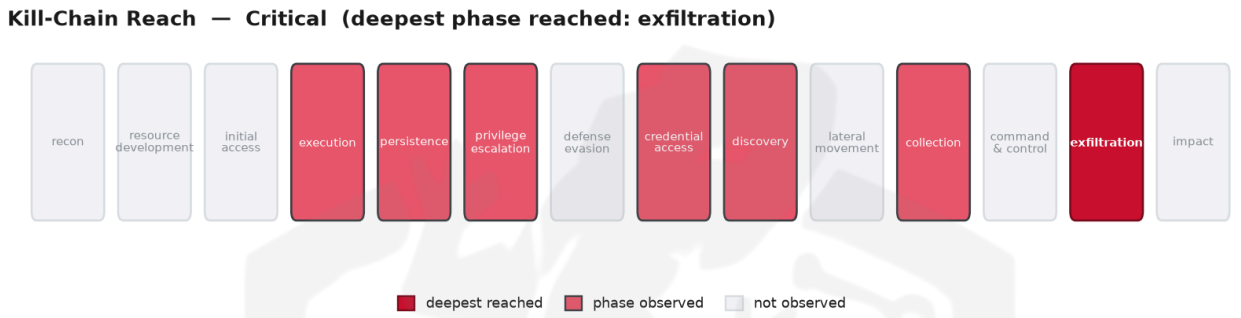
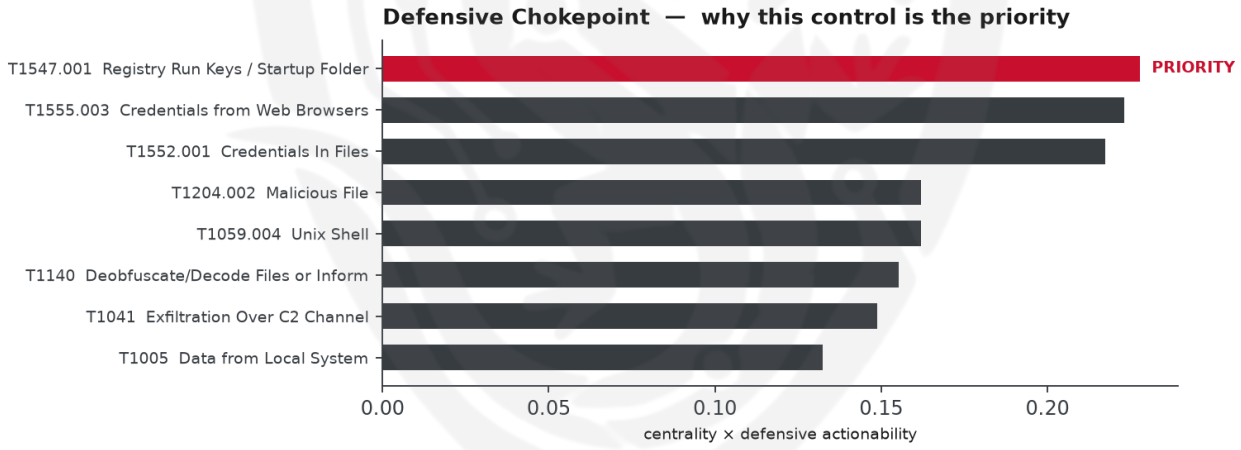
THREAT REPORT: UNKNOWN_ADVERSARY MALICIOUS ACTIVITY

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 has been identified as utilizing the MacSync Stealer malware family to target unknown sectors and countries. The threat actor's techniques include various methods of data collection and exfiltration, with a priority defensive action being to audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. Priority should be given to monitoring for suspicious activity, particularly the creation of .lnk or script files in Startup by browser or email temporary paths. The operational risk band for this threat is Critical, indicating a high level of potential harm.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, is utilizing the MacSync Stealer malware family to carry out their operations. The central vulnerability exploited is currently unknown, but

the techniques used include Sharepoint, Email Collection, Keychain, and other methods of data collection and exfiltration. The victimology of this threat is also unknown, but the use of MacSync Stealer suggests a focus on stealing sensitive information.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a chain of attack that includes data collection, exfiltration, and other malicious activities. The priority technique, or graph chokepoint, is T1547.001 Registry Run Keys / Startup Folder, which is a critical point in the attack chain. To mitigate this threat, the priority control is to "Audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries; alert on .lnk or script creation in Startup by browser/email temp paths."

Infrastructure and Corroboration

The infrastructure used by the threat actor is not well-defined, with no specific hosting providers or ASNs observed. However, abuse.ch has corroborated the presence of Unknown Stealer and Unknown malware, which may be related to the MacSync Stealer family. Additionally, AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, 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)

- T1213.002 Sharepoint
- T1114 Email Collection
- 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
- T1555.003 Credentials from Web Browsers
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1057 Process Discovery
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1059.004 Unix Shell
- T1027 Obfuscated Files or Information
- T1070.004 File Deletion
- T1564.001 Hidden Files and Directories

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2399).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4811; 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
RedCurl	0.4811
Inception	0.4036
APT3	0.4014
Tropic Trooper	0.3931
Molerats	0.3922

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: 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	buywx[.]com	
Domain	cincycarpetcleaning[.]com	
Domain	homeinspectionsdelaware[.]com	Unknown Stealer
Domain	vacationrentalvirginia[.]com	Unknown Stealer

Type	Indicator	Context
Domain	sonyda[.]com	
Domain	trailblazehealth[.]com	Unknown Stealer
Domain	sdlasik[.]com	
Domain	pine-1[.]com	
Domain	toledotreeservices[.]com	
Domain	olympiapetemergency[.]com	
Domain	newjerseypetsitter[.]com	
Domain	charlottefilmstudios[.]com	
Domain	seattlefilmstudios[.]com	
Domain	alluringsites[.]com	
Domain	jerryshvac[.]com	
Domain	customroofingcontractors[.]com	Unknown malware
Domain	kidsjumpandplay[.]com	
Domain	floridakitchencabinet[.]com	
Domain	journey71[.]com	
Domain	realtorsmichigan[.]com	
Domain	fullcolorprinters[.]com	
Domain	nationalspacecouncil[.]com	
Domain	miamidadenotary[.]com	
Domain	lalandscapelighting[.]com	
Domain	aisolutions247[.]com	
Domain	healthcareqai[.]com	
Domain	briskinternet[.]com	Unknown Stealer · malware_download
Domain	belldredgingpump[.]com	
Domain	kylesplumbing[.]com	

Type	Indicator	Context
Domain	modernhomeai[.]com	
Domain	coeragent[.]com	
Domain	beachjiujitsu[.]com	
Domain	bcrealestateagency[.]com	
Domain	fractocode[.]com	
Domain	houstonpestcontrolcompany[.]com	
Domain	whichitaautosales[.]com	
Domain	3plfast[.]com	
Domain	aidevmaster[.]com	
Domain	dallasoverheaddoors[.]com	
Domain	dualverify[.]com	

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:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Observed here:** T1547.001 Registry Run Keys / Startup Folder was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1053 Scheduled Task/Job (persistence)
- **Basis:** 37 of 170 documented groups that use Registry Run Keys / Startup Folder also use Scheduled Task/Job (conditional 0.64, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

The actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and achieve their objective, potentially by creating a new scheduled task that appears benign, in an attempt to evade detection. This technique may be particularly effective if the actor can blend their malicious task with legitimate system tasks, making it harder to distinguish. To counter this, the defensive control would involve alerting on new scheduled tasks (Event ID 4698); restricting schtasks/at to admins; and baselining legitimate task creators.

Also plausible (same tactic): T1078 Valid Accounts (n=27, lift 1.2), T1543 Create or Modify System Process (n=18, lift 1.8)

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