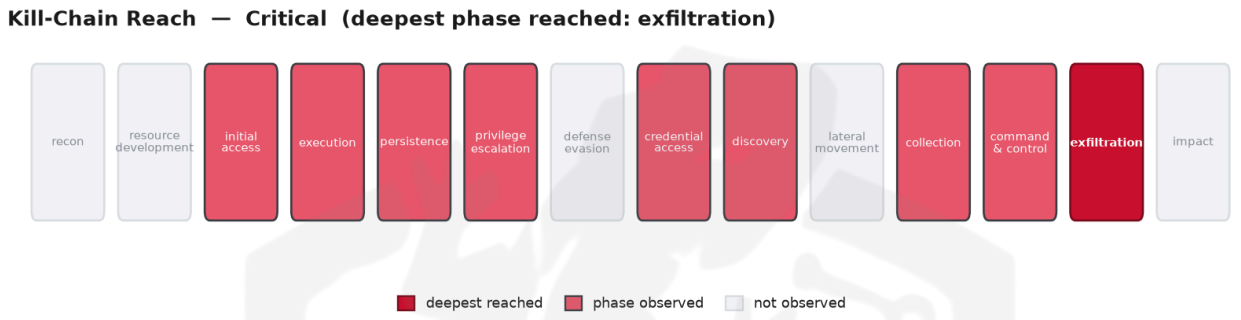
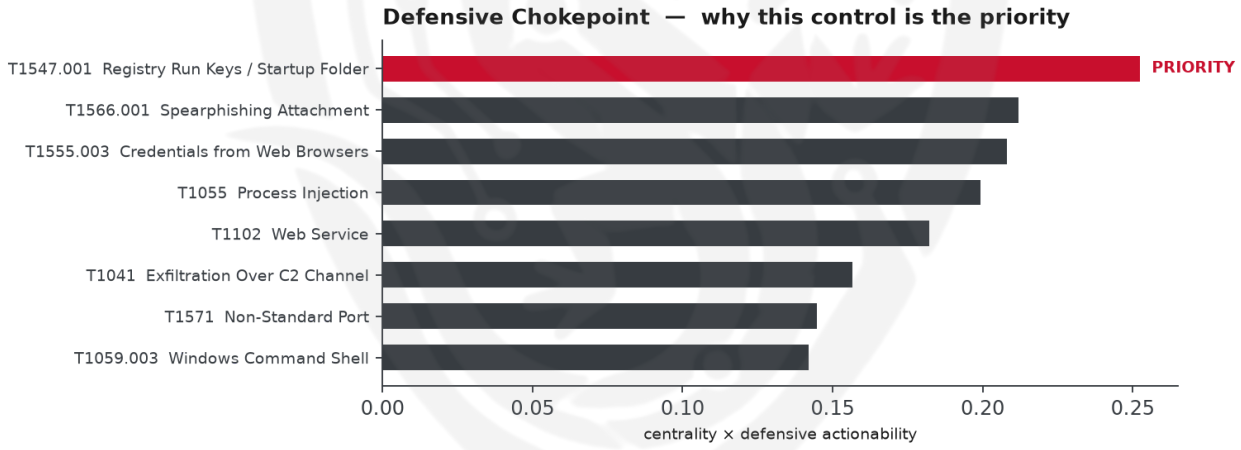
THREAT REPORT: DARK CARACAL TARGETS TELECOMMUNICATIONS IN SOUTH AMERICA

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 threat actor Dark Caracal is deploying the GoCaracal, Bandook – S0234, and AsioGate malware families against telecommunications providers in Brazil, Chile, Colombia, Ecuador, El Salvador, Uruguay, Venezuela and the Bolivarian Republic of … . No specific CVE is identified for the campaign. The observed techniques span credential harvesting, system discovery, process injection and data exfiltration. Priority should be given to auditing Windows startup folders and Run/RunOnce registry keys for unauthorized entries, and alerting on shortcut or script creation in those locations from browser or email temporary paths.

Threat Overview

Dark Caracal is leveraging multiple malware families—GoCaracal, Bandook – S0234, and AsioGate—to compromise telecommunications infrastructure across several South-American nations. The campaign does not cite a concrete vulnerability (the central CVE is listed as “Data Insufficient”). Victims are primarily telecom operators in the listed countries, with the adversary employing a broad set of ATT&CK techniques to gain persistence, harvest credentials, and exfiltrate data.

Attack Chain and Priority Control

The observed activity follows a typical intrusion sequence: initial spearphishing attachment (T1566.001) delivers a malicious file (T1204.002), which is then deobfuscated (T1140, T1027) and executed via Windows command shell (T1059.003). The malware performs system and process discovery (T1082, T1057), injects into legitimate processes (T1055), harvests credentials from browsers (T1555.003) and keylogs (T1056.001), and establishes persistence through registry run keys and the startup folder (T1547.001). Data is encrypted with symmetric cryptography (T1573.001) and exfiltrated over web-service channels (T1041, T1102) using non-standard ports (T1571) and internal proxies (T1090.001).

Priority technique: T1547.001 Registry Run Keys / Startup Folder
Priority control: 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

Third-party enrichment shows the command-and-control infrastructure is hosted by Aeza Group LLC and Mamut Rahal Software - Fzco. AbuseIPDB reports no high-confidence malicious indicators associated with the observed IPs, and abuse.ch does not list any corroborated malware families for this activity.

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
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1555.003 Credentials from Web Browsers
- T1083 File and Directory Discovery
- T1102 Web Service
- T1057 Process Discovery

- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1571 Non-Standard Port
- T1027 Obfuscated Files or Information
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1090.001 Internal Proxy

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2658).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.6051; 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
Inception	0.6051
Darkhotel	0.5732
Higaisa	0.551
Ajax Security Team	0.5285
APT37	0.5285

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
IP	45[.]152[.]198[.]108	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	176[.]124[.]220[.]153	AbuseIPDB 0% (FI) · AS210644 Aeza Group LLC
IP	82[.]117[.]87[.]192	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	82[.]117[.]87[.]138	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	185[.]96[.]80[.]54	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	109[.]120[.]187[.]217	AbuseIPDB 0% (FI) · AS210644 Aeza Group LLC
IP	109[.]172[.]95[.]121	AbuseIPDB 0% (FI) · AS210644 Aeza Group LLC
IP	138[.]124[.]112[.]213	AbuseIPDB 0% (FI) · AS210644 Aeza Group LLC
IP	138[.]124[.]14[.]130	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	185[.]125[.]101[.]181	AbuseIPDB 0% (FI) · AS210644 Aeza Group LLC
IP	185[.]96[.]80[.]110	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	193[.]233[.]245[.]45	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	193[.]233[.]245[.]52	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	46[.]226[.]162[.]68	AbuseIPDB 0% (GB) · AS210644 Aeza Group LLC
IP	62[.]60[.]237[.]22	AbuseIPDB 0% (FI) · AS210644 Aeza Group LLC
IP	77[.]110[.]104[.]98	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC

Type	Indicator	Context
IP	77[.]110[.]105[.]244	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	77[.]110[.]105[.]56	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	77[.]110[.]105[.]59	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	77[.]110[.]98[.]66	AbuseIPDB 0% (FI) · AS210644 Aeza Group LLC
IP	79[.]137[.]192[.]38	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
IP	80[.]71[.]224[.]30	AbuseIPDB 0% (IT) · AS198566 Mamut Rahal Software - Fzco
IP	85[.]192[.]30[.]211	AbuseIPDB 0% (RU) · AS216246 Aeza Group LLC
Domain	contabilidad[.]icu	
Domain	documentodigital[.]cloud	
Domain	getpdfdigital[.]cloud	
Domain	soportedigital[.]cloud	
Domain	gestionadocs[.]me	
Domain	getpdf[.]digital	
Domain	visualizarpdf[.]online	
Hash	27cc65cb6261ef0d584287cf09bdafcc	
Hash	40d99e70de5918c6cad144dfc1ad4acd806aca3b	
Hash	0a6da70548f14834acb8960689a589b48ff422f8385ae445a281aab77045fe22	

Type	Indicator	Context
Hash	1e499c815146124c4a6d2b48c99068b980ad74e1a2cfd16013f8d75a9425a0ca	
Hash	77f7ad29f4a8037ee5f38d3d87fb91cfd97cb8f7fa7883edf3fce506df5200c0	
Hash	8c03d072df2e1bf14b0c00a8ab99834138c8b69f301849bf09cb44394e916015	
Hash	a2cdf2fe741de4b13ad2298b387a6c32da4a94da180ae75bf8547386aee7376b	
Hash	c9da1b08a39491dfdbede6ff4c1a2d383f57cb29e2d3532aee08d6e0a5c1dda6	
Hash	9f2be216c5df190806e621e970c9f3e106048441	

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:** of the 37+ groups that use Registry Run Keys / Startup Folder, this pairing runs 1.9x above base rate, a disproportionately-coupled move rather than the obvious one.

With T1547.001 Registry Run Keys / Startup Folder blocked, Dark Caracal could preserve the same objective by pivoting to T1053 Scheduled Task/Job, a technique disproportionately paired with it across tracked groups. Defensive countermeasure: Alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1543 Create or Modify System Process (n=18, lift 1.8), T1098 Account Manipulation (n=12, lift 2.0)

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