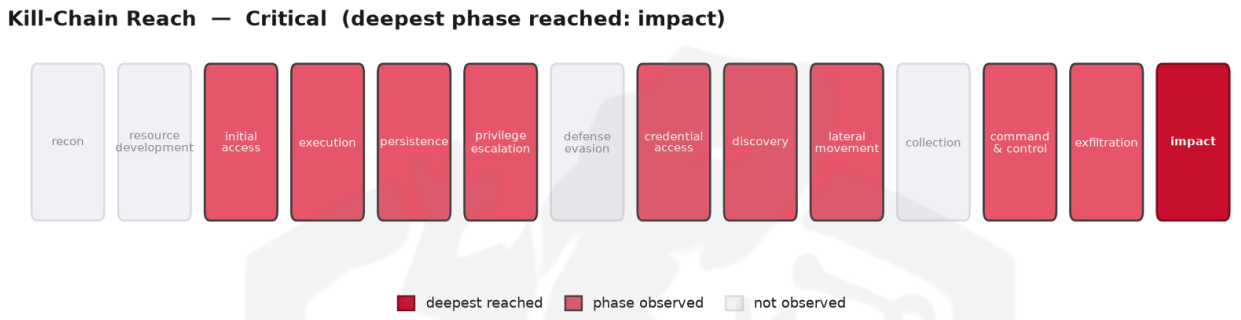
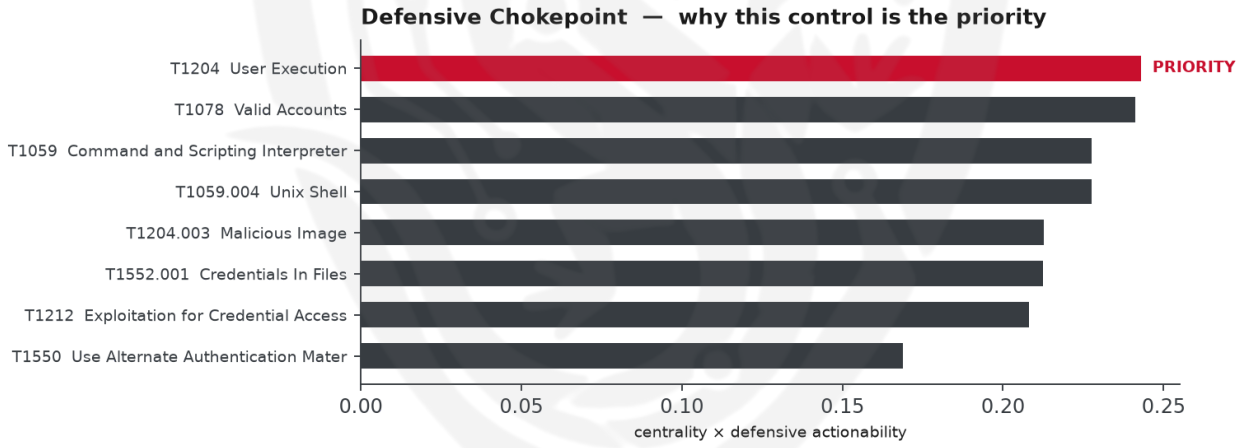
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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-2026-33017, a vulnerability that poses a significant threat to the technology sector. The threat actor's tactics, techniques, and procedures (TTPs) involve a range of techniques to gain access to and exfiltrate data from targeted systems. Priority should be given to patching the exploited vulnerability and implementing additional controls to prevent further exploitation. The lack of specific information on the threat actor and targeted country highlights the need for a proactive and comprehensive defense strategy.

Threat Overview

The threat actor, whose identity is currently unknown, is exploiting CVE-2026-33017, as well as potentially leveraging other vulnerabilities such as CVE-2026-55255. The actor is targeting the technology sector,

using various techniques, including account discovery, exploitation of public-facing applications, and exfiltration over web services. The malware families used in the campaign are currently unknown.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving initial access, execution, and exfiltration of data. The priority technique, T1204 User Execution, is a critical chokepoint in the attack chain. To mitigate this threat, the top priority control is to: Patch CVE-2026-33017 on all affected systems as the top priority, then: Block execution of downloaded HTA/JS/LNK; enforce mark-of-the-web; disable Office macros from the internet; user awareness on lures.

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted on CognetCloud Inc, according to third-party observations. Additionally, abuse.ch has corroborated the presence of VShell malware families in relation to this activity. However, AbuseIPDB has only reported a low confidence level of 1% for the indicators associated with this campaign, highlighting the need for continued monitoring and analysis.

Technical Appendix

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

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

- T1087.001 Local Account
- T1071 Application Layer Protocol
- T1190 Exploit Public-Facing Application
- T1567 Exfiltration Over Web Service
- T1552 Unsecured Credentials
- T1550 Use Alternate Authentication Material
- T1087 Account Discovery
- T1059 Command and Scripting Interpreter
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1204 User Execution
- T1212 Exploitation for Credential Access
- T1059.004 Unix Shell
- T1204.003 Malicious Image
- T1078 Valid Accounts
- T1571 Non-Standard Port
- T1496 Resource Hijacking
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1550.001 Application Access Token

Analytical Scores

- Priority technique (graph chokepoint): T1204 User Execution (centrality 0.3037).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3162; 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
APT18	0.3162
Confucius	0.2958
APT33	0.2935
Rocke	0.2846
TeamTNT	0.284

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 1%.
- Malware families corroborated by abuse.ch: VShell.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

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[.]207[.]216[.]55	AbuseIPDB 1% (HK) · VShell · AS401696 CognetCloud Inc
URL	hxxp://45[.]207[.]216[.]55:8084/slt	

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