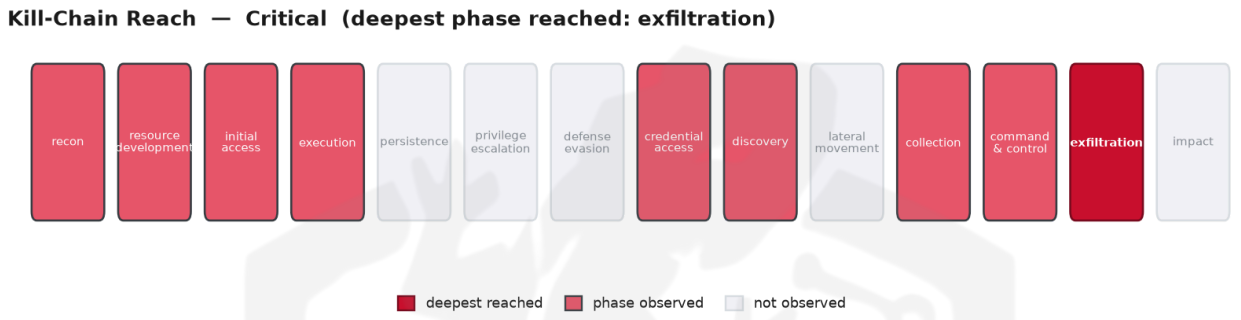
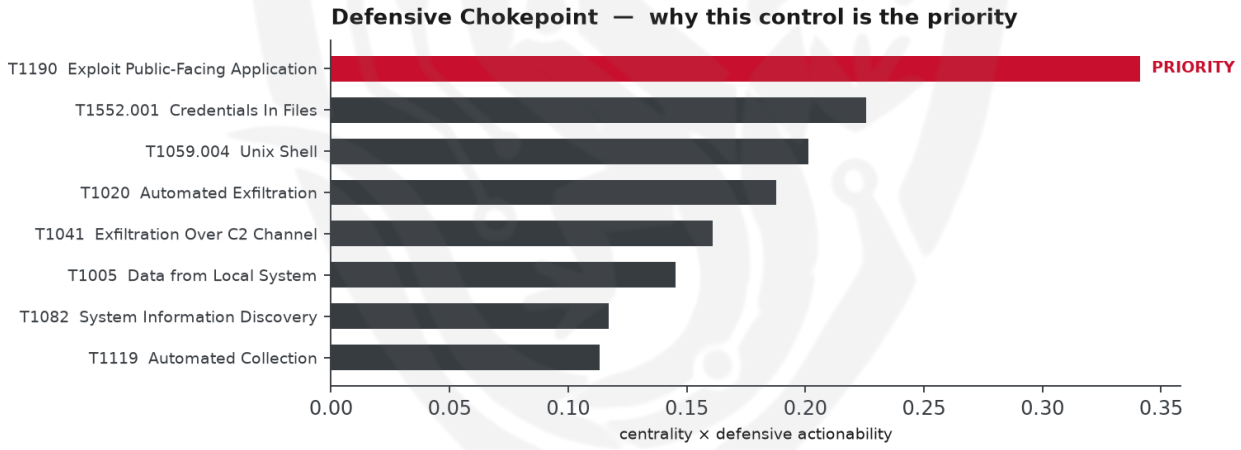
# THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

## 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 is exploiting a critical vulnerability, CVE-2026-41940, to target technology and hosting sectors. The threat actor is leveraging GitHub Actions to power a distributed exploitation campaign against cPanel and WHM. Priority should be given to patching the affected systems to prevent further exploitation. The campaign's ability to exfiltrate data poses a significant risk, making immediate action necessary.

## Threat Overview

The threat actor is exploiting the CVE-2026-41940 vulnerability in public-facing applications, targeting the technology and hosting sectors. The malware families used in the campaign are not specified, but the

exploitation of the vulnerability is the primary concern. The actor is using various techniques, including compromising software dependencies and development tools, to gain access to the targeted systems.

## Attack Chain and Priority Control

The attack chain involves multiple techniques, including compromising software dependencies, DNS manipulation, and local data staging, ultimately leading to the exploitation of the public-facing application. The priority technique is T1190 Exploit Public-Facing Application, which is the graph chokepoint. To mitigate this, the priority control is: Patch CVE-2026-41940 on all affected systems as the top priority, then: Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

## Infrastructure and Corroboration

There is no specific information on the hosting providers or ASNs observed, as the data is not available. Additionally, 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)

- T1195.001 Compromise Software Dependencies and Development Tools
- T1071.004 DNS
- T1074.001 Local Data Staging
- T1119 Automated Collection
- T1082 System Information Discovery
- T1005 Data from Local System
- T1190 Exploit Public-Facing Application
- T1595.002 Vulnerability Scanning
- T1020 Automated Exfiltration
- T1552.001 Credentials In Files
- T1041 Exfiltration Over C2 Channel
- T1059.004 Unix Shell
- T1584.006 Web Services
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

### Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.3412).
- Operational risk: Critical (score 0.968, reaches exfiltration).

## Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4728; 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 |
|---|---|
| Winter Vivern | 0.4728 |
| Volatile Cedar | 0.3299 |
| APT18 | 0.3086 |
| Ember Bear | 0.3073 |
| VOID MANTICORE | 0.3041 |

## 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 | f5b0b742-240a-4811-8a5b-b0ba6060685d[.]dnshook[.]site |
| URL | hxxp://43[.]228[.]157[.]68:80/api/dl/amd64 |
| URL | hxxp://43[.]228[.]157[.]68:80/api/dl/arm64 |
| URL | hxxp://43[.]228[.]157[.]68:80/api/github-heartbeat |
| URL | hxxp://43[.]228[.]157[.]68:80/api/github-results |
| Hash | 572745566ec674c6eae10c179b0de2ba |
| Hash | e219da0599dea936ee867792e2dfe6a2c2a7c68b |
| Hash | 22f721fd3a81d2e27cbf90a122bb977f630c50b79daa98350f0e57b04dfa81f1 |

## 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:** the threat actor used T1195.001 Compromise Software Dependencies and Development Tools here as an alternative initial-access technique.
- **Projected pivot:** T1195.001 Compromise Software Dependencies and Development Tools (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to compromising software dependencies and development tools, T1195.001, to potentially inject malicious code into the software development lifecycle, which may allow them to maintain access or regain a foothold after the initial block. This technique could be used to target vulnerabilities in the software supply chain, which would likely be a high-impact target for the actor. To counter this potential move, the defensive control of verifying software supply chain integrity (signing, SBOM); pin and monitor third-party dependencies and update channels should be implemented.

- **Defensive countermeasure:** Verify software supply chain integrity (signing, SBOM); pin and monitor third-party dependencies and update channels.