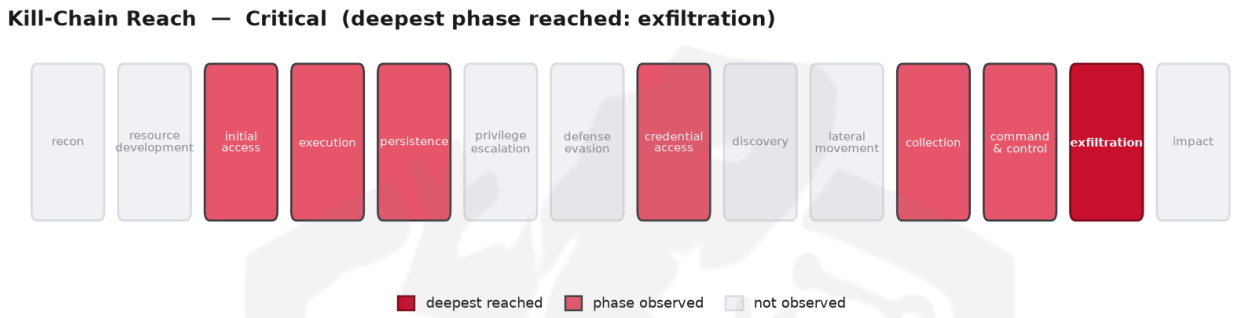
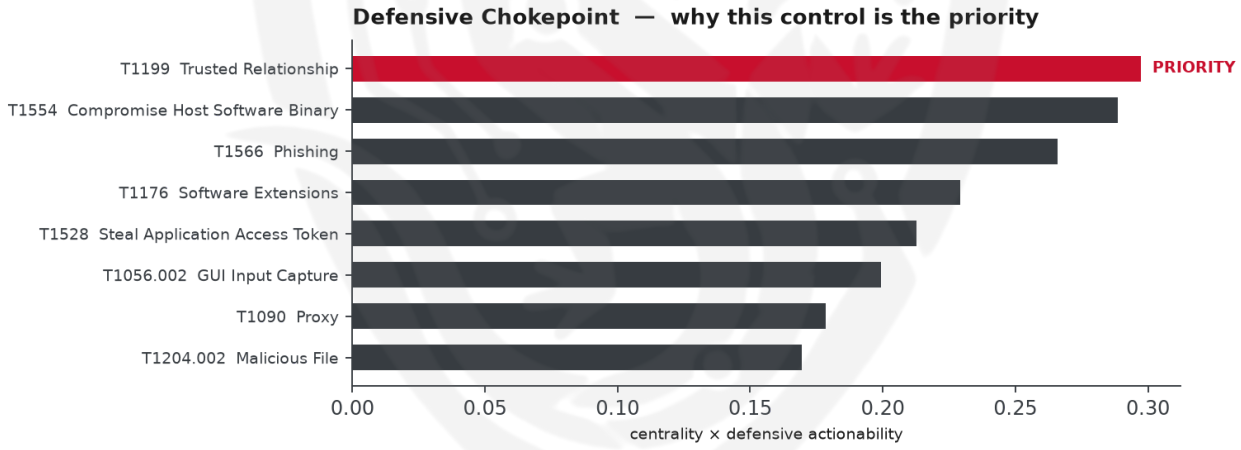
THREAT REPORT: UNKNOWN_ADVERSARY CHROMIUM EXTENSION CAMPAIGN

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 involves a Chromium extension that uses AI-related branding to redirect browser search, targeting the Technology and Hospitality sectors. The threat actor's identity and specific malware families used are unknown. Priority should be given to auditing and least-privilege trusted third-party/B2B connections, as well as monitoring partner-account activity, due to the critical operational risk band. The campaign's ability to reach exfiltration poses a significant threat to affected organizations.

Threat Overview

The threat actor, whose identity is unknown, is utilizing a Chromium extension to carry out malicious activities, including keylogging, stealing web session cookies, and email collection. The central

vulnerability exploited is unknown, but the actor is using various techniques to achieve their goals, including browser session hijacking, phishing, and subverting trust controls.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, starting with the installation of a malicious Chromium extension, which then enables keylogging, web session cookie theft, and email collection. The priority technique is T1199 Trusted Relationship, which is the graph chokepoint. To mitigate this threat, the priority control is to "Audit and least-privilege trusted third-party/B2B connections; monitor partner-account activity."

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)

- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1114 Email Collection
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1176 Software Extensions
- T1567 Exfiltration Over Web Service
- T1185 Browser Session Hijacking
- T1090 Proxy
- T1528 Steal Application Access Token
- T1554 Compromise Host Software Binary
- T1199 Trusted Relationship
- T1056.002 GUI Input Capture
- T1566 Phishing
- T1553 Subvert Trust Controls
- T1573 Encrypted Channel
- T1132 Data Encoding
- T1213 Data from Information Repositories
- T1189 Drive-by Compromise
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1199 Trusted Relationship (centrality 0.2973).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4564; 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
FIN4	0.4564
PLATINUM	0.3689
Darkhotel	0.3501
Ajax Security Team	0.3227
RedCurl	0.3162

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	perplexity-ai[.]online
URL	hxxp://perplexity-ai[.]online/
URL	hxxp://perplexity-ai[.]online/*
URL	hxxp://perplexity-ai[.]online/search/
URL	hxxps://perplexity-ai[.]online/favicon[.]ico
URL	hxxps://perplexity-ai[.]online/search/

Type	Indicator
URL	hxxps://perplexity-ai[.]online/search?output=firefox&q=

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:** T1199 Trusted Relationship (initial-access)
- **Observed here:** the threat actor used T1189 Drive-by Compromise here as an alternative initial-access technique.
- **Projected pivot:** T1189 Drive-by Compromise (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

With T1199 Trusted Relationship blocked, the threat actor could preserve the same objective by pivoting to T1189 Drive-by Compromise, a technique observed in this campaign. Defensive countermeasure: Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.

- **Defensive countermeasure:** Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.