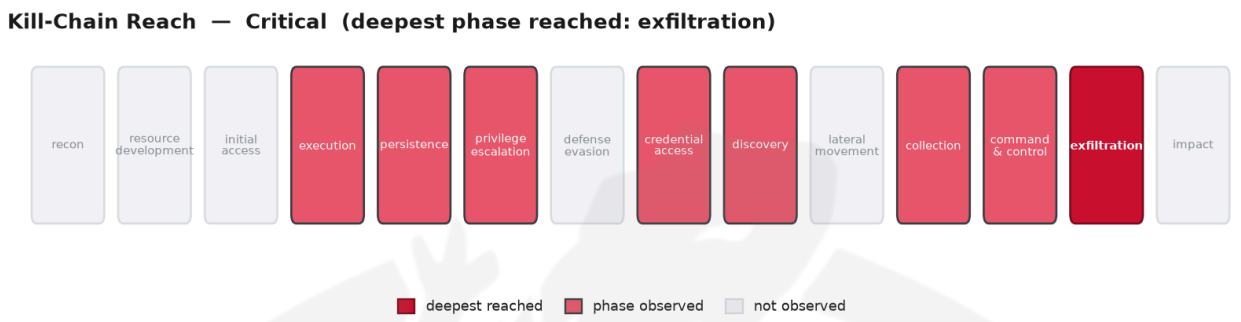
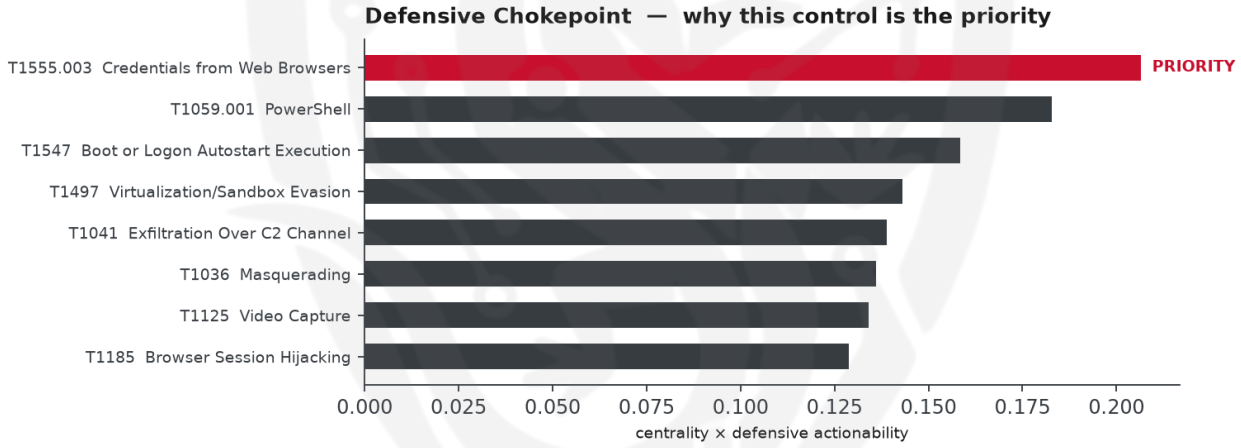
THREAT REPORT: POWERCAT MALWARE CAMPAIGN

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 is associated with the Powercat malware, which is delivered through fake game cheats and functions as an infostealer. The campaign's targets and affected countries are currently unknown. Priority should be given to restricting access to browser credential stores to prevent further exploitation. The threat actor's use of Powercat malware poses a significant risk to affected systems, emphasizing the need for immediate defensive action.

Threat Overview

The threat actor, whose identity is currently unknown, is utilizing the Powercat malware family to steal sensitive information. The malware's capabilities include screen capture, keylogging, and stealing web session cookies, among others. The victimology of this campaign is not well understood due to insufficient data, but the use of Powercat malware suggests a focus on infostealing.

Attack Chain and Priority Control

The attack chain involves various techniques, including screen capture, keylogging, and browser session hijacking, ultimately leading to the exfiltration of sensitive information. The priority technique in this chain is T1555.003, Credentials from Web Browsers, which is the primary method used by the malware to obtain sensitive information. To mitigate this threat, the priority control is to "Restrict access to browser credential stores; alert on reads of Login Data / cookies files by non-browser processes; enforce disk encryption."

Infrastructure and Corroboration

There is currently no available information on the hosting providers or ASNs observed in relation to this campaign, as indicated by the lack of data in the infrastructure and corroboration section. 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
- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1547 Boot or Logon Autostart Execution
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1036 Masquerading
- T1185 Browser Session Hijacking
- T1555.003 Credentials from Web Browsers
- T1125 Video Capture
- T1016 System Network Configuration Discovery
- T1497 Virtualization/Sandbox Evasion
- T1057 Process Discovery
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1027 Obfuscated Files or Information
- T1518.001 Security Software Discovery
- T1071.001 Web Protocols
- T1518 Software Discovery
- T1564.001 Hidden Files and Directories

Analytical Scores

- Priority technique (graph chokepoint): T1555.003 Credentials from Web Browsers (centrality 0.2949).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4949; 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
Stealth Falcon	0.4949
APT42	0.4577
Darkhotel	0.4372
Inception	0.4036
Windshift	0.4003

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
Domain	powercat[.]dog	malware_download
Domain	ce953a0eb08246617b7f849486c4b26a7af37e9d2e8f0e13b3ae1bf0da8a70a[.]xyz	
Domain	alpha[.]ce953a0eb08246617b7f849486c4b26a7af37e9d2e8f0e13b3ae1bf0da8a70a[.]xyz	
Domain	beta[.]ce953a0eb08246617b7f849486c4b26a7af37e9d2e8f0e13b3ae1bf0da8a70a[.]xyz	

Type	Indicator	Context
Domain	charlie[.]ce953a0eb08246617b7f849486c4b26a7af37e9d2e8f0e13b3ae1bf0da8a70a[.]xyz	
Domain	hotel[.]ce953a0eb08246617b7f849486c4b26a7af37e9d2e8f0e13b3ae1bf0da8a70a[.]xyz	
Domain	juliett[.]ce953a0eb08246617b7f849486c4b26a7af37e9d2e8f0e13b3ae1bf0da8a70a[.]xyz	
Domain	kilo[.]ce953a0eb08246617b7f849486c4b26a7af37e9d2e8f0e13b3ae1bf0da8a70a[.]xyz	
Domain	lima[.]ce953a0eb08246617b7f849486c4b26a7af37e9d2e8f0e13b3ae1bf0da8a70a[.]xyz	
Domain	oscar[.]ce953a0eb08246617b7f849486c4b26a7af37e9d2e8f0e13b3ae1bf0da8a70a[.]xyz	
URL	hxxps://ce953a0eb08246617b7f849486c4b26a7af37e9d2e8f0e13b3ae1bf0da8a70a[.]xyz	
URL	hxxps://powercat[.]dog/cool	
URL	hxxps://powercat[.]dog/watermelon5	
Hash	a33a96cbd92eef15116c0c1dcaa8feb6eee28a818046ac9576054183e920eeb5	
Hash	1d8e87144890cfe06a208c99a50748f7	
Hash	ccb902ac93fce95a87d19262ef90688c	
Hash	725567384190916da37957e90bd5892a6b4fbe09	
Hash	ac5bb68591b4350858878d2184bdac63cedfcb60	
Hash	a9b4823a1b2c0702a1eb8a1bf18db2d9c9604d2d2dd98a99f1d388bf7cfa71e3	
Hash	c0c3a0331b57d10d23a172a79bdf13ab066255de41774e5a19dd8a8e8446e1fa	

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:** T1555.003 Credentials from Web Browsers (credential-access)

- **Observed here:** T1555.003 Credentials from Web Browsers was the only credential-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1003 OS Credential Dumping (credential-access)
- **Basis:** of the 21+ groups that use Credentials from Web Browsers, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1003 OS Credential Dumping to maintain access to sensitive credentials, as this technique allows them to extract credentials from the operating system, which may include those not stored in web browsers, thereby potentially bypassing the blocked control. This technique may be particularly appealing as it enables the actor to access credentials that are not stored in web browsers, which could include domain administrator credentials or other high-value targets. To counter this potential pivot, the mandated defensive control of protecting LSASS (RunAsPPL, Credential Guard), alerting on LSASS handle access, and disabling WDigest should be implemented.

Also plausible (same tactic): T1552 Unsecured Credentials (n=15, lift 3.5), T1110 Brute Force (n=12, lift 2.3)

Detection and hardening for the pivot (T1003 OS Credential Dumping)

- **Telemetry:** Sysmon (process access); EDR credential-theft telemetry
- **Detect:**
  - Sysmon 10 (process access) targeting lsass.exe with suspicious access masks
  - Access to ntds.dit / SAM / SYSTEM hives; vssadmin/shadow-copy abuse
  - comsvcs.dll MiniDump, procdump, or reg save of security hives
- **Harden:**
  - Enable Credential Guard and LSA protection (RunAsPPL)
  - Restrict debug privilege; tiered admin to limit credential exposure
- **MITRE:** M1043 Credential Access Protection, M1028 Operating System Configuration, M1026 Privileged Account Management, M1017 User Training · DS0009 Process, DS0022 File, DS0024 Windows Registry