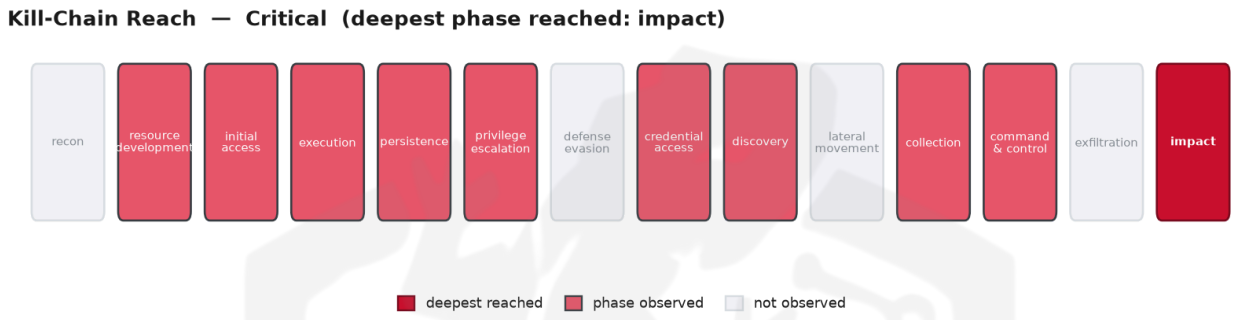
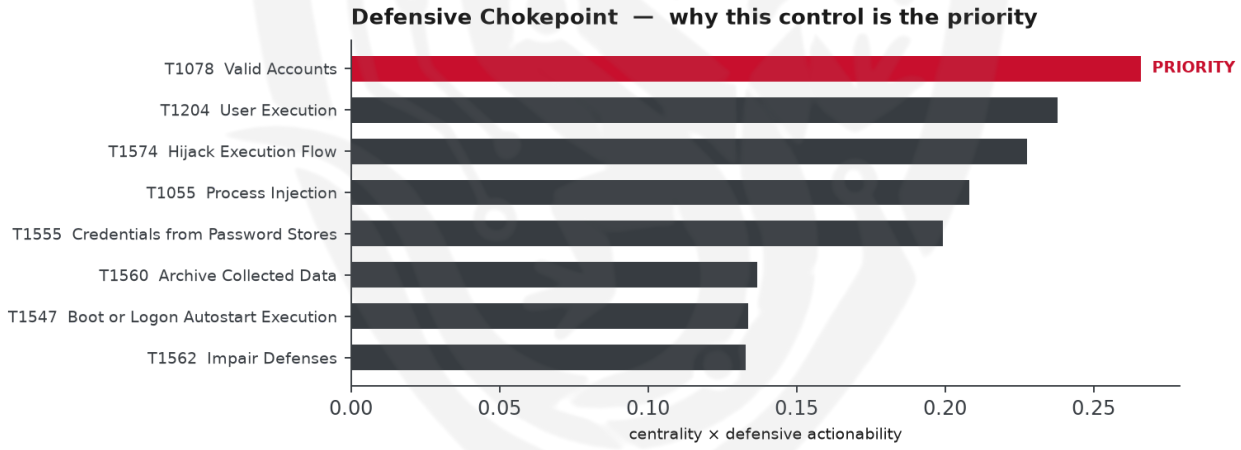
THREAT REPORT: UNKNOWN_ADVERSARY MALICIOUS STEAM WALLPAPERS

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 found to be stealing accounts through malicious wallpapers on Steam, targeting users in several countries including Canada, China, and India. The malware families involved include DarkComet, Fynloski, and Vidar, among others. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The threat actor's use of valid accounts is a critical technique that requires immediate attention.

Threat Overview

The threat actor, whose identity is unknown, is utilizing a range of malware families including DarkComet, DarkKomet, and Lumma to steal web session cookies and credentials from password stores. The targeted countries include British Indian Ocean Territory, Canada, China, and others, although the specific sectors

targeted are not known. The actor is exploiting various techniques to achieve their goals, including creating or modifying system processes and hiding artifacts.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, starting with user execution and process injection, followed by stealing web session cookies and credentials from password stores. The priority technique is T1078 Valid Accounts, which is the graph chokepoint. To mitigate this threat, the priority control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this activity, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with high confidence by AbuseIPDB, 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)

- T1543 Create or Modify System Process
- T1539 Steal Web Session Cookie
- T1547 Boot or Logon Autostart Execution
- T1564 Hide Artifacts
- T1071 Application Layer Protocol
- T1140 Deobfuscate/Decode Files or Information
- T1562 Impair Defenses
- T1555 Credentials from Password Stores
- T1055 Process Injection
- T1560 Archive Collected Data
- T1608 Stage Capabilities
- T1204 User Execution
- T1574 Hijack Execution Flow
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1496 Resource Hijacking
- T1485 Data Destruction
- T1518 Software Discovery
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2658).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3985; 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
Tropic Trooper	0.3985
Rocke	0.3569
Threat Group-3390	0.3274
APT19	0.3244
LuminousMoth	0.3186

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	Context
URL	hxxps://www[.]dropbox[.]com/s/zhp1b06imehwylq/Synaptics[.]rar?dl=1	malware_download
URL	hxxps://docs[.]google[.]com/uc?id=0BxsMXGfPIZfSVzUyaHFYVkQxeFk&export=download	malware_download
URL	hxxp://202[.]144[.]192[.]29/download2/Themes2[.]zip	
URL	hxxp://202[.]144[.]192[.]29/audit[.]php	
URL	hxxp://brightly[.]to/download2/Themes2[.]zip	

Type	Indicator	Context
Hash	fc586cad94e5a10dd5be6a6ae6096bd02dfbfd094365bec87e788ed0798d6f67	
Hash	18dedc0009f0927cba6425c84cce9883	
Hash	5620f01284329f561b1839a36be55355	
Hash	74414ed4b63aadec039b603c32762b80	
Hash	8c2cc585ad8a13a72a704c0fda0c9854	
Hash	95856f2ce428c728d9781d3296558068	
Hash	c133c3dd9f7d6934598025047df41abf	
Hash	ded08ae5df7f1b12e5fdb767dbbed0b1	
Hash	59868381885b33f6c8809cd3d945da7d167439a3	

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:** T1078 Valid Accounts (initial-access)
- **Observed here:** T1078 Valid Accounts was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1190 Exploit Public-Facing Application (initial-access)
- **Basis:** 32 of 170 documented groups that use Valid Accounts also use Exploit Public-Facing Application (conditional 0.50, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

With T1078 Valid Accounts blocked, the threat actor could preserve the same objective by pivoting to T1190 Exploit Public-Facing Application, a technique commonly paired with it across tracked groups. Defensive countermeasure: Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

Also plausible (same tactic): T1133 External Remote Services (n=25, lift 2.4), T1199 Trusted Relationship (n=10, lift 2.2)

Detection and hardening for the pivot (T1190 Exploit Public-Facing Application)

- **Telemetry:** WAF / reverse-proxy logs; Web server logs; EDR on the DMZ host
- **Detect:**
  - Exploit strings and anomalous request paths in access logs; 500s spikes
  - The web/app service account spawning shells or network tools
  - Outbound connections from a server that should never initiate them
- **Harden:**
  - Patch internet-facing software fast; virtual-patch at the WAF meanwhile
  - Egress filtering from DMZ hosts; least-privilege service accounts
- **MITRE:** M1051 Update Software, M1050 Exploit Protection, M1016 Vulnerability Scanning, M1030 Network Segmentation · DS0015 Application Log, DS0009 Process, DS0029 Network Traffic