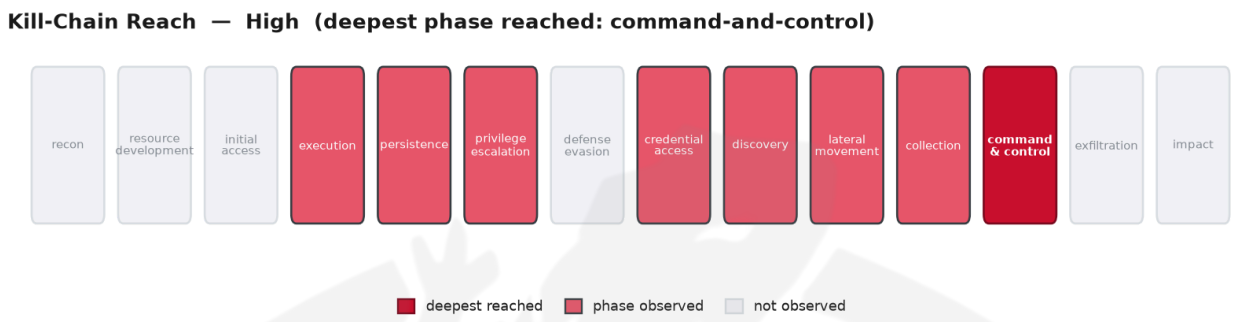
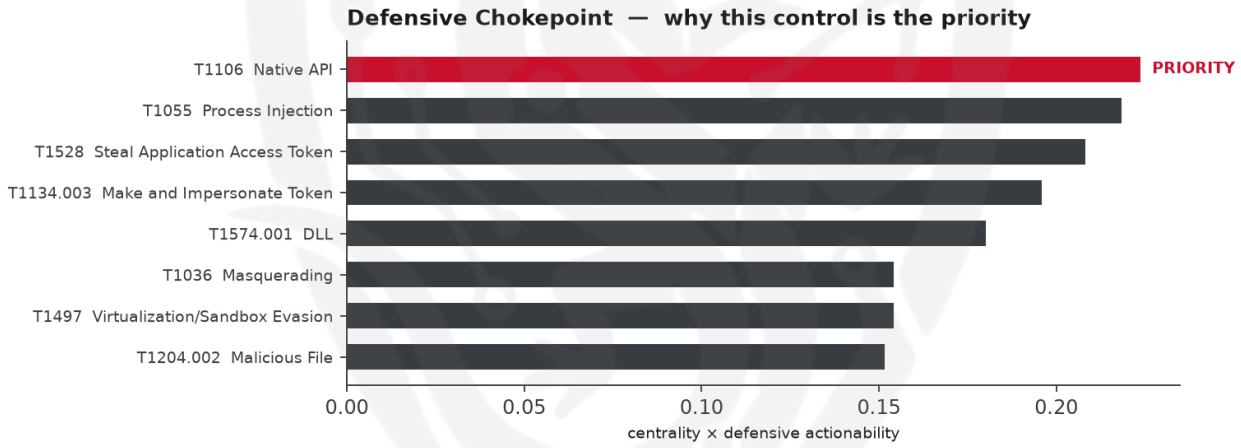
THREAT REPORT: TODDYCAT

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 source attributes this activity to ToddyCat, a threat actor who has been observed using various techniques to gain access to Gmail accounts. The malware families Umbrij and TomBerBil have been identified as part of this campaign. Priority should be given to defending against the use of Native API by non-system processes. The threat actor's targets and motivations are not well understood due to insufficient data.

Threat Overview

ToddyCat, the observed threat actor, has been associated with the malware families Umbrij and TomBerBil. The central vulnerability exploited is not well understood due to insufficient data. The threat actor's victimology is also not well understood, with insufficient data on targeted countries and sectors.

Attack Chain and Priority Control

The attack chain involves a range of techniques, including Scheduled Task, System Owner/User Discovery, Steal Web Session Cookie, and others. The priority technique is T1106 Native API, which is the graph chokepoint. To defend against this, the priority control is to Enable EDR API-telemetry; alert on unusual direct Native API use from non-system processes.

Infrastructure and Corroboration

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

- T1053.005 Scheduled Task
- T1033 System Owner/User Discovery
- T1539 Steal Web Session Cookie
- T1204.002 Malicious File
- T1574.001 DLL
- T1082 System Information Discovery
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1036 Masquerading
- T1055 Process Injection
- T1497 Virtualization/Sandbox Evasion
- T1528 Steal Application Access Token
- T1134.003 Make and Impersonate Token
- T1057 Process Discovery
- T1114.002 Remote Email Collection
- T1102.002 Bidirectional Communication
- T1059.006 Python
- T1071.001 Web Protocols
- T1550.001 Application Access Token

Analytical Scores

- Priority technique (graph chokepoint): T1106 Native API (centrality 0.2797).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4781; 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	0.4781
Higaisa	0.4132
Tropic Trooper	0.3536
WIRTE	0.3499
BRONZE BUTLER	0.3474

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	2fuserinfo[.]email
Hash	9f5f2f0fb0a7f5aa9f16b9a7b6dad89f
Hash	28cb7b261f4eb97e8a4b3b0d32f8def1
Hash	1ab58838e5790efb22f2d35ab98c0b7d
Hash	22aaeb4946ba6d2f2e27feb7dbb295de
Hash	3432dd9ac0df80ef86eb80bd080f839b
Hash	3d3a621f852c42d97fd7260681e42508
Hash	a7d7d6c4c3f227f7117261c63b9e23a9
Hash	bae82a15d1dbfb024617b9b56a8e5f66
Hash	f169d6d172dfb775895a5e2b1540c854

Type	Indicator
Hash	f61fbfb7aa1cd5dc8f70b055b51563e2

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:** T1106 Native API (execution)
- **Observed here:** ToddyCat used T1053.005 Scheduled Task here as an alternative execution technique.
- **Projected pivot:** T1053.005 Scheduled Task (execution)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

ToddyCat could pivot to utilizing T1053.005 Scheduled Task to maintain persistence and execute malicious actions at a later time, potentially leveraging the Windows Task Scheduler to blend in with legitimate system activity. This technique may allow ToddyCat to bypass the blocked Native API control and continue their campaign objectives. To counter this potential move, the defensive control would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Detection and hardening for the pivot (T1053.005 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
  - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
  - Restrict schtasks/at to administrators; disable the legacy at.exe
  - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File