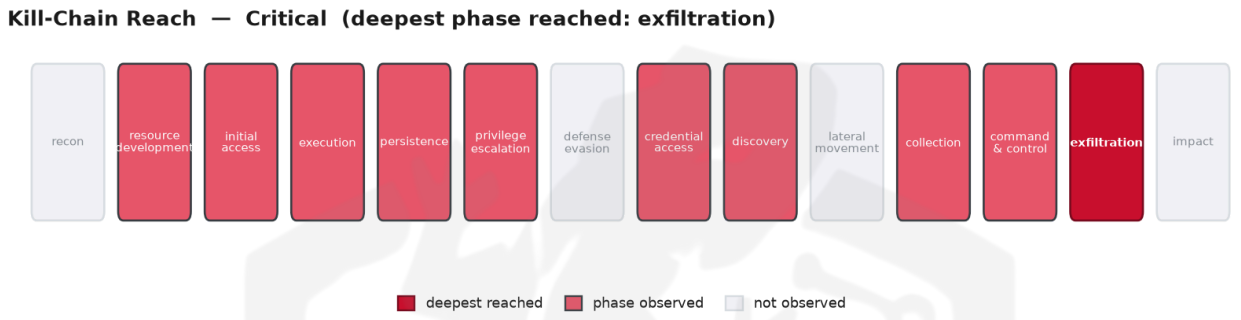
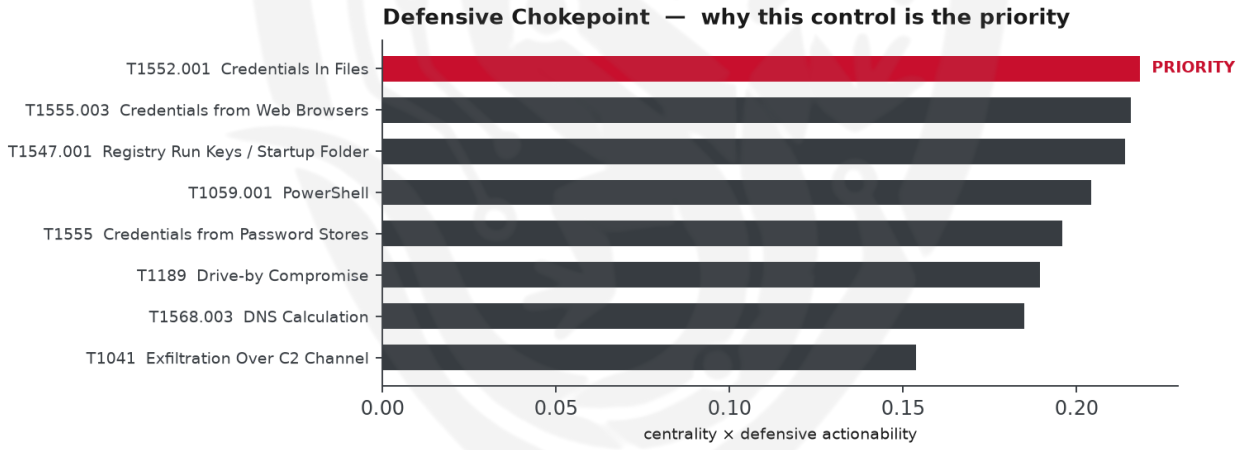
THREAT REPORT: UNKNOWN_ADVERSARY MALVERTISING CAMPAIGN

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 attributed to a malvertising campaign that has affected 29 organizations, utilizing malware families such as SectopRAT and StealC. The campaign's impact is significant, and priority should be given to removing secrets from code, configuration, and registry to mitigate the threat. The targeted sectors and countries are currently unknown, making it essential to focus on the technical aspects of the campaign to develop an effective defense strategy.

Threat Overview

The threat actor, whose identity is currently unknown, has been observed using various techniques, including scheduled tasks, web session cookie theft, and symmetric cryptography, to carry out their malicious activities. The malware families used, SectopRAT and StealC, have been identified as key

components of the campaign. The lack of information on the central CVE and targeted sectors makes it challenging to determine the full scope of the threat.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, starting with drive-by compromise and software packing, followed by deobfuscation and decoding of files, and ultimately leading to exfiltration over a command and control channel. The priority technique, T1552.001 Credentials In Files, is a critical chokepoint in this chain. To mitigate this threat, the priority control is to "Remove secrets from code/config/registry; deploy a secrets manager; scan repos and hosts for credentials."

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign has been observed to be hosted on providers such as RouterHosting LLC and Hostinger International Limited. Additionally, abuse.ch has corroborated the presence of the SectopRAT malware family, providing further evidence of the campaign's activities. However, according to AbuseIPDB, there are no 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)

- T1053.005 Scheduled Task
- T1539 Steal Web Session Cookie
- T1573.001 Symmetric Cryptography
- T1497.001 System Checks
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1036 Masquerading
- T1555.003 Credentials from Web Browsers
- T1552.001 Credentials In Files
- T1568.003 DNS Calculation
- T1608.005 Link Target
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1189 Drive-by Compromise
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow

Analytical Scores

- Priority technique (graph chokepoint): T1552.001 Credentials In Files (centrality 0.3119).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5112; 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	0.5112
RedCurl	0.4075
APT33	0.4063
Higaisa	0.406
BRONZE BUTLER	0.3901

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: SectopRAT.
- 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	104[.]194[.]133[.]210	AbuseIPDB 0% (NL) · AS14956 RouterHosting LLC
IP	107[.]189[.]24[.]67	AbuseIPDB 0% (NL) · AS14956 RouterHosting LLC
IP	107[.]189[.]26[.]86	AbuseIPDB 0% (NL) · AS14956 RouterHosting LLC

Type	Indicator	Context
IP	107[.]189[.]21[.]86	AbuseIPDB 0% (NL) · AS14956 RouterHosting LLC
IP	45[.]59[.]124[.]17	AbuseIPDB 0% (CH) · AS14956 RouterHosting LLC
IP	107[.]189[.]17[.]143	AbuseIPDB 0% (NL) · AS14956 RouterHosting LLC
IP	45[.]59[.]125[.]228	AbuseIPDB 0% (CH) · AS14956 RouterHosting LLC
IP	45[.]59[.]122[.]134	AbuseIPDB 0% (CH) · AS14956 RouterHosting LLC
IP	45[.]59[.]122[.]235	AbuseIPDB 0% (CH) · AS14956 RouterHosting LLC
IP	107[.]189[.]22[.]118	AbuseIPDB 0% (NL) · AS14956 RouterHosting LLC
IP	107[.]189[.]20[.]32	AbuseIPDB 0% (NL) · AS14956 RouterHosting LLC
IP	107[.]189[.]20[.]95	AbuseIPDB 0% (NL) · AS14956 RouterHosting LLC
IP	45[.]59[.]117[.]145	AbuseIPDB 0% (CH) · SectopRAT · AS14956 RouterHosting LLC
IP	45[.]59[.]114[.]190	AbuseIPDB 0% (CH) · SectopRAT · AS14956 RouterHosting LLC
IP	45[.]59[.]123[.]122	AbuseIPDB 0% (CH) · SectopRAT · AS14956 RouterHosting LLC
IP	45[.]59[.]117[.]67	AbuseIPDB 0% (CH) · SectopRAT · AS14956 RouterHosting LLC
IP	191[.]101[.]80[.]211	AbuseIPDB 0% (GB) · AS47583 Hostinger International Limited
IP	2[.]24[.]131[.]246	AbuseIPDB 0% (GB) · AS47583 Hostinger International Limited
IP	195[.]110[.]58[.]222	AbuseIPDB 0% (GB) · AS47583 Hostinger International Limited

Type	Indicator	Context
Domain	download-app[.]us	
Domain	5ca8758c-02d0-4a72-89c8-d468b66dda41[.]com	
Domain	claude[.]ai[.]download-app[.]us	
URL	hxxp://107[.]189[.]24[.]255	
Hash	04dcc1abb68aae9d3ae4901cc140dbb8	
Hash	71fdd6fb7f0acd3e9a6206851452e11b	
Hash	82011a9ff3692236df69427eb200ba05799205b0	
Hash	da7a5028b9694c406a881eb85e5acd8ea375a890	
Hash	1cd58cfba596da296ab1878d74023e00c399345a1b6c2a0e5446c53563f4e3bb	
Hash	1fe3646d27d286db8123297e06ae7badf3e26f352a04f91b6d82c28869a91664	
Hash	26bae4d7012bf59847ab4036a065419c3d4ca47e020479f55b3b2c6d0d21394a	
Hash	f8acb8f5cf88b77a4c27d7fd6856aa299bb178e85f9963c2fbd447d818da3ed0	
Hash	fd826215add30c1319eefa291b6eaf8ddfa7720cfe816c49aef6fe8a88de7939	

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

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:** T1552.001 Credentials In Files (credential-access)
- **Observed here:** the threat actor used T1539 Steal Web Session Cookie here as an alternative credential-access technique.
- **Projected pivot:** T1539 Steal Web Session Cookie (credential-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to Steal Web Session Cookie (T1539) in an attempt to maintain access and achieve their objectives, potentially by exploiting weaknesses in browser session management to intercept or manipulate session cookies. This technique may allow the actor to bypass traditional authentication mechanisms and move laterally within the network. To counter this potential move, the mandated defensive control is to protect and monitor browser session-cookie stores; enforce short session lifetimes and re-auth; alert on cookie theft patterns.

- **Defensive countermeasure:** Protect and monitor browser session-cookie stores; enforce short session lifetimes and re-auth; alert on cookie theft patterns.