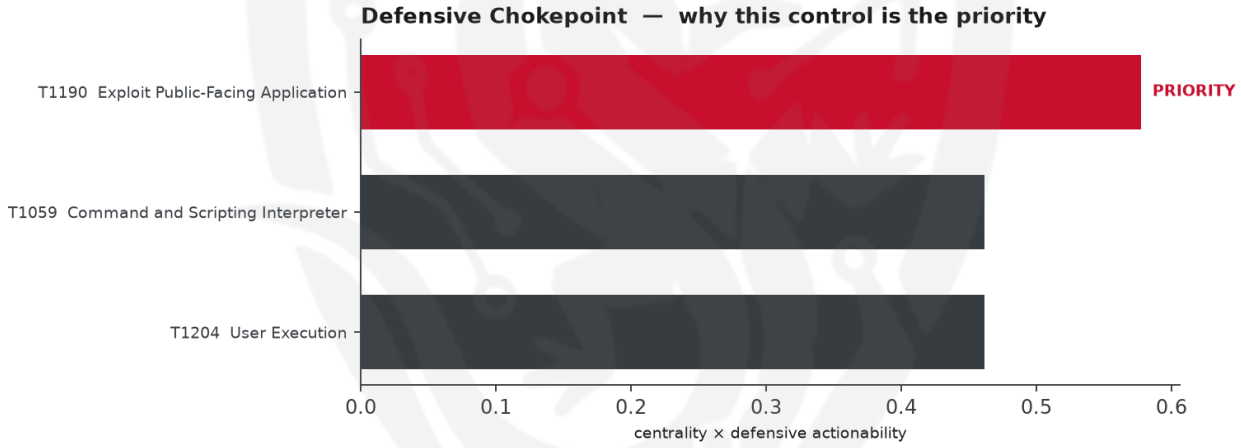
THREAT REPORT: UNK_MASSTRACTION CAMPAIGN

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 source attributes this activity to UNK_MassTraction, a threat actor exploiting the CVE-2024-42009 vulnerability, primarily targeting the education sector in the United States of America and Canada. The malware families involved include IceCube, SquareShell, VShell, and SNOWLIGHT. Priority should be given to patching the affected public-facing applications and restricting management interfaces to mitigate the threat.

Threat Overview

UNK_MassTraction, the observed cluster of activity, is associated with the exploitation of CVE-2024-42009, alongside other cited vulnerabilities such as CVE-2023-2868 and CVE-2025-49113. The techniques inferred from the report include Command and Scripting Interpreter, Exploit Public-Facing Application, and User Execution, with the primary focus on exploiting public-facing applications. The education sector in the United States and Canada is the main target of this campaign.

Attack Chain and Priority Control

The attack chain involves exploiting public-facing applications, which is the graph chokepoint, identified as T1190 Exploit Public-Facing Application. This technique is crucial for the threat actor to gain initial access. The priority control, as recommended, is to "Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only. In parallel, patch CVE-2024-42009 on all affected systems."

Infrastructure and Corroboration

The malicious infrastructure associated with UNK_MassTraction is hosted on providers such as BlueVPS Ou and Clouvider Limited. While there are no malware families corroborated by abuse.ch, AbuseIPDB flags some indicators, though none reach the 80% confidence threshold, with the highest confidence seen being 30%. These corroboration points provide additional context to the threat landscape without altering the primary threat assessment.

Technical Appendix

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

Observed Techniques (ATT&CK, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1059 Command and Scripting Interpreter - T1190 Exploit Public-Facing Application - T1204 User Execution

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.5774).
- Operational risk: Low (score 0.191, reaches execution).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4364; 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
TA578	0.4364
TA459	0.4082
TA577	0.3482
Nomadic Octopus	0.3482
Gallmaker	0.3482

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 30%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	45[.]86[.]229[.]111	AbuseIPDB 0% (ES) · AS62005 BlueVPS Ou
IP	194[.]213[.]18[.]133	AbuseIPDB 30% (US) · AS62240 Clouvider Limited
IP	45[.]150[.]109[.]151	AbuseIPDB 0% (NL) · AS62005 BlueVPS Ou
URL	hxxps://45[.]150[.]109[.]151[.]sslip[.]io:23088/app/js/jquery[.]min[.]js	
URL	hxxps://194[.]213[.]18[.]133[.]sslip[.]io:23088/app/js/jquery[.]min[.]js	
Hash	a02f124c5ce4180bd130a62ee03262f399c33491de3aed36e0b15155ae4926c0	

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 UNK_MassTraction actor could pivot to using T1047 Windows Management Instrumentation to maintain their objective by leveraging WMI's native capabilities to execute commands and interact with the system, potentially allowing them to bypass the initial block on public-facing application exploitation. This technique may be particularly appealing as it enables the actor to perform various tasks, such as gathering system information or executing malicious code, all while blending in with legitimate WMI activity. To counter this potential move, the mandated defensive control of monitoring wmiprvse.exe child-process creation, restricting remote WMI (DCOM) at the host firewall, and enabling WMI-Activity operational logging should be implemented.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=23, lift 1.5), T1569 System Services (n=8, lift 1.8)

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