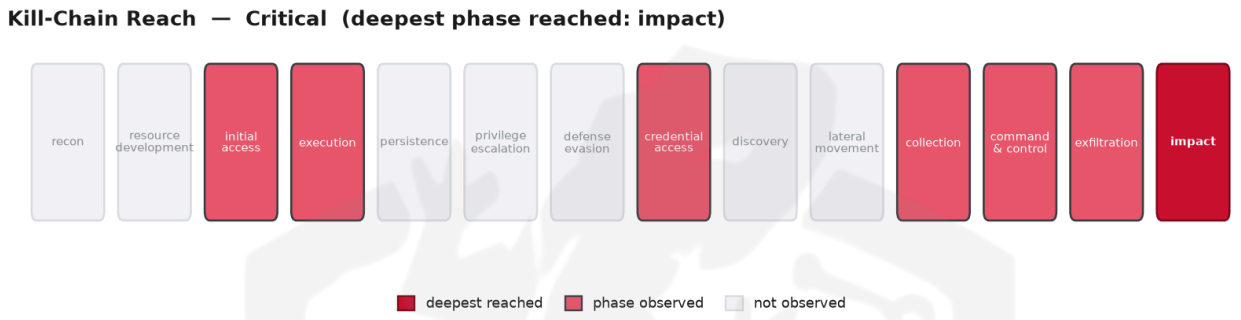
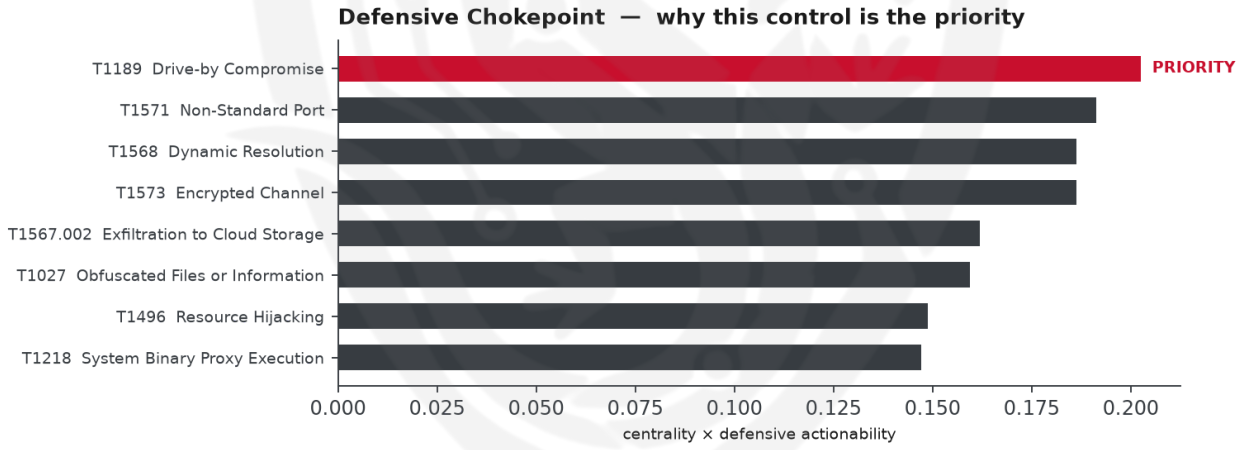
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 observed cluster of activity has been targeting the education sector in the United States of America, leveraging various techniques to compromise systems. The priority defensive action should be to enforce browser isolation and patching, as well as block known-malicious domains at the proxy and disable risky plugins. This campaign poses a critical operational risk due to its potential impact. The threat actor's identity remains unknown, and the focus should be on mitigating the technical mechanics of the attack.

Threat Overview

The threat actor, whose identity is unknown, is utilizing a range of techniques including direct network flood, JavaScript, stealing web session cookies, and domain generation algorithms to target educational

institutions. The victimology suggests that student web proxies are being turned into DDoS bots, highlighting the need for robust defensive measures.

Attack Chain and Priority Control

The attack chain involves a combination of techniques, including drive-by compromise, which is identified as the priority technique. This technique is a critical chokepoint in the attack chain, allowing the threat actor to gain initial access to the system. The priority control to mitigate this threat is to "Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins."

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this campaign, and no malware families have been corroborated by abuse.ch. Additionally, AbuseIPDB has not flagged any indicators with a confidence level 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)

- T1498.001 Direct Network Flood
- T1059.007 JavaScript
- T1539 Steal Web Session Cookie
- T1568.002 Domain Generation Algorithms
- T1071.004 DNS
- T1036.005 Match Legitimate Resource Name or Location
- T1218 System Binary Proxy Execution
- T1568 Dynamic Resolution
- T1571 Non-Standard Port
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1567.002 Exfiltration to Cloud Storage
- T1496 Resource Hijacking
- T1213 Data from Information Repositories
- T1189 Drive-by Compromise
- T1071.001 Web Protocols
- T1204.001 Malicious Link
- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1189 Drive-by Compromise (centrality 0.2025).

- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3831; 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
TA551	0.3831
LazyScripter	0.3727
RedEcho	0.3608
Machete	0.3466
Transparent Tribe	0.3405

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
Domain	21baseballacademy[.]com
Domain	lucideon[.]top
Domain	c[.]vipersfutbol[.]com
Domain	cdn[.]caan[.]edu
Domain	cdn[.]conditionfuneral[.]com
Hash	0a913561831bdf2c26dcf18b852b5cc1
Hash	c6851a038da578a80eeb201e0588c84c
Hash	10ddbbae0070267b8d15888b09a3cdb19fa74d861315b71f21c9ace8b9f85c75

Type	Indicator
Hash	4b188d179e50e8208a6efec85e273e88d8fc390c836f299ba12915e0840408fd
Hash	eb4e1394d537d8eba509dd5c57e7aaf4c1df57715c7161330012a11f6202af84

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:** T1189 Drive-by Compromise (initial-access)
- **Observed here:** T1189 Drive-by Compromise was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1566 Phishing (initial-access)
- **Basis:** 27 of 170 documented groups that use Drive-by Compromise also use Phishing (conditional 0.87, lift 1.5, i.e. ~1.5x base rate). Strongest same-tactic neighbour.

The actor could pivot to T1566 Phishing to maintain their objective by crafting convincing emails that trick users into divulging sensitive information or installing malware, potentially exploiting the same vulnerabilities they attempted to leverage through drive-by compromise. This technique may allow the actor to bypass the blocked control and still achieve their goals by relying on social engineering tactics. The defensive control to counter this potential pivot would be to enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button.

Also plausible (same tactic): T1195 Supply Chain Compromise (n=3, lift 1.5)

Detection and hardening for the pivot (T1566 Phishing)

- **Telemetry:** Email security gateway logs; Endpoint (Office child processes); Proxy/DNS
- **Detect:**
  - Office apps (winword/excel) spawning script or LOLBIN child processes
  - Mark-of-the-Web bypass; ISO/IMG/LNK/HTML-smuggling attachments detonating
  - First-contact domains and newly registered domains in mail links
- **Harden:**
  - Attachment sandboxing; block high-risk types (iso, img, lnk, htm) at the gateway
  - Attack-surface-reduction rules for Office child processes; user reporting button
- **MITRE:** M1049 Antivirus/Antimalware, M1031 Network Intrusion Prevention, M1017 User Training, M1021 Restrict Web-Based Content · DS0015 Application Log, DS0009 Process, DS0029 Network Traffic