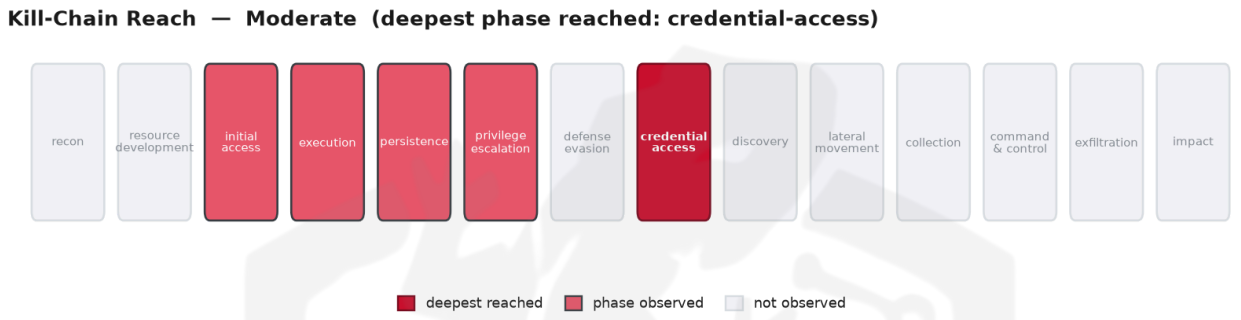
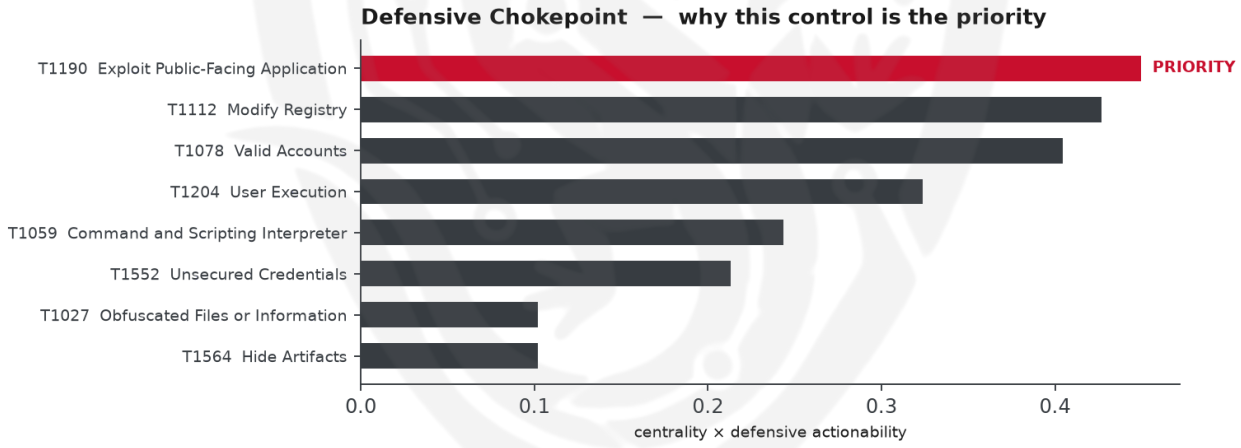
# THREAT REPORT: CRASHSTEALER MACOS INFOSTEALER CAMPAIGN

## 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 CrashStealer malware, a C++ macOS infostealer posing as a crash reporter. The targeted country and sectors are not specified due to insufficient data. Priority should be given to defensive actions against this threat, particularly focusing on public-facing applications. The threat actor behind this campaign remains unattributed.

## Threat Overview

The threat actor, responsible for the CrashStealer malware, exploits various techniques to achieve their goals. The malware family involved is CrashStealer, with the central CVE and targeted country being data insufficient. The techniques inferred from the report include obfuscated files or information, command and

scripting interpreter, valid accounts, modify registry, exploit public-facing application, user execution, unsecured credentials, and hide artifacts.

## Attack Chain and Priority Control

The attack chain involves a series of techniques, including exploiting public-facing applications, which is identified as the priority technique (T1190). This chokepoint is critical in the attack chain. The priority action is to patch the affected public-facing CVE immediately, apply a WAF virtual patch, and restrict management interfaces to VPN-only.

## Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed, malware families corroborated by abuse.ch, or indicators at a high confidence level from AbuseIPDB, as all these metrics are reported as not applicable or below the threshold.

---

## 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.* - T1027 Obfuscated Files or Information - T1059 Command and Scripting Interpreter - T1078 Valid Accounts - T1112 Modify Registry - T1190 Exploit Public-Facing Application - T1204 User Execution - T1552 Unsecured Credentials - T1564 Hide Artifacts

### Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.4789).
- Operational risk: Moderate (score 0.424, reaches credential-access).

### Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3536; 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 |
|---|---|
| BlackOasis | 0.3536 |
| TA577 | 0.3198 |
| Nomadic Octopus | 0.3198 |
| Gallmaker | 0.3198 |
| FIN4 | 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 | Context |
|---|---|---|
| Domain | cohezo[.]com | |
| Domain | werknova[.]co | malware_download |
| Domain | endpoint-api-v1[.]com | |
| Domain | werkbit[.]io | |
| Domain | cohezo[.]io | |
| Domain | collabox[.]uk | |
| Domain | cordinex[.]io | |
| Domain | icky-lyrical[.]com | |
| URL | hxxps://endpoint-api-v1[.]com/login | |
| URL | hxxp://endpoint-api-v1[.]com/d/f1b24e/download | |

| Type | Indicator | Context |
|---|---|---|
| URL | hxxps://cohezo[.]com/calendar/0f4df3a7-5914-4245-a616-311ca554ee0c | |
| URL | hxxps://cohezo[.]io/download?invite=OX-3SEY-64KI | |
| URL | hxxps://collabox[.]uk/calendar/1cdf0e32-9ba0-4be5-8823-39a2e6364a20 | |
| URL | hxxps://cordinex[.]io/download?invite=MZ-AB95-QD50 | |
| URL | hxxps://endpoint-api-v1[.]com/d/f1b24e | |
| URL | hxxps://icky-lyrical[.]com | |
| URL | hxxps://icky-lyrical[.]com/api/download?access_code= | |
| URL | hxxps://icky-lyrical[.]com/storage/secure/Cohezo/windows/small/69cf7d0ea7cfd/cohezo_setup[.]msi | |
| URL | hxxps://icky-lyrical[.]com/storage/secure/werkbit/mac | |
| URL | hxxps://werkbit[.]io | |
| URL | hxxps://werknova[.]co/calendar/90f99c64-9fcc-451c-bae1-0b095c04e5c8 | |
| Hash | ed33a3c8d9e861515623a73b27ea4913 | |
| Hash | 8063358813c37992cfe3fcd92038a0334c14353d | |
| Hash | 08801f81960cd8c1077b4aa2e8124840d56a272842fdcc73263c9968e787e0bd | |
| Hash | 09bd60ce11ee4324e2052a439a08676e31aac787edda3f9bd02325390b5db2d2 | |
| Hash | 3a9d703ba7f7564399365db7ab8b04238806ef7a53df0b6822f32b80bf0f5a80 | |
| Hash | 4ed199e27a4dc193468569b221b19180e5ae95cab8df84d92e082b68d33672f5 | |
| Hash | 5bb675af9c403896d5f31611cf42304cf482d16f6f3ab6a868a9aa853aa5c179 | |
| Hash | 81ef05cc4d07cd22cd7cd7099f278dd9b9a3ae8ad4770b3d387892e1c6cfb7d7 | |
| Hash | 88334ea00ff94a366cd2a9283a508b97c269839894fddfe91913f3d92e95b6ab | |
| Hash | a1966a6d6f54a025f30d55571d21d6537977ca73ffa734c13494b9c806cd7007 | |
| Hash | f3857c0b84a24b7fc912d55f8b14c67c23d5837b1a6932164d5d62273d4affeb | |
| Hash | fba5bbe87fa351eedf2f3c16653cc9e4196d73604529bb50a609e2d3ebf1828b | |

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:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** T1190 Exploit Public-Facing Application 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 23+ groups that use Exploit Public-Facing Application, this pairing runs 1.5x 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 by leveraging the Windows Task Scheduler to execute malicious code at set intervals, which may allow them to regain a foothold in the system. This technique in particular could be appealing as it enables the actor to blend in with legitimate system activity and may be less conspicuous than exploiting a public-facing application. The defensive control to counter this potential pivot 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=8, lift 1.8), T1574 Hijack Execution Flow (n=13, lift 1.4)

**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