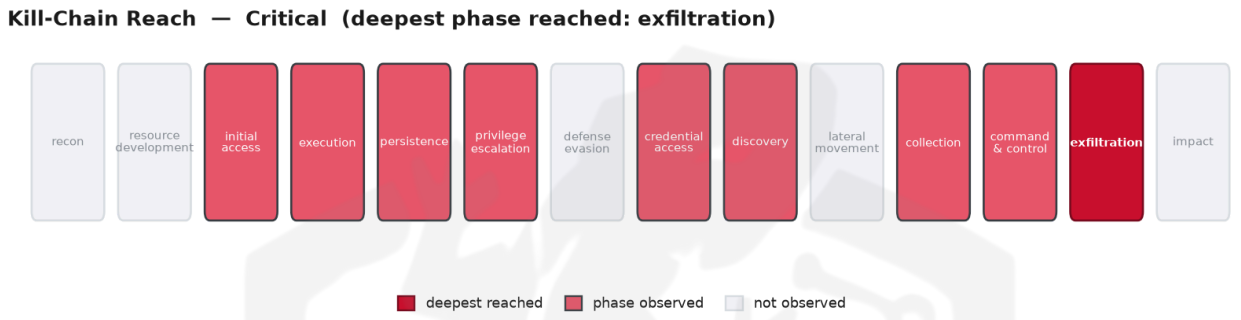
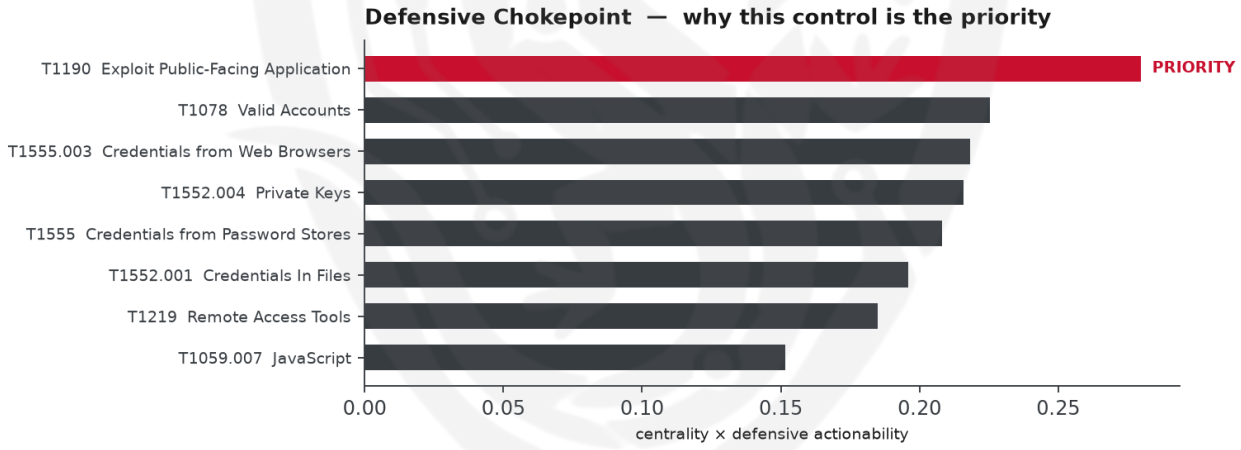
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 linked to the exploitation of CVE-2026-48558, utilizing malware families such as TaskWeaver and Djinn Stealer. The technology sector has been targeted, and priority should be given to patching the affected systems to prevent further exploitation. The threat actor's ability to exploit public-facing applications poses a significant risk, and immediate action is necessary to mitigate this threat.

Threat Overview

The threat actor, whose identity is currently unknown, has been observed using the TaskWeaver and Djinn Stealer malware families to exploit the CVE-2026-48558 vulnerability. The targeted sector is technology,

and the actor's goals and motivations are not clearly understood at this time. The exploitation of this vulnerability allows the actor to gain access to sensitive information and potentially exfiltrate data.

Attack Chain and Priority Control

The observed attack chain involves a series of techniques, including system owner/user discovery, archive via utility, and exploit public-facing application. The priority technique is T1190 Exploit Public-Facing Application, which serves as a chokepoint in the attack chain. To mitigate this threat, the following concrete control should be applied: Patch CVE-2026-48558 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

The malicious infrastructure has been observed to be hosted by Evoxt Sdn. Bhd. However, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB, with the highest confidence seen being 0%. These findings are based on third-party enrichment and corroboration, and do not override the primary source pulse.

Technical Appendix

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

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

- T1560.001 Archive via Utility
- T1033 System Owner/User Discovery
- T1132.001 Standard Encoding
- T1059.007 JavaScript
- T1082 System Information Discovery
- T1005 Data from Local System
- T1190 Exploit Public-Facing Application
- T1555 Credentials from Password Stores
- T1219 Remote Access Tools
- T1555.003 Credentials from Web Browsers
- T1552.004 Private Keys
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1041 Exfiltration Over C2 Channel
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1573.002 Asymmetric Cryptography
- T1071.001 Web Protocols
- T1552.007 Container API

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.2797).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4683; 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
Stealth Falcon	0.4683
MuddyWater	0.4211
APT33	0.4168
RedCurl	0.3953
Inception	0.3501

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	Context
IP	96[.]126[.]130[.]126	AbuseIPDB 0% (JP) · AS149440 Evoxt Sdn. Bhd.
Domain	a[.]dev-tunnels[.]com	
Hash	00cc86d1144020c24c8fbb3a8dc6b908926497ebd23be3bf854360f93d1c8f4c	
Hash	f4a72600a3735c2a4d843875ea61bbb6f935a1af51a81f2fbc992ce11ba94afc	

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