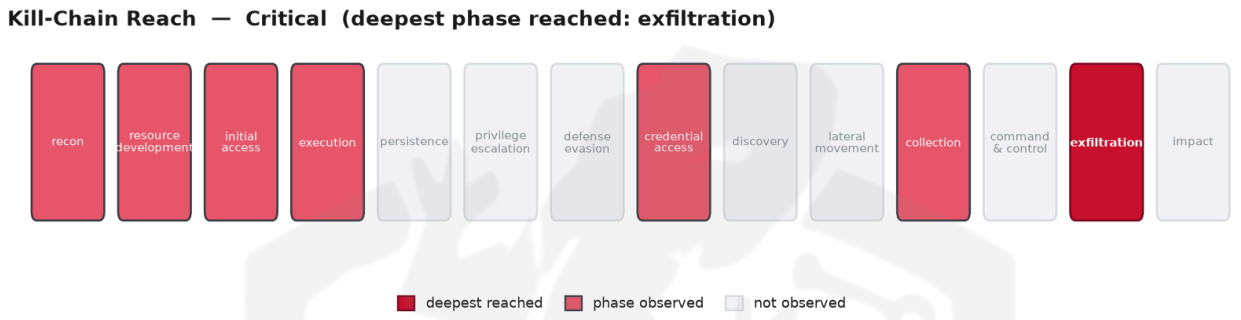
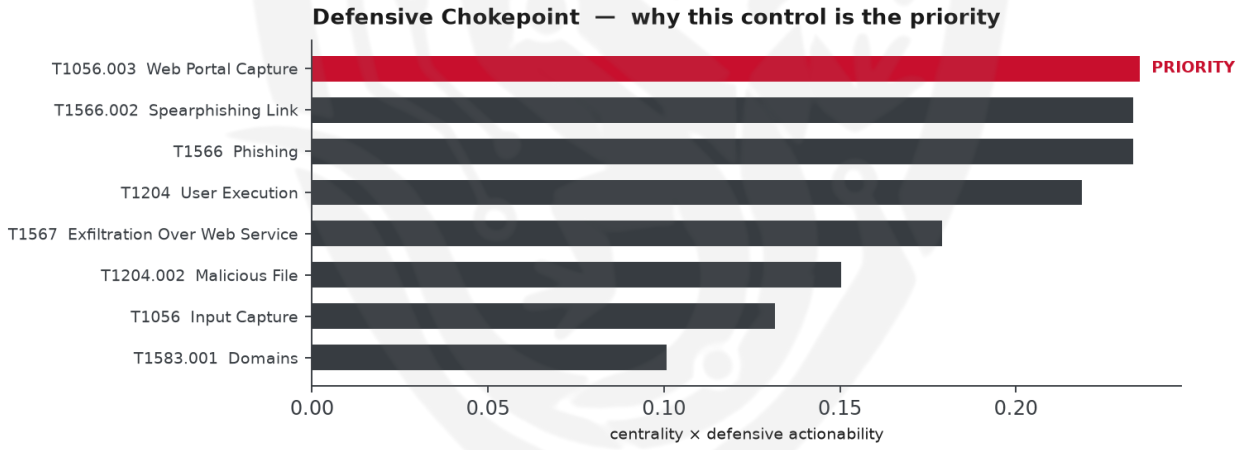
THREAT REPORT: UNKNOWN_ADVERSARY PHISHING CAMPAIGN

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 is targeting individuals in Chile, with a focus on phishing and web session cookie theft. The threat actor is utilizing various techniques to compromise accounts and exfiltrate data. Priority should be given to defending against web portal capture and restricting accessibility to prevent further compromise. The campaign's ability to reach exfiltration poses a critical operational risk.

Threat Overview

The threat actor is conducting a phishing campaign, impersonating the PasasteSinTAG portal, and exploiting various techniques to steal web session cookies and compromise email accounts. The campaign is targeting individuals in Chile, but the specific sectors affected are unknown. The techniques used include phishing, spearphishing, and drive-by compromise, among others.

Attack Chain and Priority Control

The observed techniques form a chain of events, starting with phishing and spearphishing, followed by the acquisition of infrastructure, and ultimately leading to exfiltration over web services. The priority technique is T1056.003 Web Portal Capture, which serves as a chokepoint in the attack chain. To mitigate this threat, the priority control is to "Alert on keylogging hooks and API-input capture; restrict accessibility/hook installation."

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs observed, and no malware families have been corroborated by abuse.ch. 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)

- T1583 Acquire Infrastructure
- T1539 Steal Web Session Cookie
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1586.002 Email Accounts
- T1608.001 Upload Malware
- T1567 Exfiltration Over Web Service
- T1583.001 Domains
- T1056.003 Web Portal Capture
- T1586 Compromise Accounts
- T1608 Stage Capabilities
- T1204 User Execution
- T1566 Phishing
- T1056 Input Capture
- T1598 Phishing for Information
- T1189 Drive-by Compromise

Analytical Scores

- Priority technique (graph chokepoint): T1056.003 Web Portal Capture (centrality 0.3361).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5052; 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
IndigoZebra	0.5052
Star Blizzard	0.4939
EXOTIC LILY	0.4264
Transparent Tribe	0.417
Mustard Tempest	0.4125

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	pasastesintag[.]pics
Domain	parastesintago[.]click
Domain	parastesintago[.]help
Domain	pasastesintagc[.]top
Domain	pasastesintago[.]cyou
Domain	pasastesintago[.]online
Domain	pasastesintag26[.]click
Domain	pasastesintap[.]cfd
Domain	pasastesintap[.]cyou
Domain	pasastesintagas[.]mom

Type	Indicator
Domain	pasastesintagi[.]best
Domain	pasastesintagi[.]rest
Domain	pasastesintagi[.]top
Domain	pasastesintagionline[.]click
Domain	pasastesintagionline[.]help
Domain	pasastesintagionline[.]sbs
Domain	pasastesintagcl[.]best
Domain	pasastesintagcl[.]icu
Domain	pasastesintagcl[.]life
Domain	pasastesintagcl[.]mom
Domain	pasastesintagcl[.]rest
Domain	pasastesintaplmw[.]click
Domain	pasastesintag[.]xyz
Domain	pasastesintagas[.]best
Domain	pasastesintagas[.]click
Domain	pasastesintagas[.]buzz
Domain	pasastesintagas[.]help
Domain	pasastesintagas[.]casa
Domain	parastesintag[.]buzz
Domain	parastesintag[.]cfd
Domain	parastesintag[.]click
Domain	parastesintag[.]cyou
Domain	parastesintag[.]help
Domain	parastesintag[.]homes
Domain	parastesintag[.]icu

Type	Indicator
Domain	parastesintag[.]lat
Domain	parastesintag[.]lol
Domain	parastesintag[.]sbs
Domain	parastesintag[.]top
Domain	parastesintag[.]yachts

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:** T1056.003 Web Portal Capture (credential-access)
- **Observed here:** the threat actor used T1056 Input Capture here as an alternative credential-access technique.
- **Projected pivot:** T1056 Input Capture (credential-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The threat actor could pivot to T1056 Input Capture to maintain their objective of capturing sensitive information, potentially by leveraging keyboard hooks or API calls to intercept user input. This would likely involve attempting to install hooks or capture input at various points in the system, which may be difficult to distinguish from legitimate activity. The defensive control to counter this would be to alert on keylogging hooks and API-input capture; restrict accessibility/hook installation.

- **Defensive countermeasure:** Alert on keylogging hooks and API-input capture; restrict accessibility/hook installation.