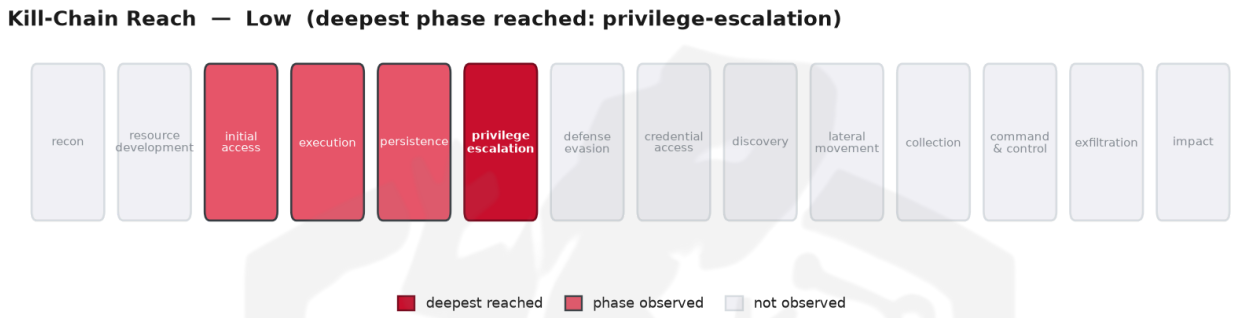
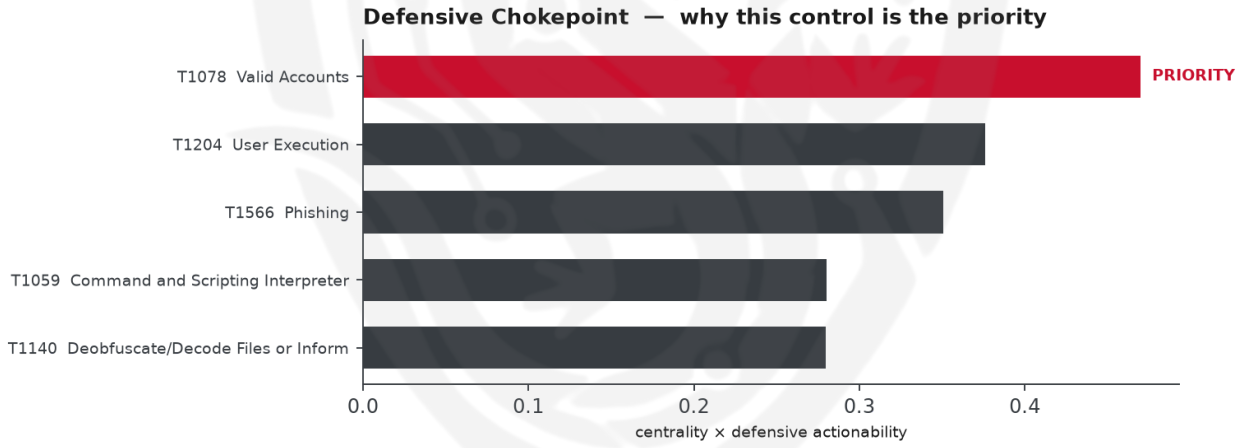
THREAT REPORT: PAMSTEALER MACOS INFOSTEALER CAMPAIGN

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 the PamStealer malware, a Rust-based macOS infostealer that validates credentials through PAM. The targeted country and sectors are not specified due to insufficient data. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The threat actor's identity remains unknown due to insufficient information.

Threat Overview

The threat actor, whose identity is not specified, is associated with the PamStealer malware family. This malware exploits an unknown vulnerability to gain access to victim systems. The victimology of this campaign is not well-defined due to a lack of information on the targeted country and sectors.

Attack Chain and Priority Control

The techniques inferred from the report include command and scripting interpreter, valid accounts, deobfuscate/decode files or information, user execution, and phishing. The priority technique is T1078 Valid Accounts, which serves as a chokepoint in the attack chain. To counter this, the lead control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs observed in this campaign. Additionally, 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%.

Technical Appendix

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

Observed Techniques (ATT&CK, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1059 Command and Scripting Interpreter - T1078 Valid Accounts - T1140 Deobfuscate/Decode Files or Information - T1204 User Execution - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.47).
- Operational risk: Low (score 0.297, reaches privilege-escalation).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4743; 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
TA459	0.4743

Historical Profile	Behavioural Overlap
APT30	0.4472
Malteiro	0.4104
TA577	0.4045
Nomadic Octopus	0.4045

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	avenger-sync[.]live
Domain	api[.]sync-master[.]online
Domain	maccyapp[.]com
Domain	api[.]live-updates[.]online
URL	hxxp://api[.]live-updates[.]online/v1
URL	hxxp://api[.]live-updates[.]online/v2
URL	hxxp://api[.]sync-master[.]online/v1
URL	hxxp://api[.]sync-master[.]online/v3
URL	hxxp://avenger-sync[.]live/api/sync
URL	hxxps://api[.]live-updates[.]online/v1
URL	hxxps://api[.]live-updates[.]online/v2
URL	hxxps://api[.]sync-master[.]online/v1
URL	hxxps://api[.]sync-master[.]online/v3
URL	hxxps://avenger-sync[.]live/api/sync
URL	hxxps://maccyapp[.]com

Type	Indicator
Hash	bae0005a0bf0d467a672600833eeed92
Hash	e291f991d4bd616203b291a36121dc8b0c15f509
Hash	06fdd1d97df1105c542ddb881d751b659d555b5522c266f6364dae9f350fcfd0
Hash	2b512f6c393edad89a89ecafe26cd23b71cfdd271c10522f8dba98997ebf39bb
Hash	36d46ac7123e0cef04f179d88e590891c7e7c64ec5a77df4512cb485e40286da
Hash	60df952153696d46a09774e44ca602393c6829f9e2c2ec4f95d571f9846242a8
Hash	96c8ad78f6ccdf83d3dcabfd33ba563f7995f7237fe825de1eefd340821abdf3
Hash	ab3a14096851cc18a253c1cd1c25df74f2cf23eb29051784ce47f9fc318f0f22
Hash	bb01f3c36110d2cc31ae51c4ff2f17be19bea625755b5339680431fab98616df
Hash	ca7f5c0668f1a871523d485e42884c3b98910117d7ca17c8b3c3b3744a936e0f
Hash	e8b18c420669deb8fc6f69e74146e499057c3c77436ac6ca54af37befa9ddaa5
Hash	f48b69e4b7fb4d53de25b4c9be8e8dbe0999c10d5306e01aa08e1761fc3dedbe
Hash	ff20b429cb1c89e1cdb6734b00cc8cf021d2d13fd686bbc70709b3dd549285d2

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:** T1078 Valid Accounts (initial-access)
- **Observed here:** T1078 Valid Accounts was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1053 Scheduled Task/Job (execution)
- **Basis:** of the 31+ groups that use Valid Accounts, this pairing runs 1.4x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1053 Scheduled Task/Job to maintain persistence and evade detection, as this technique allows them to execute malicious tasks under the guise of legitimate system maintenance, potentially leveraging the existing valid account access that was previously blocked. This technique may be particularly appealing to the actor because it enables them to schedule tasks to run at specific intervals, making it harder to distinguish between benign and malicious activity. The defensive control to

counter this would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1072 Software Deployment Tools (n=6, lift 2.3)

Detection and hardening for the pivot (T1053 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
  - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
  - Restrict schtasks/at to administrators; disable the legacy at.exe
  - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File