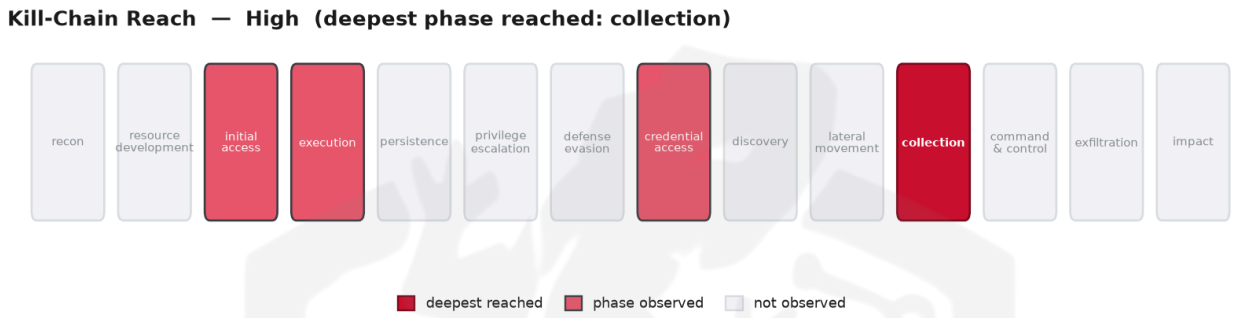
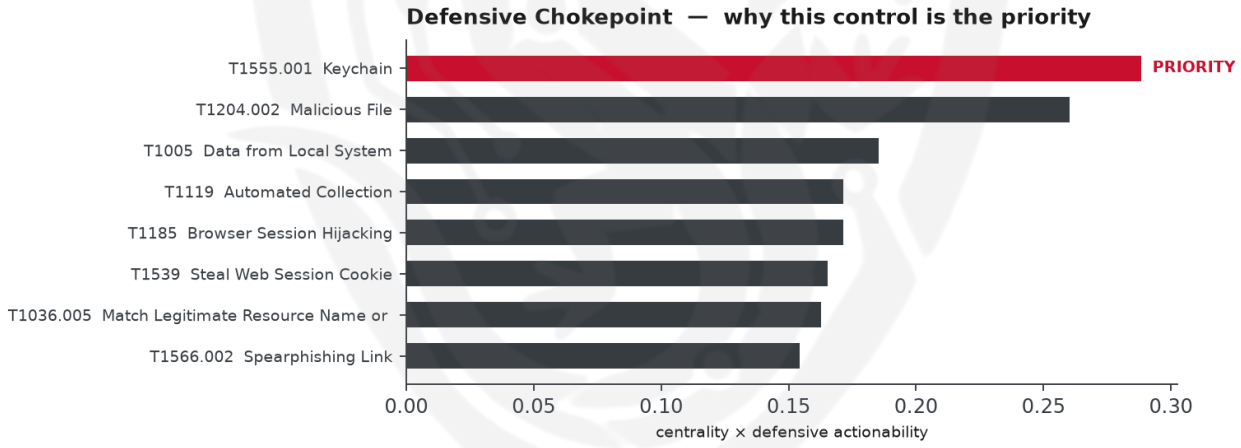
THREAT REPORT: UNKNOWN_ADVERSARY CLICKFIX CAMPAIGN

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 delivers a macOS infostealer via DMG, targeting unknown countries and sectors, with a priority defensive action to restrict access to browser/OS credential stores. The threat actor utilizes various malware families, including AMOS, Atomic macOS Stealer, Odyssey, and NNApp. Priority should be given to defending against the exploitation of these malware families. The campaign's impact is considered high due to its ability to reach the collection stage.

Threat Overview

The threat actor, observed in the ClickFix campaign, utilizes a range of malware families, including AMOS, Atomic macOS Stealer, Odyssey, and NNApp, to deliver a macOS infostealer via DMG. The campaign

exploits various techniques, including obfuscated files, automated collection, and browser session hijacking, to steal sensitive information. The victimology of this campaign is currently unknown.

Attack Chain and Priority Control

The observed techniques in the ClickFix campaign form a complex attack chain, involving techniques such as DLL, obfuscated files, and match legitimate resource name or location. The priority technique in this chain is T1555.001 Keychain, which is the graph chokepoint. To defend against this campaign, the priority control is to: Restrict access to browser/OS credential stores; alert on credential-vault access; enforce disk encryption.

Infrastructure and Corroboration

The malicious infrastructure associated with the ClickFix campaign is hosted on providers such as Omegatech LTD and Femo IT Solutions Limited, as observed in third-party enrichment. Additionally, abuse.ch has corroborated the presence of malware families such as ClearFake and unknown malware. However, according to AbuseIPDB, the confidence level of the indicators is below 80%, with the highest confidence seen being 29%.

Technical Appendix

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

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

- T1574.001 DLL
- T1027 Obfuscated Files or Information
- T1036.005 Match Legitimate Resource Name or Location
- T1119 Automated Collection
- T1555.001 Keychain
- T1005 Data from Local System
- T1185 Browser Session Hijacking
- T1204.002 Malicious File
- T1539 Steal Web Session Cookie
- T1566.002 Spearphishing Link

Analytical Scores

- Priority technique (graph chokepoint): T1555.001 Keychain (centrality 0.4118).
- Operational risk: High (score 0.562, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4667; 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
Whitefly	0.4667
Mofang	0.4303
Evilnum	0.4146
BlackTech	0.4041
Sidewinder	0.3984

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 29%.
- Malware families corroborated by abuse.ch: ClearFake, 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
IP	178[.]16[.]52[.]101	AbuseIPDB 29% (DE) · ClearFake · AS202412 Omegatech LTD
IP	196[.]251[.]107[.]171	AbuseIPDB 0% (DE) · AS214351 Femo IT Solutions Limited
Domain	fewfwfwfwfwf[.]info	
Domain	svs-verificationdate[.]beer	Unknown malware
Hash	25b6fc4f9c54a28ba7bfc4dfeafb62c99b59ea6f0d17679219b876b321965095	
Hash	067ad6221b2224d5cdb64e51c5516132d820cf4d7edf9ec170643943e79c04b7	

Type	Indicator	Context
Hash	d6f479736ba55d3c4e895c4940d035cf772f3192fb8dc496f09a801aed16d970	
Hash	833008c03d40422192051584d829d730497108bef31751cceb0cc043dd96bbfb	
Hash	8111edf01ac6cb5c77e249d4e84fd92a85b5e89c2e2bef92fbe00b6f1cc2aa8e	
Hash	f0038a5f46720da5982b6984ceef10cf99359432e102b12a0b0657498d36f670	

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:** T1555.001 Keychain (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 threat actor could pivot to Steal Web Session Cookie (T1539) to maintain access to sensitive information, potentially by exploiting weaknesses in browser security or user behavior, if they were previously relying on Keychain (T1555.001) for credential theft. This technique may allow the actor to bypass traditional authentication mechanisms and access restricted resources, which would likely be a high-priority objective. To counter this, 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.