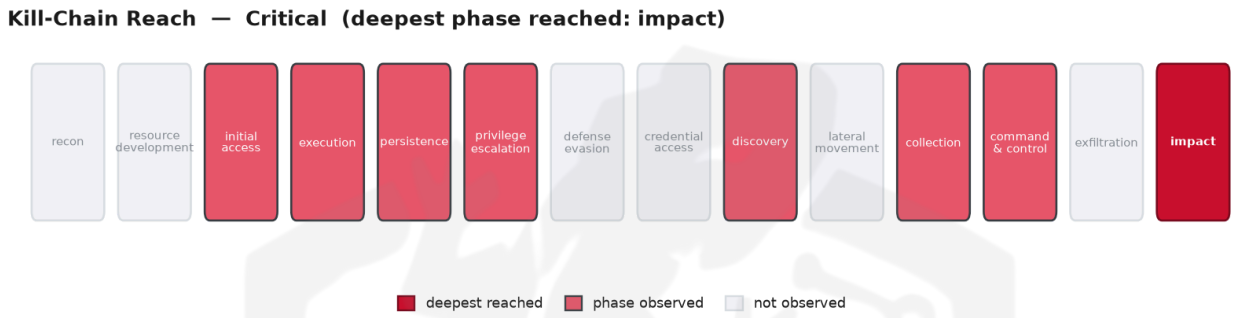
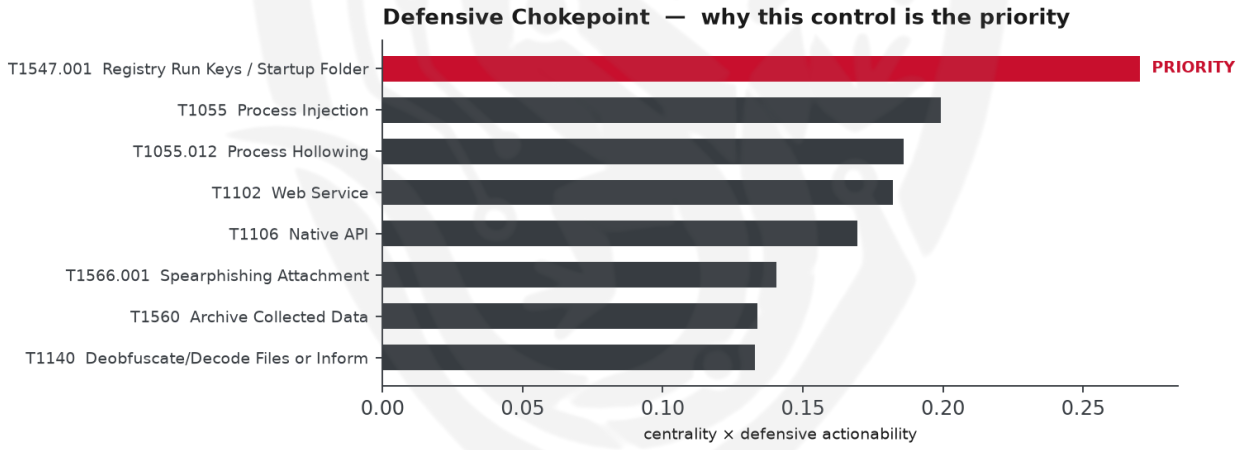
THREAT REPORT: APT37 OPERATION CAPSULE VAULT

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 APT37, who has been observed using the ROKRAT malware to target the Education and Government sectors. The threat actor's attack chain involves various techniques, including screen capture, malicious file execution, and process injection. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to mitigate the threat.

Threat Overview

The observed cluster of activity, attributed to APT37, involves the use of the ROKRAT malware family, which employs a range of techniques to achieve its goals. The victimology suggests that the Education and Government sectors are being targeted, although specific details on the targeted country are

insufficient. The malware's capabilities include screen capture, system information discovery, and data exfiltration.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including initial infection through spearphishing attachments, followed by screen capture, system information discovery, and process injection. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which is used to establish persistence on the compromised system. The concrete control to mitigate this threat is to "Audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries; alert on .lnk or script creation in Startup by browser/email temp paths."

Infrastructure and Corroboration

The malicious infrastructure associated with this activity is hosted on providers such as PacketHub S.A., Clouvider Limited, and DataCamp Limited. While there are no corroborated malware families from abuse.ch, AbuseIPDB has flagged some indicators with a low confidence level, with the highest confidence seen being 2%. These findings are attributed to their respective sources, including AbuseIPDB and the hosting providers.

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
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1106 Native API
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1560 Archive Collected Data
- T1083 File and Directory Discovery
- T1102 Web Service
- T1057 Process Discovery
- T1547.001 Registry Run Keys / Startup Folder
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1102.002 Bidirectional Communication
- T1518.001 Security Software Discovery
- T1059.003 Windows Command Shell

- T1485 Data Destruction
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2846).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5849; 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
Dark Caracal	0.5849
Windshift	0.5604
APT37	0.5582
Inception	0.5381
Darkhotel	0.5045

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 2%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	89[.]187[.]161[.]220	AbuseIPDB 2% (JP) · AS60068 DataCamp Limited
IP	5[.]180[.]208[.]57	AbuseIPDB 0% (US) · AS62240 Clouvider Limited
IP	5[.]180[.]208[.]60	AbuseIPDB 0% (US) · AS62240 Clouvider Limited
IP	160[.]238[.]37[.]95	AbuseIPDB 0% (KR) · AS147049 PacketHub S.A.

Type	Indicator	Context
IP	89[.]147[.]101[.]197	AbuseIPDB 0% (KR) · AS147049 PacketHub S.A.
IP	160[.]238[.]37[.]100	AbuseIPDB 0% (KR) · AS147049 PacketHub S.A.
Hash	e5c9bb3938f2a24e755ee39073fc3aca	

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:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Observed here:** T1547.001 Registry Run Keys / Startup Folder was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1053 Scheduled Task/Job (persistence)
- **Basis:** 37 of 170 documented groups that use Registry Run Keys / Startup Folder also use Scheduled Task/Job (conditional 0.64, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

The adversary, APT37, could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and achieve their objectives, potentially by creating a new scheduled task that masquerades as a legitimate system process. This technique may allow them to bypass the blocked Registry Run Keys / Startup Folder control, as scheduled tasks can still be used to execute malicious code at regular intervals. To counter this, the defensive control would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1078 Valid Accounts (n=27, lift 1.2), T1543 Create or Modify System Process (n=18, lift 1.8)

Detection and hardening for the pivot (T1053 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