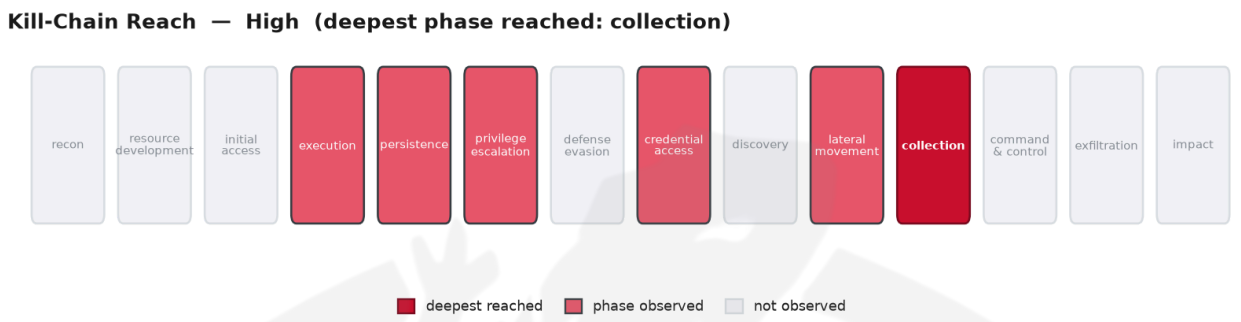
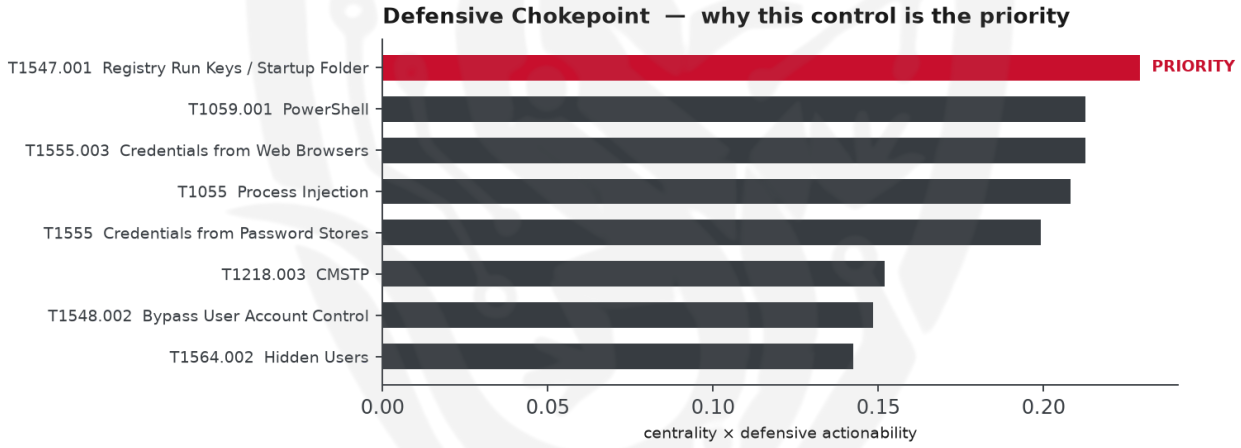
THREAT REPORT: APT-C-36

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 APT-C-36, a threat actor targeting the finance sector in Colombia. The actor utilizes a range of malware families, including AsyncRAT, njRAT, and LimeRAT, to compromise victim systems. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to mitigate the threat. The threat actor's use of various techniques, including screen capture and keylogging, poses a significant risk to sensitive information.

Threat Overview

APT-C-36, the observed threat actor, employs a toolkit that includes malware families such as AsyncRAT, njRAT, Njw0rm, LV, Bladabindi, and LimeRAT. The central vulnerability exploited is currently unknown. The threat actor targets the finance sector in Colombia, using various techniques to compromise victim systems.

Attack Chain and Priority Control

The threat actor's attack chain involves a range of techniques, including screen capture, keylogging, and process injection. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which serves as a chokepoint in the attack chain. To mitigate this threat, the priority control 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 is hosted on providers such as Omegatech LTD, Ghosty Networks LLC, and Colombia Telecomunicaciones S.A. ESP Bic. According to AbuseIPDB, none of the indicators have a confidence level of 80% or higher, with the highest confidence seen being 10%. Abuse.ch has not corroborated any malware families in this campaign.

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
- T1218.011 Rundll32
- T1056.001 Keylogging
- T1059.007 JavaScript
- T1548.002 Bypass User Account Control
- T1115 Clipboard Data
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1055 Process Injection
- T1218.003 CMSTP
- T1555.003 Credentials from Web Browsers
- T1125 Video Capture
- T1564.002 Hidden Users
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1059.005 Visual Basic
- T1021.001 Remote Desktop Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2413).
- Operational risk: High (score 0.604, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4315; 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
Molerats	0.4315
Silence	0.3888
Cobalt Group	0.3807
Gorgon Group	0.368
Patchwork	0.3459

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 10%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	178[.]16[.]52[.]80	AbuseIPDB 10% (DE) · AS202412 Omegatech LTD
IP	64[.]89[.]160[.]17	AbuseIPDB 1% (LU) · AS205759 Ghosty Networks LLC
IP	181[.]235[.]8[.]24	AbuseIPDB 0% (CO) · AS3816 Colombia Telecomunicaciones S.A. ESP Bic
Domain	rema200426[.]duckdns[.]org	

Type	Indicator	Context
Hash	a4fbd707f4ce7ca68e6137cef1c56b6f408e5f0a0f14 8434d996bb98c3a21fff	
Hash	a73cb9d5d46e19f3daa4a14cfe5d8fa4319a3d6245 2039e4972e6a316bbb26f4	

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 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, which may allow them to evade detection. This technique could be particularly effective if the adversary has already established a foothold on the system and has the necessary privileges to create scheduled tasks. To counter this potential move, the defensive control would involve alerting on new scheduled tasks (Event ID 4698); restricting 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