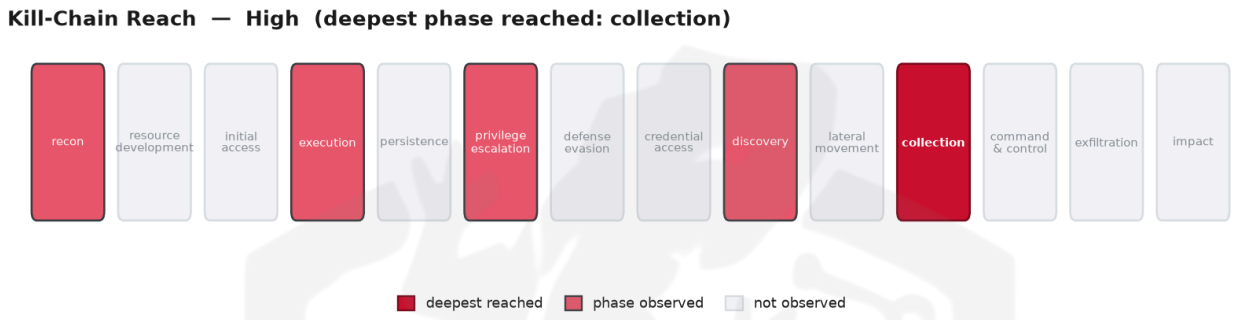
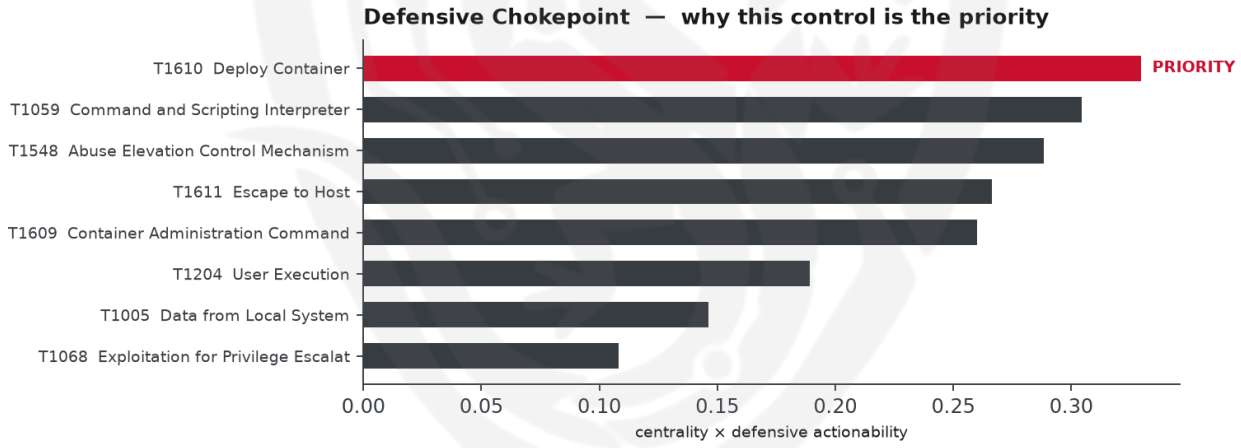
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 exploiting CVE-2026-46316, although the specific targets and sectors affected are not well understood. The threat actor is utilizing various techniques to gather information and escalate privileges. Priority should be given to patching the exploited vulnerability and implementing specific mitigations. The operational risk band for this activity is considered high.

Threat Overview

The threat actor, whose identity is not specified, is exploiting CVE-2026-46316. The techniques used include gathering victim host information, system information discovery, and data extraction from local systems. The actor is also utilizing techniques such as escaping to the host, deploying containers, and abusing elevation control mechanisms.

Attack Chain and Priority Control

The observed techniques form a chain that allows the threat actor to gather information, escalate privileges, and deploy containers. The priority technique is T1610 Deploy Container, which is the graph chokepoint. The concrete control to mitigate this technique is to "Patch CVE-2026-46316 on all affected systems as the top priority, then: Apply the specific MITRE ATT&CK mitigation for this technique; add host/network detections and least-privilege controls around it."

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed. According to abuse.ch, no malware families have been corroborated, and 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)

- T1592 Gather Victim Host Information
- T1082 System Information Discovery
- T1005 Data from Local System
- T1611 Escape to Host
- T1610 Deploy Container
- T1548 Abuse Elevation Control Mechanism
- T1059 Command and Scripting Interpreter
- T1609 Container Administration Command
- T1204 User Execution
- T1068 Exploitation for Privilege Escalation

Analytical Scores

- Priority technique (graph chokepoint): T1610 Deploy Container (centrality 0.4118).
- Operational risk: High (score 0.562, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3586; 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
Windigo	0.3586
APT37	0.25
Whitefly	0.2449
TA578	0.239
CURIUM	0.2349

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
Hash	e0ab84da2d2783c8cae3624e8ce58b99ad79219753b249671ff7f743abdacc35
Hash	838ea8d6b201e2eed181f3fd890f99ecb6178b52
Hash	fbf0b6abd651622864eb921f891b3e7c538fc8a9

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:** T1610 Deploy Container (execution)
- **Observed here:** the threat actor used T1059 Command and Scripting Interpreter here as an alternative execution technique.
- **Projected pivot:** T1059 Command and Scripting Interpreter (execution)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to using T1059 Command and Scripting Interpreter to execute commands and scripts, potentially leveraging native operating system tools to maintain access and achieve their objectives. This may involve using command-line interpreters to run scripts or commands that can bypass some security controls, which would likely be a next step in their campaign. To counter this, the mandated defensive control of Constrain PowerShell for unprivileged users (Constrained Language Mode + AppLocker); enable script-block logging; block wscript/cscript where unneeded should be implemented.

Detection and hardening for the pivot (T1059 Command and Scripting Interpreter)

- **Telemetry:** Sysmon / EDR process + command line; PowerShell Script Block Logging (4104); AMSI
- **Detect:**
  - Security 4688 / Sysmon 1 with full command lines; encoded or obfuscated PowerShell
  - PowerShell 4104 script-block content; suspicious cmdlets and download cradles
  - Office or browser processes spawning powershell/cmd/wscript
- **Harden:**
  - Enable Script Block Logging + AMSI; Constrained Language Mode
  - Application control (WDAC/AppLocker); remove/limit unused interpreters
- **MITRE:** M1049 Antivirus/Antimalware, M1038 Execution Prevention, M1042 Disable or Remove Feature, M1045 Code Signing · DS0009 Process, DS0012 Script, DS0017 Command