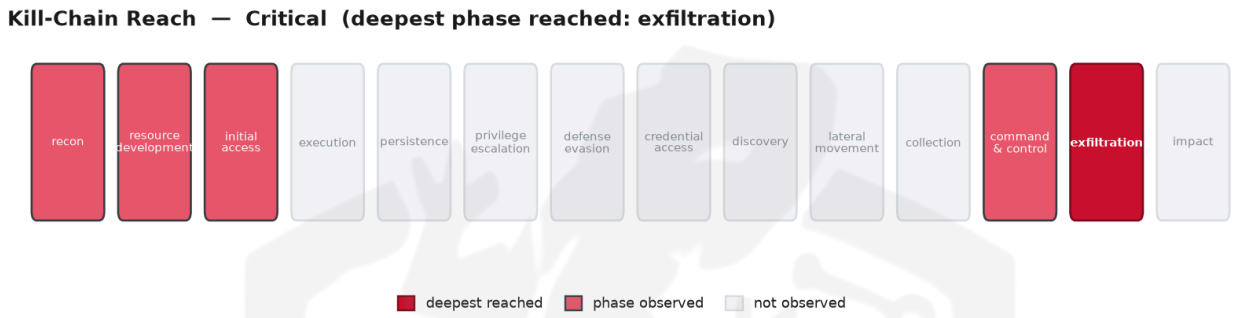
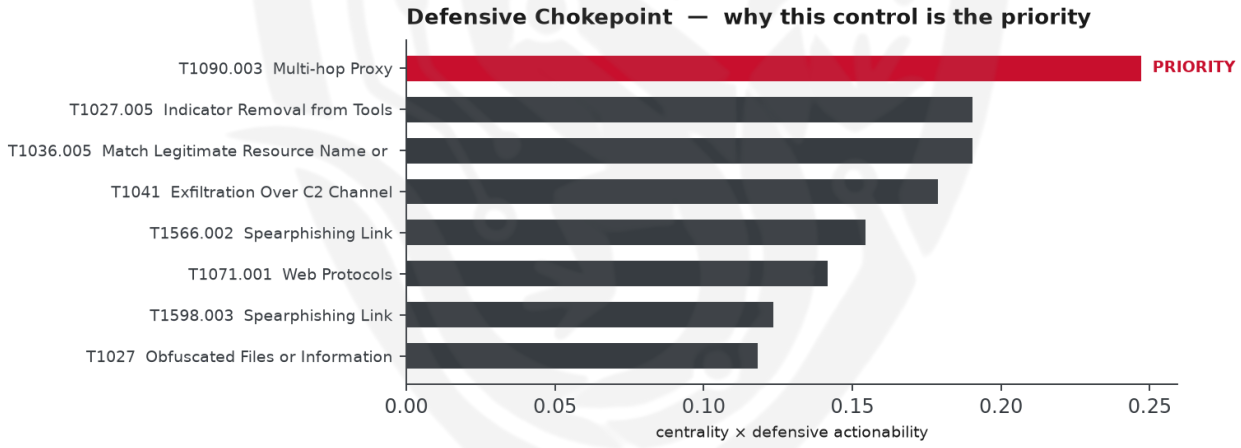
THREAT REPORT: UNKNOWN_ADVERSARY GLOBAL SMISHING OPERATION

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 targeting various sectors, including telecommunications, finance, and government, in multiple countries such as Australia, Chile, and Germany. The threat actor is utilizing a range of techniques to carry out their operation, with a focus on smishing. Priority should be given to defending against the multi-hop proxy technique used by the threat actor. The operation's global reach and diverse targeting suggest a high level of sophistication.

Threat Overview

The threat actor, whose identity is currently unknown, is engaging in a global smishing operation that affects multiple countries and sectors. The operation involves the use of various techniques, including client configurations, web protocols, and domain manipulation. The threat actor's targets include

telecommunications, finance, retail, government, and transportation sectors in countries such as Australia, Chile, Colombia, Germany, Mexico, and the Netherlands.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, starting with client configurations and web protocols, followed by domain manipulation and indicator removal. The priority technique in this chain is the multi-hop proxy (T1090.003), which serves as a chokepoint. To mitigate this technique, the specific MITRE ATT&CK mitigation for T1090.003 should be applied, and host/network detections and least-privilege controls should be put in place around it.

Infrastructure and Corroboration

There is currently no 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.

Technical Appendix

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

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

- T1592.004 Client Configurations
- T1071.001 Web Protocols
- T1583.001 Domains
- T1027.005 Indicator Removal from Tools
- T1598.003 Spearphishing Link
- T1090.003 Multi-hop Proxy
- T1036.005 Match Legitimate Resource Name or Location
- T1041 Exfiltration Over C2 Channel
- T1027 Obfuscated Files or Information
- T1566.002 Spearphishing Link

Analytical Scores

- Priority technique (graph chokepoint): T1090.003 Multi-hop Proxy (centrality 0.4118).
- Operational risk: Critical (score 0.926, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4117; 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
ZIRCONIUM	0.4117
WIRTE	0.3742
Ferocious Kitten	0.3656
Transparent Tribe	0.354
RedEcho	0.343

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

No indicators were attached to this pulse.

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:** T1090.003 Multi-hop Proxy (command-and-control)
- **Observed here:** the threat actor used T1071.001 Web Protocols here as an alternative command-and-control technique.
- **Projected pivot:** T1071.001 Web Protocols (command-and-control)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to using T1071.001 Web Protocols to maintain their command and control channel, potentially leveraging common web protocols to blend in with legitimate traffic and evade detection. This technique may allow the actor to continue communicating with their command and control server, potentially using HTTP or HTTPS requests to transmit data. The defender would likely implement the mandated defensive control, which is to egress-filter to known-good; inspect HTTP(S) for beaconing; alert on anomalous web C2 patterns.

Detection and hardening for the pivot (T1071.001 Application Layer Protocol)

- **Telemetry:** Proxy / DNS logs; Network flow / TLS metadata
- **Detect:**

    - Beaconing: regular-interval, low-jitter connections to rare destinations
    - HTTP(S) to newly registered or low-reputation domains; odd user-agents
    - DNS with high entropy or excessive TXT-record query volume
- **Harden:**
    - Force egress through an inspecting proxy; block direct outbound
    - TLS inspection where lawful; DNS filtering and logging
- **MITRE:** M1031 Network Intrusion Prevention, M1037 Filter Network Traffic · DS0029 Network Traffic