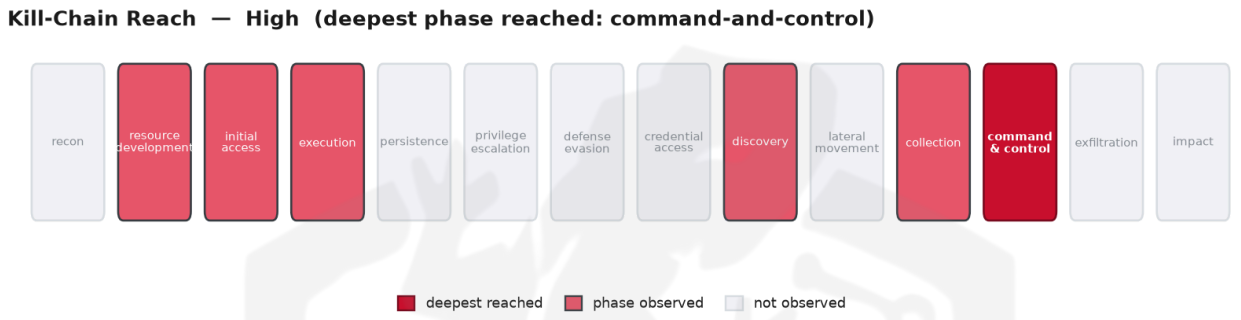
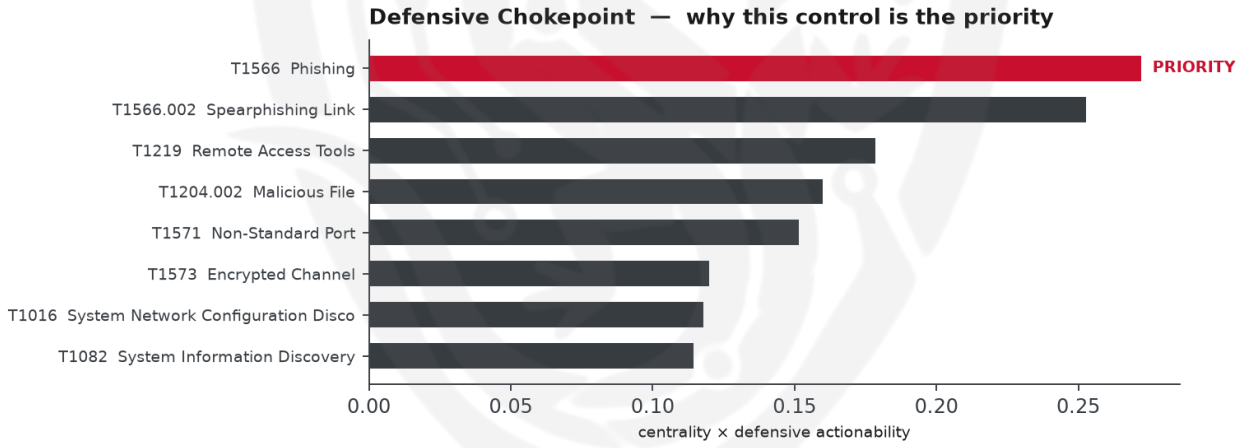
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 has been identified, although the threat actor remains unknown. The campaign involves a range of techniques, including phishing and system discovery, to compromise targets. Priority should be given to defensive actions that mitigate these techniques, particularly phishing. The threat actor's ability to reach command-and-control stages poses a high operational risk.

Threat Overview

The threat actor, whose identity is insufficient to determine, employs various techniques to carry out their campaign. These techniques include screen capture, system owner/user discovery, and phishing, among others. The victimology and targeted sectors are not well-defined due to insufficient data. However, the techniques used suggest a broad range of potential targets.

Attack Chain and Priority Control

The attack chain involves multiple techniques, starting with initial access through phishing or drive-by compromise, followed by system discovery and potential lateral movement. The priority technique identified is T1566 Phishing, which serves as a critical chokepoint in the attack chain. To mitigate this, the priority control is to: Enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button.

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs used by the threat actor. Additionally, no malware families have been corroborated by abuse.ch, and 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)

- T1113 Screen Capture
- T1033 System Owner/User Discovery
- T1059.007 JavaScript
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1497.001 System Checks
- T1566.002 Spearphishing Link
- T1608.004 Drive-by Target
- T1082 System Information Discovery
- T1608.001 Upload Malware
- T1219 Remote Access Tools
- T1016 System Network Configuration Discovery
- T1588.002 Tool
- T1566 Phishing
- T1571 Non-Standard Port
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1102.002 Bidirectional Communication
- T1518.001 Security Software Discovery
- T1189 Drive-by Compromise
- T1124 System Time Discovery

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2721).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5095; 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
Darkhotel	0.5095
TA2541	0.4871
Windshift	0.4549
SideCopy	0.4457
FIN7	0.4429

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: 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	avanzaringenieriaysalud[.]com	
Domain	qualproengineering[.]com	
Domain	canetworkcabling[.]com	
Domain	nobaggagechallenge[.]com	
Domain	lakewoodexteriors[.]com	
Domain	pharmahubbd[.]com	

Type	Indicator	Context
Domain	cpadllc[.]com	
Domain	right-end[.]com	
Domain	docusnok[.]dn3[.]co	
Domain	ursinhofestas[.]com[.]br	
Domain	verbodoavivamento[.]org[.]br	
Domain	nivelasemos[.]us	
Domain	elaborar[.]us	
Domain	mikelmak[.]com	
Domain	curitibaredes[.]com[.]br	
Domain	mogibusinesscenter[.]com[.]br	
Domain	floresdecasa[.]cl	
Domain	insureongo[.]net	malware_download
Domain	cotgfoods[.]com	
Domain	pehnavni[.]com	
Domain	dpcuments[.]com	
Domain	quickwebsign[.]com	Unknown malware
Domain	docsignsecured[.]info	
Domain	micasaprefabricadadehormigon[.]com	
Domain	workspaceviewer[.]com	
Domain	firdous[.]pro	
Domain	l[.]xpcbofl[.]com	
Domain	gmapsistemas[.]com[.]br	
Domain	livesocially[.]co	
Domain	bobsrvsc[.]com	
Domain	docusign[.]nzworldtravel[.]com	

Type	Indicator	Context
Domain	vsilex[.]com	
Domain	wilsongroup[.]in	
Domain	workspacegateway[.]com	
Domain	bolsasgotadagua[.]com	
Domain	zoom[.]allwellhealthcare[.]com	
Domain	dardsaaz[.]com	
Domain	absolutecaninepa[.]com	
Domain	workspaceviewers[.]com	
Domain	americanmovingco[.]org	

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:** T1566 Phishing (initial-access)
- **Observed here:** the threat actor used T1189 Drive-by Compromise here as an alternative initial-access technique.
- **Projected pivot:** T1189 Drive-by Compromise (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The threat actor could pivot to T1189 Drive-by Compromise to maintain their objective by exploiting vulnerabilities in software or plugins to compromise a system, potentially using malicious websites or advertisements to infect victims. This technique may be used as an alternative to phishing, as it can still achieve the actor's goals of gaining initial access to a system. The defender would likely counter this by enforcing the mandated defensive control: Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.

- **Defensive countermeasure:** Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.