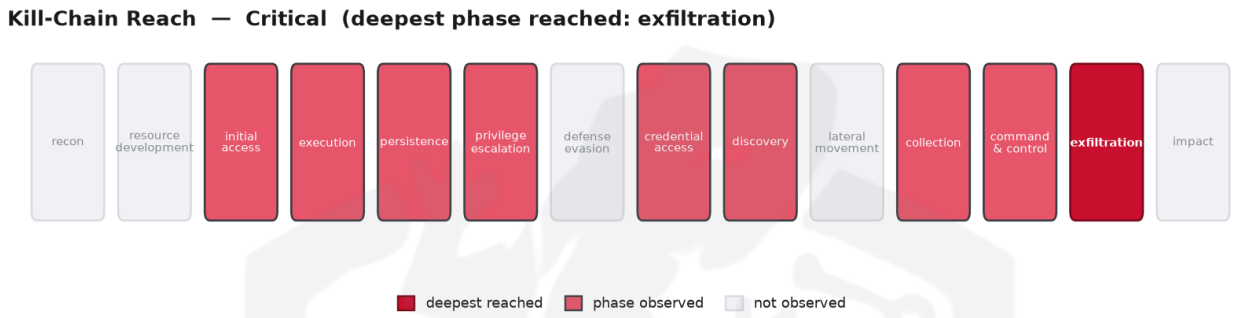
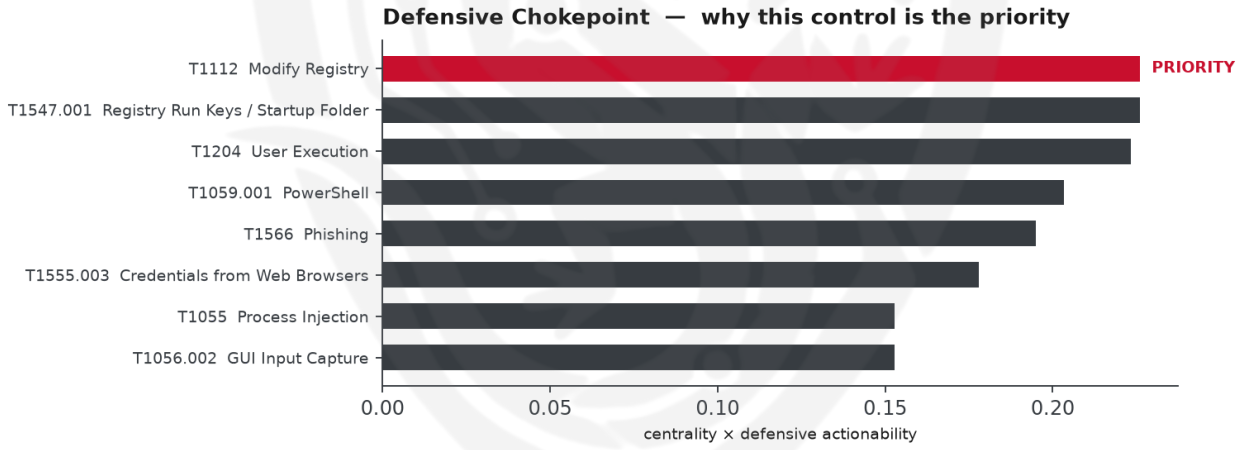
THREAT REPORT: FAKE XENO ROBLOX CHEATS DELIVER JAVA STEALER

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 delivering a powerful Java stealer through fake Roblox cheats on Discord and forums. The malware family involved is Powercat, which is capable of various techniques including screen capture, keylogging, and web session cookie theft. The priority defensive action should be to monitor sensitive registry keys for modification and restrict registry-edit tools for unprivileged users. Given the potential for exfiltration, it is critical to take immediate action to prevent further compromise.

Threat Overview

The threat actor, whose identity is currently insufficient to determine, is utilizing the Powercat malware family to target unsuspecting users. The malware is delivered through fake Roblox cheats on Discord and

forums, and once installed, it can perform a range of malicious activities. The victimology of this campaign is currently unclear, but the techniques used by the malware suggest a high level of sophistication.

Attack Chain and Priority Control

The attack chain involves various techniques, including screen capture, keylogging, and web session cookie theft, ultimately leading to exfiltration of sensitive data. The priority technique in this chain is T1112 Modify Registry, which is a critical step in the malware's ability to persist and evade detection. To mitigate this threat, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

There is currently no available information on the hosting providers or ASNs observed in this campaign, and no malware families have been corroborated by abuse.ch. Additionally, 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
- T1548.002 Bypass User Account Control
- T1082 System Information Discovery
- T1005 Data from Local System
- T1055 Process Injection
- T1112 Modify Registry
- T1555.003 Credentials from Web Browsers
- T1125 Video Capture
- T1083 File and Directory Discovery
- T1497 Virtualization/Sandbox Evasion
- T1204 User Execution
- T1057 Process Discovery
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1056.002 GUI Input Capture
- T1566 Phishing
- T1571 Non-Standard Port
- T1027 Obfuscated Files or Information

- T1132 Data Encoding
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.238).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4907; 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
APT37	0.4907
Inception	0.4697
Dark Caracal	0.4607
Stealth Falcon	0.4189
Patchwork	0.414

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
Domain	ce953a0eb08246617b7f849486c4b26a7af37e9d2e8f0e13b3ae1bf0da8a70a[.]xyz
URL	hxxps://solthere[.]net/justacoolkat10
URL	hxxps://solthere[.]net/api/v1/redeem
Hash	0aadd62b535e683a5a2fe31fde546d07

Type	Indicator
Hash	0d03faf1764297c908158da77c8ffcae
Hash	163c8d117ef5a4e4e9c3e92a726af0eb
Hash	26a94168fa25af0bcb46a18ede50af86
Hash	2ead73ed62f1c2beb9043ce92e774e0b
Hash	1a462c76efc4e73725b9e95c4a00fddb
Hash	4bdaf7792e908f163ebef137854c571d
Hash	7b96170259a376ea79411c5713beb396
Hash	9699bd6a448d0662a1e9e353223263b6
Hash	9930036e8f787674db39094e21413e77
Hash	d123dbb5c5980bfeb22586197d2cc403
Hash	000dcd8d78a97b9f78f872fea559f9b1706f0bc2
Hash	4a4c6265d2f80d9b833f141a7f841349de94ccf5
Hash	6525189bce7adf3bb3b84906ffd1e27cdc111bd9
Hash	86dc6db6e8c67644e8c4c84656c92937a347777c
Hash	de74e45ff4f99c385d1ec91d4f6a197fc90845b0
Hash	27655272c15d508ce4d33cdae686e4b1ba05877fae5ba2c557da437c47cf0957
Hash	609b1004d90f85936d56e507b3220796103d201b8e7677ee3e82872e5b4aa73f
Hash	9b2e33ae75f419facf56f321b3f2447b83b76d6c1d9b29fcde41c7d65c321dce
Hash	bf973513f76a24d92c4953d8c9540d427234107afa9881f4e62b55c79c5bf7cb
Hash	c08a0d5b30b1088284a3c473279eb59557de517e7d8662495272b22634c8b5ed
Hash	10f634c18e75faf733a834ee6fd1997b3cf25700
Hash	1b93e05e58e5aa32aaf18d58b888a008d5a35341
Hash	21bd2be3535cfe40b652290a3a94e4538e31885e
Hash	362458ae08945378f2ea9fd2bb31e3ae5382d79d
Hash	997dae041966070f26aa7bb1b8ab663fb8609678

Type	Indicator
Hash	c4d541e31cef2ccccd57d27e5cc6997c4d52020a
Hash	16f38cf540bcb045ae03d310c13c068718f1d23b2bb7b893deb86ff880c1c599
Hash	1f0ceed271a42b0c8eaaa9966b0152a7a1e7ccc1534be23b02c8ef5ab239efdb
Hash	3b500f46ce6dc31ad635c6b511462a31b632ee531d9e102084413af016102c98
Hash	6195dda8339036ad74fd4fb185c5fc02eb28270faa2b41ec3d9303cba7e8d2c6
Hash	7aa2ddc2a6f3c97723dc3a882f481398dd575401b3bb7a4f4c1939d2990e8418
Hash	879f5aac13722af56c2fb7b0bc31a2ae318356aafdfe93274e23a32e494fd0f2

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:** T1112 Modify Registry (persistence)
- **Observed here:** T1112 Modify Registry was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1543 Create or Modify System Process (persistence)
- **Basis:** of the 14+ groups that use Modify Registry, this pairing runs 2.8x above base rate, a disproportionately-coupled move rather than the obvious one.

With T1112 Modify Registry blocked, the threat actor could preserve the same objective by pivoting to T1543 Create or Modify System Process, a technique disproportionately paired with it across tracked groups. Defensive countermeasure: Restrict service/daemon creation to admins; monitor service and driver installs.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=19, lift 1.9), T1505 Server Software Component (n=11, lift 2.0)

Detection and hardening for the pivot (T1543 Create or Modify System Process)

- **Telemetry:** Windows Security / System log; Sysmon
- **Detect:**
  - System 7045 (new service installed); Security 4697 (service installed)
  - Sysmon 1 for sc.exe / services created; unusual ImagePath or user-context services
  - Registry writes under HKLM\SYSTEM\CurrentControlSet\Services
- **Harden:**
  - Restrict service creation to admins; application control on service binaries
  - Baseline installed services and alert on new/anomalous ones

- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0019 Service, DS0024 Windows Registry, DS0009 Process