audit your camera inventory for internet exposure. Use firewall rules or network ACLs to block direct inbound access to camera management ports (TCP 80, 443, 554 RTSP, 8080, 37777) from any public IP. If cameras must be remotely accessible, place them behind a VPN or zero-trust access gateway. Remove any cameras from DMZ or directly-routed internet segments until hardening is confirmed.
2. Detection, Query firewall and DNS logs for outbound connections from camera IP ranges to non-organizational endpoints, particularly unusual geographies or high-frequency beacon patterns. Check RTSP stream access logs (if your NVR or VMS captures them) for sessions initiated outside business hours or from unrecognized source IPs. Search SIEM for authentication events against camera management interfaces; flag any successful login not tied to a known admin account. Use Shodan or Censys to identify externally visible camera services on your public IP ranges. Example Shodan query: org:"YourOrgName" port:554 OR port:80 OR port:443 OR port:8080 to identify RTSP and HTTP camera services exposed to the internet.
3. Eradication, Change all camera credentials immediately; replace any factory-default or hardcoded passwords with unique, complex credentials stored in a privileged access management system. Disable UPNP on cameras and upstream routers to prevent automatic port exposure. Where firmware updates are available from the manufacturer, apply them. Check vendor security portals (e.g., Hikvision, Dahua, Axis, and any other deployed brands) for relevant patches and hardening guidance. Disable unused services on each device (Telnet, FTP, unnecessary HTTP endpoints). Document each device's firmware version and credential status.
4. Recovery, After hardening, re-scan your external attack surface using Shodan, Censys, or an equivalent tool to confirm no camera management interfaces remain internet-reachable. Validate that NVR/VMS access logs show only authorized sessions post-change. Monitor camera network segments for anomalous outbound traffic for a minimum of 30 days. Confirm firmware versions match the latest available release from each vendor.
5. Post-Incident, This campaign exposes three control gaps: (1) absent asset management for IoT and physical security devices, which are often outside standard IT inventory; (2) no network segmentation between camera infrastructure and corporate networks; (3) no monitoring or alerting on camera network traffic. Address each with formal controls: add IoT/OT devices to asset inventory, implement a dedicated VLAN for physical security systems with deny-all egress except to the NVR, and extend SIEM coverage to include camera network segments. Map these gaps to NIST CSF 2.0 Identify (ID.AM) and Protect (PR.AC, PR.PT) functions for governance tracking.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior leadership, legal counsel, and potentially CISA (via https://www.cisa.gov/report) if forensic evidence confirms an active or historical unauthorized RTSP stream session from a foreign IP geolocation, if camera network traffic analysis reveals persistent outbound beaconing consistent with an implant, or if any camera subnet has layer-2 adjacency to corporate networks containing PII, PHI, or classified information that may trigger breach notification obligations under HIPAA, GDPR, or applicable state law.
Recovery Notes	After completing network isolation and credential rotation, conduct a full external attack surface re-scan using Shodan and Censys scoped to your public IP ranges before returning any camera to operational status — a clean scan result with zero exposed camera management ports is the minimum bar for recovery confirmation. Monitor the dedicated camera VLAN for outbound connections to non-NVR destinations continuously for a minimum of 30 days post-hardening, given that nation-state implants have been documented using low-frequency beaconing designed to survive credential rotations if firmware was not also updated and services were not restarted. Retain all forensic captures (firewall logs, NVR session logs, device config exports, Zeek conn.log and dns.log) for a minimum of 12 months in write-protected storage, as nation-state attribution investigations and potential regulatory inquiries may require historical evidence well beyond the immediate incident window.
Forensic Artifacts	Hikvision ISAPI authentication logs (`GET /ISAPI/System/SecurityManager/Loglist`) and Dahua CGI syslog (`/mnt/mtd/Config/syslog`) — these record every login attempt with source IP, timestamp, and success/failure status, and are the primary artifact for identifying unauthorized administrative access used by nation-state operators to access or reconfigure camera streams | NVR/VMS RTSP session records (Milestone XProtect: `C:\ProgramData\Milestone\XProtect Management Server\Logs\`; Genetec: `C:\Program Files (x86)\Genetec Security Center\Logs\`) showing stream channel, source IP, session start/end time, and duration — nation-state ISR collection sessions typically appear as anomalously long-duration connections from non-local IPs accessing specific camera channels covering high-value physical areas | Firewall NetFlow or connection state logs scoped to camera source IPs with non-RFC1918 destinations — the primary network-layer artifact for detecting compromised cameras acting as implant hosts, showing periodic outbound TCP/UDP sessions on non-RTSP ports that indicate C2 beaconing rather than legitimate NVR streaming | UPnP port mapping table extracted from border router before remediation (`upnpc -l` via miniupnpc, or router admin export) — documents which camera management ports (TCP 37777 for Dahua P2P cloud, TCP 8080 for Hikvision web) were automatically exposed to the public internet by UPnP, establishing the attack surface that nation-state actors exploited for initial access | DNS query logs from the camera network segment (extracted from router, dedicated DNS resolver, or Zeek dns.log on a tap host) filtered for queries originating from camera IP ranges to hostnames not matching NVR, NTP, or vendor update server patterns — nation-state-deployed implants on camera firmware generate DNS lookups to C2 infrastructure that are distinct from the limited, predictable DNS profile of a legitimately operating IP camera

Per-Action IR Details

Containment — Immediately audit your camera inventory for internet exposure. Use firewall rules or network ACLs to block direct inbound access to camera management ports (TCP 80, 443, 554 RTSP, 8080, 37777) from any public IP. If cameras must be remotely accessible, place them behind a VPN or zero-trust access gateway. Remove any cameras from DMZ or directly-routed internet segments until hardening is confirmed.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 12.2 (Establish and Maintain a Secure Network Architecture)

Compensating: On Linux-based perimeter firewalls or the NVR host itself, use iptables to DROP inbound traffic on TCP 80, 443, 554, 8080, and 37777 from 0.0.0.0/0 scoped to camera subnet CIDRs: `iptables -I FORWARD -d /24 -p tcp --dport 554 -j DROP`. On Windows-based NVR hosts, use `netsh advfirewall firewall add rule name='Block RTSP Inbound' protocol=TCP dir=in localport=554 action=block`. For VPN-less remote access, deploy WireGuard (free, open-source) on a dedicated jump host to gate all camera management access. Run a one-time Shodan CLI query (`shodan search 'port:554 net:'`) to confirm external visibility before and after ACL changes.

Evidence: Before isolating cameras, capture a full snapshot of current network state: run `arp -a` or pull the ARP table from your router/switch to document all camera MAC-to-IP mappings; export current firewall rule sets and NAT/port-forward tables (these will show which camera ports were exposed and for how long); pull DHCP lease history from your router for all camera IP assignments to establish first-seen dates; capture active RTSP session state using `netstat -an | grep 554` on the NVR host to identify any live unauthorized streams at time of containment; pull router/firewall connection state tables to document any established sessions to camera IPs from external addresses that existed at moment of isolation.

Detection — Query firewall and DNS logs for outbound connections from camera IP ranges to non-organizational endpoints, particularly unusual geographies or high-frequency beacon patterns. Check RTSP stream access logs (if your NVR or VMS captures them) for sessions initiated outside business hours or from unrecognized source IPs. Search SIEM for authentication events against camera management interfaces; flag any successful login not tied to a known admin account. Shodan or Censys queries against your public IP ranges can identify externally visible camera services — run this query now.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 13.6 (Collect DNS Query Audit Logs)

Compensating: Without a SIEM, use the following targeted queries manually: (1) On pfSense/OPNsense, filter firewall logs by source IP in your camera subnet with destination NOT in your internal RFC1918 ranges — export to CSV and sort by destination country using a free GeoIP lookup (e.g., `geoiplookup` on Linux). (2) On the NVR, locate the VMS access log — for Milestone XProtect these are in `C:\ProgramData\Milestone\XProtect Management Server\Logs\`; for Genetec, check `C:\Program Files (x86)\Genetec Security Center\Logs\`. (3) For Hikvision cameras, access the device web UI at http:///ISAPI/System/IO/inputs and pull the event log; for Dahua, SSH in and run `cat /mnt/mtd/Config/syslog` to extract auth events. (4) Use Wireshark with display filter `ip.src == && !(ip.dst == )` on a mirrored camera VLAN port to capture live exfiltration or C2 beacon traffic. (5) Run `nmap -sV --script rtsp-url-brute -p 554 ` to enumerate active RTSP streams and identify unauthenticated feeds.

Evidence: Extract and preserve the following before log rotation destroys evidence: (1) Hikvision device access logs via ISAPI endpoint `GET /ISAPI/System/userCheck` and `GET /ISAPI/System/SecurityManager/Loglist` — these record all authentication attempts with source IP and timestamp; (2) Dahua syslog entries at `/mnt/mtd/Config/syslog` documenting remote login events and stream access; (3) NVR/VMS session logs showing RTSP stream initiation events with source IP, stream channel, and duration — nation-state ISR operations typically show long-duration, low-bandwidth RTSP sessions (passive viewing) from non-local IPs; (4) DNS query logs for camera-originating queries — compromised cameras used as implant platforms will generate periodic DNS lookups to C2 infrastructure not matching NVR or NTP hostnames; (5) Firewall NetFlow or connection logs showing persistent outbound TCP sessions from camera IPs on non-standard ports (not 554 to NVR), which indicate embedded malware beaconing rather than legitimate RTSP streaming.

Eradication — Change all camera credentials immediately; replace any factory-default or hardcoded passwords with unique, complex credentials stored in a privileged access management system. Disable UPNP on cameras and upstream routers to prevent automatic port exposure. Where firmware updates are

available from the manufacturer, apply them — check vendor portals for Hikvision, Dahua, Axis, and any other deployed brands. Disable unused services on each device (Telnet, FTP, unnecessary HTTP endpoints). Document each device's firmware version and credential status.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST CM-6 (Configuration Settings), NIST CM-7 (Least Functionality), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.2 (Use Unique Passwords), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams managing 10+ cameras without a PAM tool, generate unique per-device passwords using `openssl rand -base64 16` for each camera and store them in KeePass (free, offline) with entries named by camera ID and MAC address. For Hikvision firmware updates, download directly from https://www.hikvision.com/en/support/download/firmware/ and apply via the device web UI under System > Maintenance > Upgrade; for Dahua, use https://www.dahuasecurity.com/support/downloadCenter/. Disable Telnet on Hikvision via ISAPI: `PUT /ISAPI/System/Network/ssh` with SSH enabled and Telnet disabled in the XML body. For UPnP, access your router admin panel and disable UPnP globally — on consumer routers this is typically under Advanced > NAT > UPnP; on Cisco IOS: `no ip nat service list`. Script credential rotation across a subnet using curl: `for ip in $(cat camera_ips.txt); do curl -u admin:oldpass -X PUT http://$ip/ISAPI/Security/users/1 -d 'newpass'; done`.

Evidence: Before changing credentials or applying firmware, capture the following as forensic baselines: (1) Full device configuration export from each camera — Hikvision: `GET /ISAPI/System/configurationData` exports full XML config including all enabled services, user accounts, and network settings; Dahua: access `http:///cgi-bin/configManager.cgi?action=getConfig&name=All` for equivalent; (2) Current firmware version string from each device — Hikvision: `GET /ISAPI/System/deviceInfo`; Dahua: `GET /cgi-bin/magicBox.cgi?action=getSystemInfo` — document this to compare against known-vulnerable versions; (3) Current user account list from each device to identify any attacker-created accounts added during the compromise period — Hikvision: `GET /ISAPI/Security/users`; (4) UPnP port mapping table from your router before disabling (`upnpc -l` using miniupnpc on Linux) to document what ports were auto-exposed to the internet by compromised devices; (5) Enabled services list per device to document attack surface at time of discovery.

Recovery — After hardening, re-scan your external attack surface using Shodan, Censys, or an equivalent tool to confirm no camera management interfaces remain internet-reachable. Validate that NVR/VMS access logs show only authorized sessions post-change. Monitor camera network segments for anomalous outbound traffic for a minimum of 30 days. Confirm firmware versions match the latest available release from each vendor.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CA-7 (Continuous Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Run Shodan CLI post-hardening: `shodan search 'net: port:554,8080,37777'` and `shodan search 'net: product:hikvision OR product:dahua OR product:axis'` — zero results is the required outcome. For ongoing traffic monitoring of the camera VLAN without a SIEM, configure a Raspberry Pi or spare Linux host as a passive tap using `tcpdump -i -w /captures/camera_$(date +%F).pcap 'src net and not dst net '` with a daily cron job and 30-day retention. Use Zeek (free) on the same tap host to generate conn.log and dns.log for the camera segment — review weekly for new external destination IPs. For firmware integrity, maintain a local hash register: `curl http:///ISAPI/System/deviceInfo | grep -i firmware` and compare against a baseline file created immediately post-patching.

Evidence: During the 30-day monitoring window, collect and preserve: (1) Daily Zeek conn.log exports from the camera network segment showing all outbound connections — nation-state implants on cameras have been documented using low-and-slow beaconing at intervals of 60-300 seconds to blend with NTP and update traffic; (2)

NVR/VMS session logs with source IP, authentication method, and stream access channel for every session — compare against a documented baseline of known admin source IPs established immediately post-hardening; (3) Weekly Shodan/Censys scan results saved as timestamped exports to demonstrate ongoing attack surface validation; (4) Firmware version query responses from each device stored as dated files to create a verifiable chain of custody showing patched state was maintained; (5) Any RTSP session logs showing stream duration outliers — legitimate monitoring sessions in a typical enterprise rarely exceed 8 hours continuously, whereas ISR collection sessions may run 12-72 hours uninterrupted.

Post-Incident — This campaign exposes three control gaps: (1) absent asset management for IoT and physical security devices, which are often outside standard IT inventory; (2) no network segmentation between camera infrastructure and corporate networks; (3) no monitoring or alerting on camera network traffic. Address each with formal controls: add IoT/OT devices to asset inventory, implement a dedicated VLAN for physical security systems with deny-all egress except to the NVR, and extend SIEM coverage to include camera network segments. Map these gaps to NIST CSF 2.0 Identify (ID.AM) and Protect (PR.AC, PR.PT) functions for governance tracking.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST CM-8 (System Component Inventory), NIST SC-7 (Boundary Protection), NIST SI-4 (System Monitoring), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 1.2 (Address Unauthorized Assets), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 8.2 (Collect Audit Logs)

Compensating: For IoT/camera asset inventory without an enterprise CMDB, build a structured CSV inventory using `nmap -sn -oG - | awk '/Up/{print $2}' | xargs -I{} nmap -sV -p 80,443,554,8080,37777 {} --script banner` to auto-discover and fingerprint all camera devices; store results in a spreadsheet with columns for IP, MAC, vendor (from OUI lookup), model, firmware version, credential-changed date, and last-seen date — review monthly. For VLAN segmentation without managed switches, deploy a dedicated physical interface on your firewall for camera traffic and apply inter-VLAN deny rules: on pfSense, create a floating rule blocking traffic from the camera interface to the LAN interface except destination NVR IP on TCP 554. For SIEM-less monitoring, deploy the Elastic Stack (free tier) with Filebeat forwarding Zeek logs from the camera tap host — this provides searchable connection history for the camera segment at no license cost. Add MITRE ATT&CK T1078 (Valid Accounts) and T1071.001 (Application Layer Protocol: Web Protocols) to your threat model for camera infrastructure, as nation-state operators have been observed authenticating with compromised credentials and using HTTP/RTSP for covert data collection.

Evidence: As part of the lessons-learned process, compile the following for the post-incident report and future detection improvement: (1) Complete timeline reconstructed from firewall connection logs showing first external access to camera management ports — this establishes the exposure window for reporting purposes; (2) Full camera inventory with exposure duration per device, derived from DHCP history and firewall NAT rule creation timestamps, to quantify scope for any regulatory notification assessment; (3) Documented list of camera models and firmware versions in use at time of discovery, cross-referenced against CISA Known Exploited Vulnerabilities catalog and ICS-CERT advisories for Hikvision (ICSA-21-336-02), Dahua, and Axis — this determines whether any devices had known CVEs that were unpatched; (4) Network architecture diagram annotated to show pre-incident camera segment routing, including any direct paths from camera subnet to corporate LAN that could have enabled lateral movement from a compromised camera acting as an implant host; (5) Gap analysis document mapping each identified control failure (absent inventory, missing segmentation, no monitoring) to NIST CSF 2.0 ID.AM and PR.AC functions for board-level governance reporting and remediation tracking.

Detection Guidance

No published IOCs are associated with this campaign in source reporting. Detection must rely on behavioral indicators. Key signals to hunt: (1) Outbound connections from camera network segments to external IPs outside configured authorized services (NTP, DNS, firmware updates from known vendor hosts); unexpected

connections to unusual geographies or high-frequency beacon patterns are anomalous. (2) RTSP stream access (TCP 554) from source IPs outside your NVR or authorized client range. (3) HTTP/HTTPS management interface logins outside business hours or from unrecognized user agents. (4) Firmware modification events or unexpected reboots on camera devices. (5) ARP anomalies or new MAC addresses appearing on camera VLANs, which may indicate adversary lateral movement or man-in-the-middle positioning (T1557). If your VMS or NVR generates access logs, parse them for session duration and source IP diversity; legitimate monitoring shows consistent, scheduled access, while adversary access often shows irregular session patterns. MITRE ATT&CK techniques to map detections against: T1125 (video capture), T1133 (external remote services), T1078 (valid accounts), T1190 (exploit public-facing application), T1557 (adversary-in-the-middle).

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.darkreading.com/cyber-risk/wartime-usage-of-compromised-ip-cameras-highlight-their-danger`	Primary source reporting on nation-state IP camera surveillance campaign, Dark Reading, March 2026	HIGH
URL	`https://unit42.paloaltonetworks.com/iot-supply-chain-cve-2021-28372/`	Palo Alto Unit 42 research on CVE-2021-28372, IoT supply chain vulnerability illustrative of the broader weakness class exploited in this campaign	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1562.001** — Disable or Modify Tools
- **T1016** — System Network Configuration Discovery
- **T1078** — Valid Accounts
- **T1203** — Exploitation for Client Execution
- **T1071.001** — Web Protocols
- **T1602** — Data from Configuration Repository
- **T1557** — Adversary-in-the-Middle
- **T1133** — External Remote Services
- **T1040** — Network Sniffing
- **T1078.001** — Default Accounts
- **T1125** — Video Capture
- **T1591** — Gather Victim Org Information
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-2** — Account Management

- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement
- **CM-3** — Configuration Change Control
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **6.3**
- **6.4**
- **6.5**
- **6.1**
- **6.2**
- **2.5**
- **2.6**
- **16.10**
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1562.001	Disable or Modify Tools	Defense-Evasion
T1016	System Network Configuration Discovery	Discovery
T1078	Valid Accounts	Defense-Evasion
T1203	Exploitation for Client Execution	Execution
T1071.001	Web Protocols	Command-And-Control
T1602	Data from Configuration Repository	Collection
T1557	Adversary-in-the-Middle	Credential-Access
T1133	External Remote Services	Persistence
T1040	Network Sniffing	Credential-Access
T1078.001	Default Accounts	Defense-Evasion
T1125	Video Capture	Collection
T1591	Gather Victim Org Information	Reconnaissance
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyber-risk/wartime-usage-of-compromised...	T3
CVE-2021-28372: How a Vulnerability in Third-Party Technology Is ...	https://unit42.paloaltonetworks.com/iot-supply-chain-cve-2021-28372/	T3
IP Camera Security: From Setup to Vulnerability Discovery - HackMag	https://hackmag.com/security/ipcams-hack	T3

Source	URL	Tier
Hikvision Has "Highest Level of Critical Vulnerability," Impacting 100 ...	https://ipvm.com/reports/hikvision-36260	T3
Critical Vulnerability in v380 Cameras: How Plaintext Credentials ...	https://medium.com/@romaxa552015/critical-vulnerability-in-v380-cam...	T3

Generated 2026-03-29 18:35 UTC by TJS Security Command Center