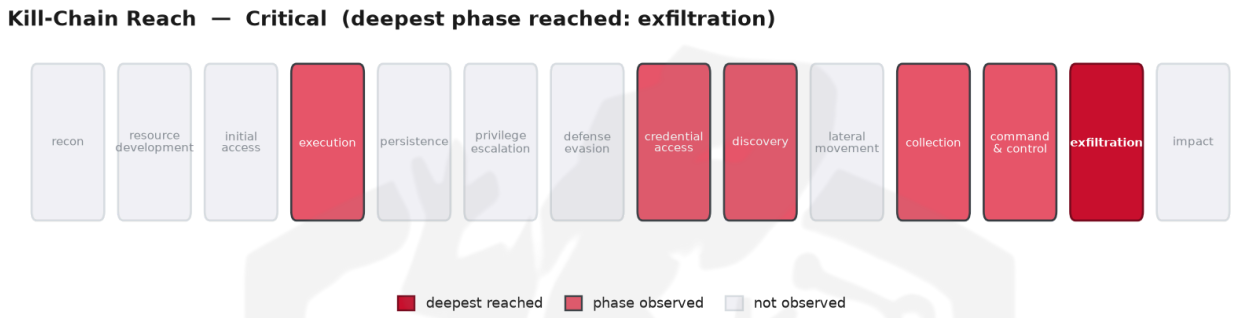
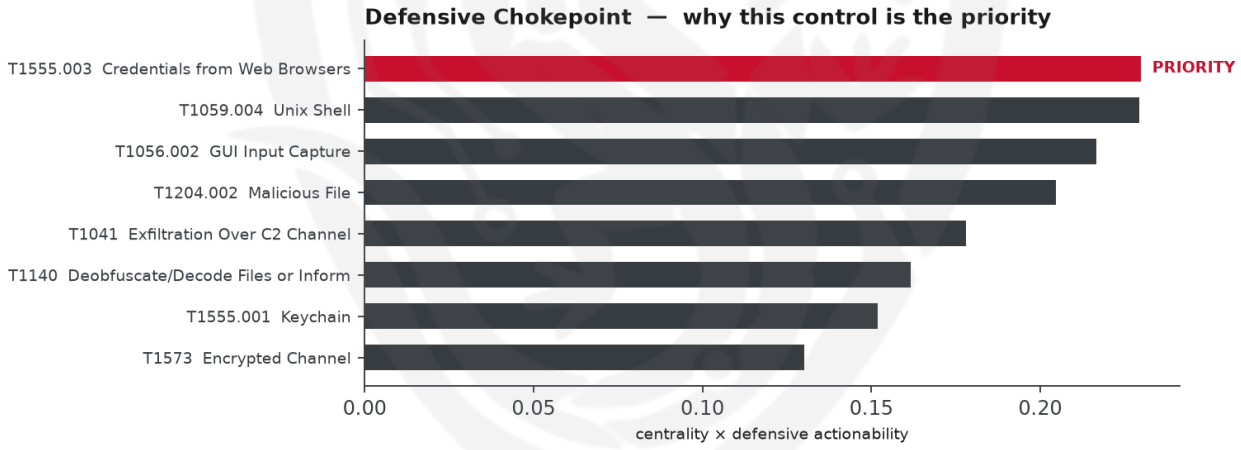
THREAT REPORT: MENTALPOSITIVE'S MACSYNC STEALER CAMPAIGN

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 source attributes this activity to the threat actor mentalpositive, which is operating the MacSync Stealer and Mac.c malware families. No specific vulnerability is identified, and the target geography and sectors are not disclosed. The campaign harvests credentials from web browsers among other data-stealing behaviors. Priority should be given to restricting access to browser credential stores, alerting on reads of Login Data or cookies files by non-browser processes, and enforcing disk encryption.

Threat Overview

mentalpositive deploys the MacSync Stealer and Mac.c malware families. The activity does not cite a particular CVE, and the victim profile is unspecified in the source.

Attack Chain and Priority Control

The observed chain begins with system information discovery (T1082) and automated collection (T1119), proceeds through credential harvesting from web browsers (T1555.003) and keychain access (T1555.001), and culminates in exfiltration over the C2 channel (T1041) using encrypted web protocols (T1573, T1071.001). The chokepoint technique is **T1555.003 Credentials from Web Browsers**, and the recommended control is: **Restrict access to browser credential stores; alert on reads of Login Data / cookies files by non-browser processes; enforce disk encryption.**

Infrastructure and Corroboration

Third-party enrichment notes that no hosting provider or ASN information is available for the malicious infrastructure. Abuse.ch corroborates the presence of related malware families MacInstaller, Unknown Stealer, and Unknown malware. No indicators meet the ≥80 % confidence threshold on AbuseIPDB.

Technical Appendix

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

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

- T1113 Screen Capture
- T1132.001 Standard Encoding
- T1036.005 Match Legitimate Resource Name or Location
- T1555.001 Keychain
- T1204.002 Malicious File
- T1119 Automated Collection
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1555.003 Credentials from Web Browsers
- T1041 Exfiltration Over C2 Channel
- T1056.002 GUI Input Capture
- T1059.004 Unix Shell
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1070.004 File Deletion
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1555.003 Credentials from Web Browsers (centrality 0.3282).

- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4543; 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
Tropic Trooper	0.4543
RedCurl	0.4389
BRONZE BUTLER	0.4202
TA551	0.417
APT42	0.4084

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: MacInstaller, Unknown Stealer, Unknown malware.
- 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
Domain	tintingsd[.]com	
Domain	houstongaragedoorinstallers[.]com	
Domain	pressureulcerlawyer[.]com	
Domain	mansfieldpediatrics[.]com	Unknown Stealer

Type	Indicator	Context
Domain	helxiagent[.]com	
Domain	lumenagnet[.]com	
Domain	blzaeagent[.]com	Unknown malware
Domain	nailscanai[.]com	MacInstaller
Domain	glowmedaesthetics[.]com	
Domain	wechatstablecoin[.]com	
Domain	numericagent[.]com	
Domain	jacksonvillemma[.]com	
Domain	lalandscapelighting[.]com	
Domain	harveylewisinsuranceagency[.]com	
URL	hxxp://jacksonvillemma[.]com/curl/7980485fb1e0b1b1d6307a92b5750c7055bc53b662005cbaa662ac634984363d	
URL	hxxp://jacksonvillemma[.]com/dynamic?txd=7980485fb1e0b1b1d6307a92b5750c7055bc53b662005cbaa662ac634984363d	
URL	hxxp://jacksonvillemma[.]com/gate?buildtxd=7980485fb1e0b1b1d6307a92b5750c7055bc53b662005cbaa662ac634984363d	
Hash	5190ef1733183a0dc63fb623357f56d6	
Hash	277acd8e241c1341852ebcd401203ecc	
Hash	7d28507870e94b809f25883dc9dae838549ddfac	
Hash	2728a7d444cd65550f652a8c66eaced0fe6d0389161f86393ab73da8f446a362	
Hash	7980485fb1e0b1b1d6307a92b5750c7055bc53b662005cbaa662ac634984363d	

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:** T1555.003 Credentials from Web Browsers (credential-access)
- **Observed here:** T1555.003 Credentials from Web Browsers was the only credential-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1003 OS Credential Dumping (credential-access)
- **Basis:** of the 21+ groups that use Credentials from Web Browsers, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

With T1555.003 Credentials from Web Browsers blocked, mentalpositive could preserve the same objective by pivoting to T1003 OS Credential Dumping, a technique disproportionately paired with it across tracked groups. Defensive countermeasure: Protect LSASS (RunAsPPL, Credential Guard); alert on LSASS handle access; disable WDigest.

Also plausible (same tactic): T1552 Unsecured Credentials (n=15, lift 3.5), T1110 Brute Force (n=12, lift 2.3)

Detection and hardening for the pivot (T1003 OS Credential Dumping)

- **Telemetry:** Sysmon (process access); EDR credential-theft telemetry
- **Detect:**
  - Sysmon 10 (process access) targeting lsass.exe with suspicious access masks
  - Access to ntds.dit / SAM / SYSTEM hives; vssadmin/shadow-copy abuse
  - comsvcs.dll MiniDump, procdump, or reg save of security hives
- **Harden:**
  - Enable Credential Guard and LSA protection (RunAsPPL)
  - Restrict debug privilege; tiered admin to limit credential exposure
- **MITRE:** M1043 Credential Access Protection, M1028 Operating System Configuration, M1026 Privileged Account Management, M1017 User Training · DS0009 Process, DS0022 File, DS0024 Windows Registry