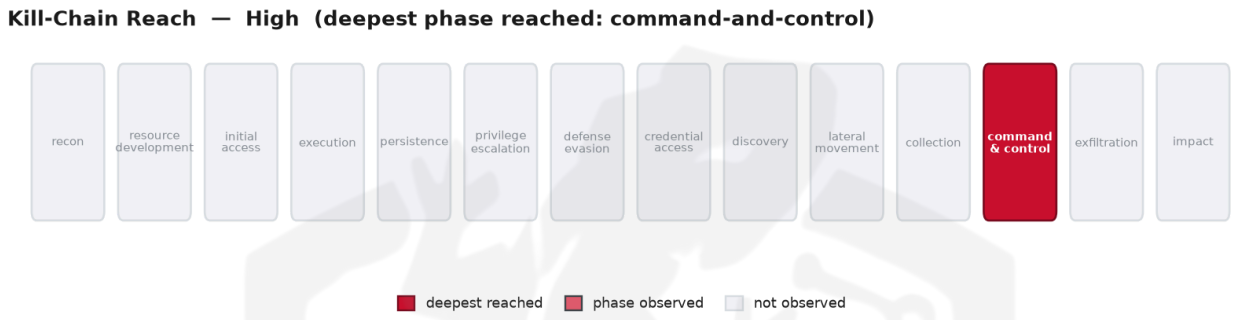
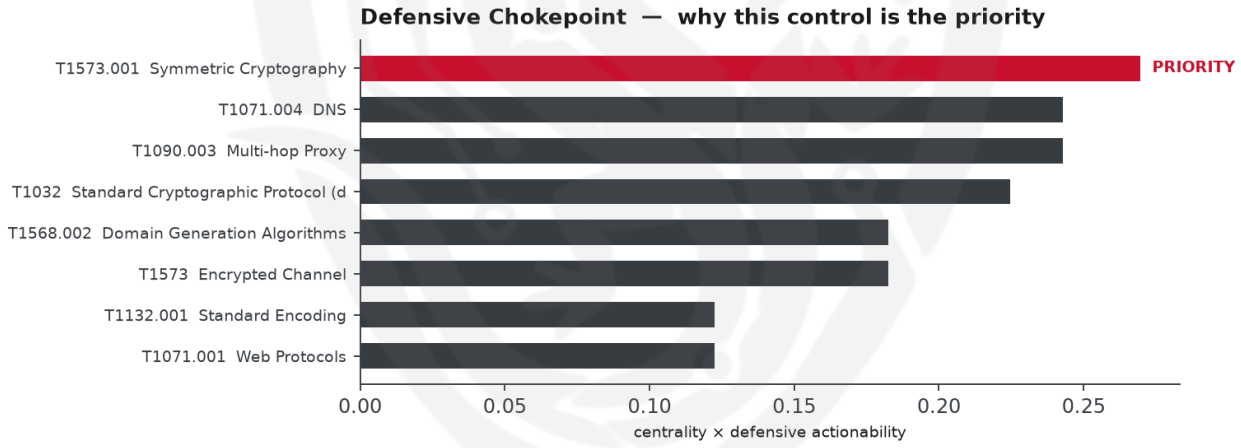
THREAT REPORT: UNKNOWN_ADVERSARY MALWARE CAMPAIGN

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 multiple malware families, including Popa, Moneytiser, Loopop, Neupop, and Hopanet. The threat actor is targeting unknown sectors and countries, and the priority defensive action should be to inspect TLS at the egress proxy where policy allows. This campaign poses a high operational risk due to its potential to establish command-and-control channels. Priority should be given to detecting and mitigating the use of symmetric cryptography.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, is utilizing a range of malware families to exploit unknown vulnerabilities. The malware families involved include Popa, Moneytiser, Loopop, Neupop, and Hopanet. The victimology of this campaign is currently unknown, but the use of techniques

such as standard encoding, domain generation algorithms, and symmetric cryptography suggests a sophisticated threat.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including standard encoding, domain generation algorithms, DNS, symmetric cryptography, and multi-hop proxy. The priority technique in this chain is T1573.001 Symmetric Cryptography, which is the graph chokepoint. To mitigate this threat, the priority control is to: Inspect TLS at the egress proxy where policy allows; alert on self-signed / non-standard symmetric-encrypted channels and beaconing.

Infrastructure and Corroboration

There is currently no information available on the hosting providers or ASNs used by the threat actor. According to abuse.ch, the malware families involved are unknown. 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)

- T1132.001 Standard Encoding
- T1568.002 Domain Generation Algorithms
- T1071.004 DNS
- T1573.001 Symmetric Cryptography
- T1032 Standard Cryptographic Protocol (deprecated)
- T1090.003 Multi-hop Proxy
- T1573 Encrypted Channel
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1573.001 Symmetric Cryptography (centrality 0.4495).
- Operational risk: High (score 0.552, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4264; 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
RedEcho	0.4264
TA551	0.3772
Inception	0.3103
Orangeworm	0.3015
Stealth Falcon	0.2767

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	nice-protect[.]com	
Domain	house-spirit[.]com	Unknown malware
Domain	gmslb[.]net	
Domain	rainproxy[.]io	malware_download
Domain	enigmaproxy[.]net	
Domain	fast-mob[.]com	
Domain	s01691[.]novel-layer[.]com	Unknown malware
Domain	pulse-vol[.]com	
Domain	zen-tava[.]com	
Domain	s1[.]gmslb[.]net	
Domain	s1252[.]gmslb[.]net	
Domain	s1244[.]gmslb[.]net	

Type	Indicator	Context
Domain	gw[.]netnut[.]net	
Domain	sdk[.]netnut[.]io	
Domain	axe-net[.]com	
Domain	byte-armor[.]com	
Domain	byte-buff[.]com	Unknown malware
Domain	cool-horizon[.]com	
Domain	digiproxy[.]cc	
Domain	earth2trust[.]com	
Domain	flashproxy[.]com	
Domain	flexible-networks[.]com	
Domain	grid-push[.]com	
Domain	iprocket[.]io	
Domain	link-flux[.]com	
Domain	litics-net[.]com	
Domain	mob-hit[.]com	
Domain	net-echo[.]com	
Domain	nova-lan[.]com	
Domain	novel-layer[.]com	
Domain	noverland[.]com	
Domain	sdkmob[.]org	
Domain	shield-sky[.]com	
Domain	sky-borders[.]com	
Domain	star-layer[.]com	
Domain	swift-zip[.]com	
Domain	tera-home[.]com	

Type	Indicator	Context
URL	hxxp://gw[.]netnut[.]net:9595	
Hash	2227df1207d2c90db46610bd98909032	
Hash	3a69aedb78677993384dfe9b476e3d26	

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:** T1573.001 Symmetric Cryptography (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 communication with their command and control server, potentially leveraging common web protocols to blend in with legitimate traffic and evade detection. This would likely involve using HTTP or HTTPS to transmit encoded or encrypted data, which may allow them to bypass some security controls. To counter this, the mandated defensive control of egress-filter to known-good; inspect HTTP(S) for beaconing; alert on anomalous web C2 patterns should be implemented.

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