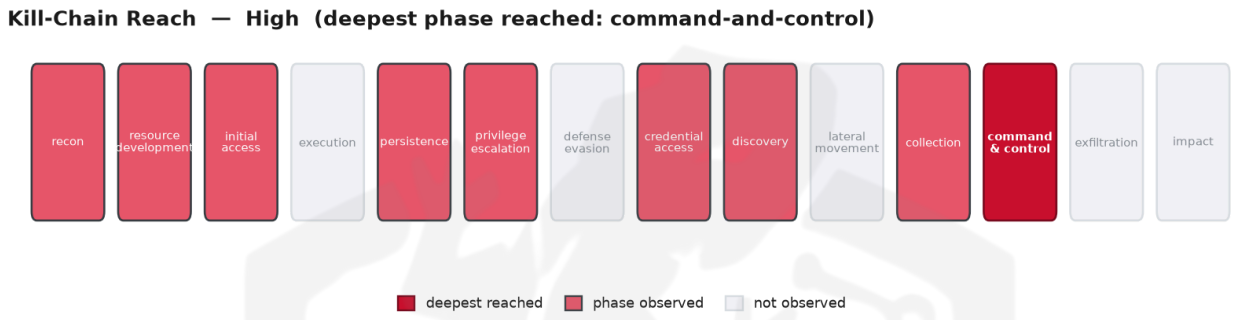
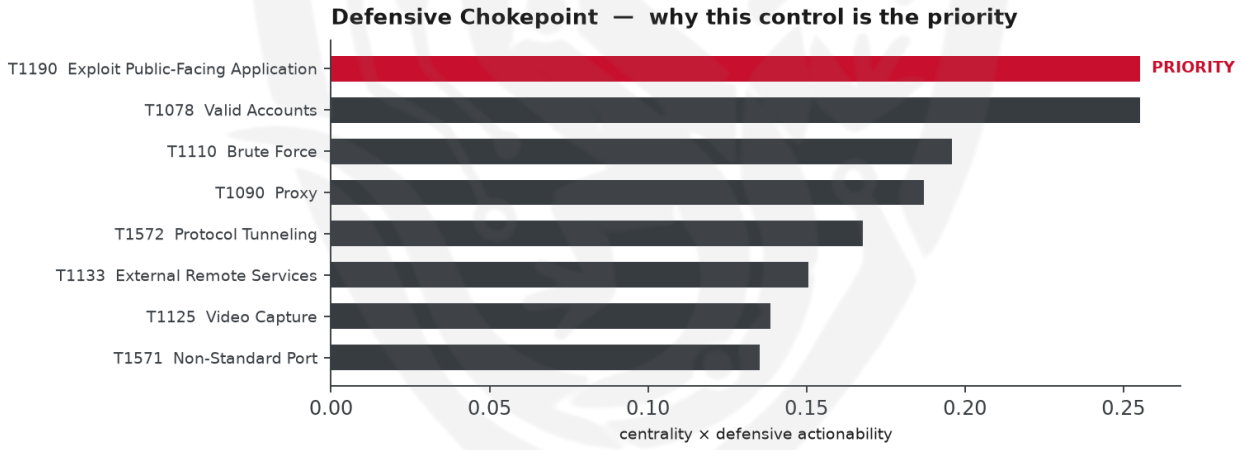
THREAT REPORT: UKRAINIAN IP CAMERA EXPLOITATION

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The observed cluster of activity has been exploiting vulnerabilities in IP cameras across multiple countries, including Austria, Bulgaria, and the United Kingdom, targeting government and retail sectors. The central vulnerability exploited is CVE-2021-33044. Priority should be given to patching the affected public-facing CVE immediately to prevent further exploitation. The threat actor's techniques include system owner discovery, external remote services, and exploit public-facing application, indicating a high operational risk band.

Threat Overview

The threat actor, whose identity is insufficient to determine, is exploiting the CVE-2021-33044 vulnerability, among others, to target IP cameras in various countries. The malware families used are not specified, but

the techniques employed include system information discovery, system owner/user discovery, and data from local system. The targeted countries include Ukraine, Germany, and Italy, among others, with a focus on government and retail sectors.

Attack Chain and Priority Control

The observed techniques form a chain that starts with system owner/user discovery and system information discovery, followed by external remote services and data from local system. The priority technique is T1190 Exploit Public-Facing Application, which is the graph chokepoint. To mitigate this, the priority control is to "Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only. In parallel, patch CVE-2021-33044 on all affected systems."

Infrastructure and Corroboration

The malicious infrastructure is hosted on providers such as Aeza Group LLC and Global Connectivity Solutions LLP, as observed. However, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1033 System Owner/User Discovery
- T1592 Gather Victim Host Information
- T1133 External Remote Services
- T1082 System Information Discovery
- T1005 Data from Local System
- T1190 Exploit Public-Facing Application
- T1572 Protocol Tunneling
- T1595.002 Vulnerability Scanning
- T1125 Video Capture
- T1090 Proxy
- T1049 System Network Connections Discovery
- T1588.002 Tool
- T1110 Brute Force
- T1078 Valid Accounts
- T1571 Non-Standard Port
- T1589.001 Credentials
- T1213 Data from Information Repositories
- T1018 Remote System Discovery
- T1584.001 Domains

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.3139).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3795; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
Magic Hound	0.3795
FIN5	0.3649
PittyTiger	0.3612
Sandworm Team	0.3595
Ember Bear	0.3471

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	89[.]208[.]97[.]165	AbuseIPDB 0% (FR) · AS210644 Aeza Group LLC
IP	213[.]165[.]63[.]49	AbuseIPDB 0% (LV) · AS215540 Global Connectivity Solutions LLP

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** T1190 Exploit Public-Facing Application was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 22+ groups that use Exploit Public-Facing Application, this pairing runs 2.0x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain their objective by leveraging WMI's native Windows capabilities to execute commands and gather information, potentially using WMI to interact with other systems or to create new processes. This technique may be particularly appealing as it allows the actor to blend in with legitimate administrative activity, making it harder to detect. To counter this potential pivot, the mandated defensive control is to monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=23, lift 1.5), T1059 Command and Scripting Interpreter (n=38, lift 1.2)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command