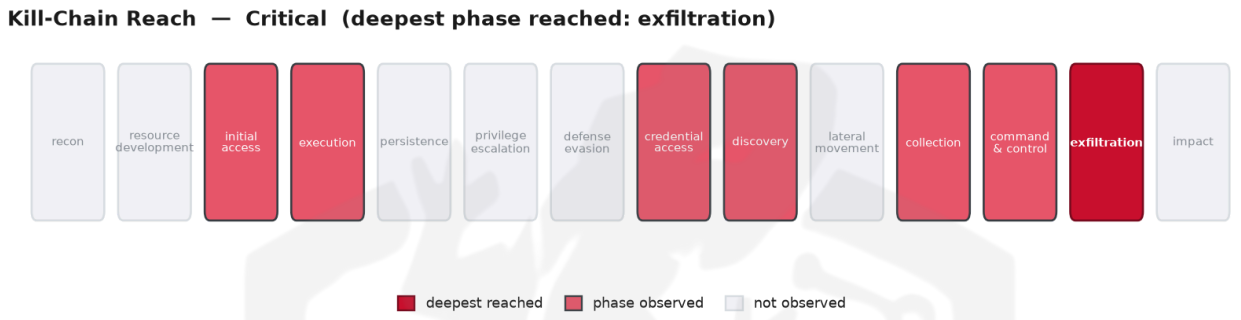
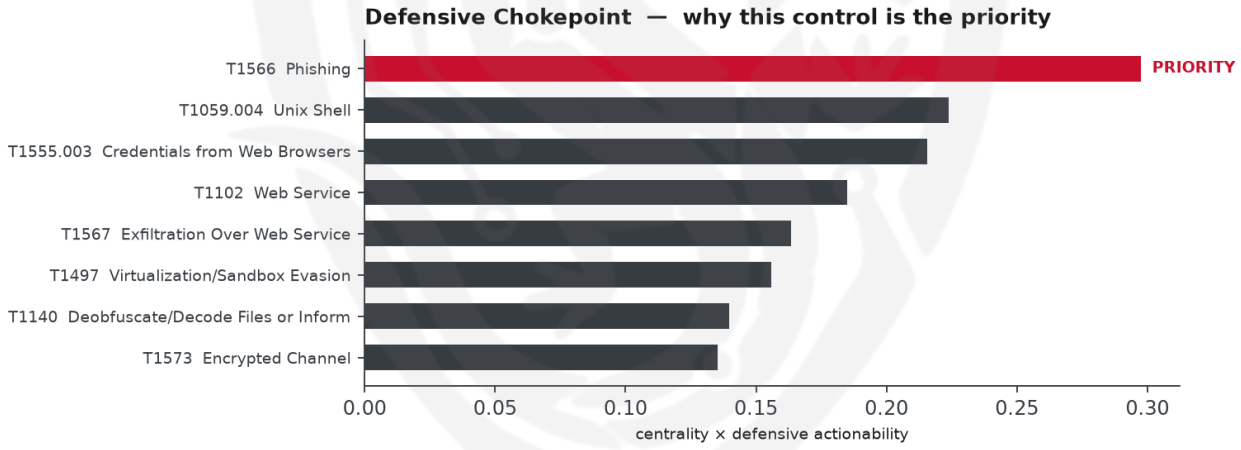
THREAT REPORT: MACSYNC AND ATOMIC STEALER CAMPAIGN

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 observed cluster of activity involves the use of MacSync, Atomic Stealer, and AMOS malware families to target macOS systems. The threat actor's identity and specific targets are not well understood, but the campaign's techniques and tactics indicate a high level of sophistication. Priority should be given to defending against social-engineering delivery methods, as the campaign relies heavily on phishing and other deceptive tactics. The operational risk band for this campaign is considered Critical, as it has been observed to reach the exfiltration stage.

Threat Overview

The threat actor, whose identity is not well understood, is utilizing a range of malware families, including MacSync, Atomic Stealer, and AMOS, to carry out their campaign. The campaign involves the exploitation

of various techniques, including stealing web session cookies, keychain access, and system information discovery. The victimology of the campaign is not well understood, but it is clear that the threat actor is targeting macOS systems.

Attack Chain and Priority Control

The observed techniques used by the threat actor can be described as a chain of events, starting with phishing and other social-engineering tactics, followed by the use of malicious files, automated collection, and system information discovery. The priority technique in this chain is T1566 Phishing, which serves as the initial entry point for the campaign. To defend against this campaign, the following control is recommended: Harden against social-engineering delivery across email, links and voice/callback lures: attachment sandboxing and link rewriting, block macro-enabled Office docs from the internet zone, train users to verify unexpected requests out-of-band, deploy a report-phish button, and enforce phishing-resistant MFA.

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs used by the threat actor, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with a confidence level of 80% or higher 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, expert-tagged by source)

- T1539 Steal Web Session Cookie
- T1555.001 Keychain
- T1204.002 Malicious File
- T1119 Automated Collection
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1567 Exfiltration Over Web Service
- T1555.003 Credentials from Web Browsers
- T1497 Virtualization/Sandbox Evasion
- T1102 Web Service
- T1566 Phishing
- T1059.004 Unix Shell
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1132 Data Encoding
- T1027.002 Software Packing

- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2974).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4649; 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
Inception	0.4649
Malteiro	0.4305
Dark Caracal	0.4305
APT37	0.4286
ZIRCONIUM	0.4183

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	applefilevault[.]com
Domain	apricotfilepoint[.]com
Domain	bananafastfile[.]com
Domain	lemonfilewave[.]com
Domain	limefilescope[.]com

Type	Indicator
Domain	mangocloudfile[.]com
Domain	orangesmartfile[.]com
Domain	cloudfilebridge[.]com
Domain	filecedarwallet[.]online
Domain	filecopperbasket[.]sbs
Domain	filecrimsonsignal[.]online
Domain	filemarblegarden[.]sbs
Domain	fileoceanhammer[.]sbs
Domain	filerubyfolder[.]sbs
Domain	filevelvettractor[.]sbs
Domain	syncdatavault[.]com
Domain	cloudsendhub[.]com

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:** T1566 Phishing (initial-access)
- **Observed here:** T1566 Phishing 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:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 38+ groups that use Phishing, this pairing runs 1.6x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1203 Exploitation for Client Execution to maintain their objective by leveraging vulnerabilities in client applications, such as browsers or Office software, which may be exposed through user interaction or unpatched flaws, potentially allowing them to execute malicious code on the client-side. This technique may be particularly appealing as a follow-up to phishing attempts, as it can exploit the same user interaction vectors, such as tricking users into opening malicious documents or clicking on links. The defensive countermeasure to mitigate this would be to patch client applications, enable exploit mitigations such as ASLR, DEP, and CFG, and implement application isolation.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=43, lift 1.3), T1106 Native API (n=18, lift 1.6)

Detection and hardening for the pivot (T1203 Exploitation for Client Execution)

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**
  - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs
  - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash
  - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
  - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
  - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015 Application Log