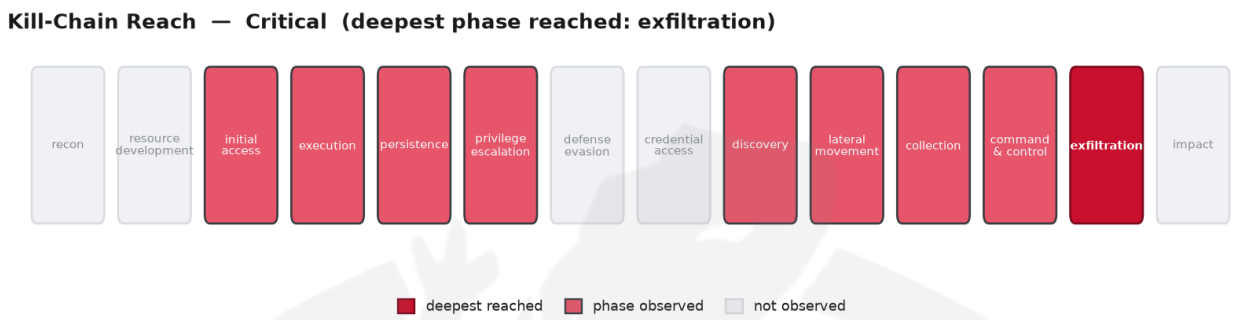
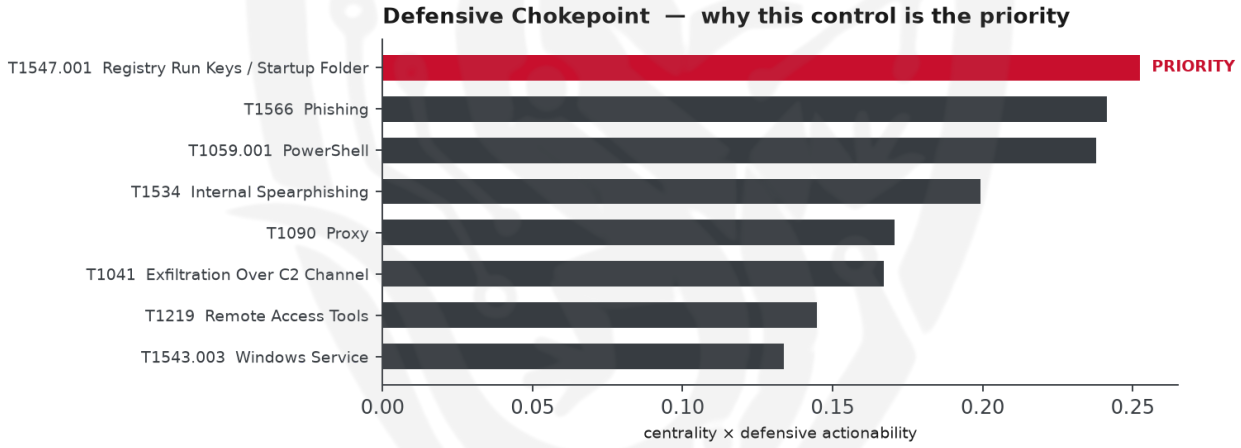
THREAT REPORT: HELPDESK HIJACKERS CAMPAIGN

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 involves the use of multiple malware families, including GoGRPC, BlindDoor, and RevSocket, to target unspecified sectors and countries. The threat actor's goals and motivations are unclear, but the campaign's use of techniques such as system owner discovery and permission groups discovery suggests a high level of sophistication. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. The campaign's ability to reach exfiltration stages poses a critical operational risk.

Threat Overview

The threat actor, whose identity is insufficient to determine, is utilizing a range of malware families, including GoGRPC, BlindDoor, RevSocket, PyGRPC, S3Siphon, and RSOX, to carry out their campaign. The victimology and targeted countries are unclear, but the techniques used suggest a focus on system

discovery and exploitation. The malware families used are diverse, indicating a potentially wide range of goals and motivations.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, including system owner discovery, permission groups discovery, and system information discovery. 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 associated with this campaign is hosted by various providers, including GWY IT Pty Ltd, SIA Nano IT, Global Connectivity Solutions LLP, and Michael Sebastian Schinzel Trading as IP-Projects GmbH & Co. KG. However, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB, 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)

- T1033 System Owner/User Discovery
- T1069 Permission Groups Discovery
- T1543.003 Windows Service
- T1082 System Information Discovery
- T1005 Data from Local System
- T1219 Remote Access Tools
- T1016 System Network Configuration Discovery
- T1090 Proxy
- T1482 Domain Trust Discovery
- T1083 File and Directory Discovery
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1534 Internal Spearphishing
- T1547.001 Registry Run Keys / Startup Folder
- T1566 Phishing
- T1573.002 Asymmetric Cryptography
- T1518.001 Security Software Discovery
- T1071.001 Web Protocols
- T1018 Remote System Discovery

- T1105 Ingress Tool Transfer

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 0.4709; 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	0.4709
Stealth Falcon	0.4499
Tropic Trooper	0.4455
Windigo	0.4447
Windshift	0.4404

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	94[.]140[.]114[.]192	AbuseIPDB 0% (LV) · AS43513 SIA Nano IT
IP	45[.]86[.]162[.]228	AbuseIPDB 0% (NL) · AS199959 GWY IT Pty Ltd
IP	5[.]253[.]59[.]222	AbuseIPDB 0% (NL) · AS215540 Global Connectivity Solutions LLP
IP	193[.]29[.]57[.]37	AbuseIPDB 0% (DE) · AS48314 Michael Sebastian Schinzel Trading as IP-Projects GmbH & Co. KG

Type	Indicator	Context
IP	46[.]30[.]191[.]126	AbuseIPDB 0% (NL) · AS199959 GWY IT Pty Ltd
IP	46[.]30[.]191[.]60	AbuseIPDB 0% (NL) · AS199959 GWY IT Pty Ltd
Domain	scansec-upd[.]com	
Domain	re102[.]fastwinnow[.]com	
Domain	re2[.]filesdwnload[.]top	
Domain	re8[.]dowlfles[.]online	
Domain	update19[.]upldf[.]online	
Domain	xeds[.]geranteeg[.]online	
URL	hxxp://re102[.]fastwinnow[.]com/download/link	
Hash	3d1819de80c5a6633bc546f7b07086a4	
Hash	7a818efa2a3af3130a3c4b69260a08aa	
Hash	925dc63fc70de650127f41e00e9ffbf3	
Hash	b42366dcf2612adb43ed0c617bfa98d4	
Hash	b6a74fcadf1efca4e9f01658529556bc	
Hash	1d93080e7e97cd265e259a5e6f4d76e5583ed211	
Hash	233dbba4110d6d52d5378eb8ca6e8edb5f271445	
Hash	3f25712f02617eda348f1703bb1096e8a121ceaf	
Hash	7ddb7a07d5ecb0056f545306225e7a59a8bc2753	
Hash	a6491268ab79940dcbb811c32f1b19a988219814	

Type	Indicator	Context
Hash	35ea50f16bd5c080c91dbaa3dd4937408ed95 63c1d9aa1cd0c751ae58db0eedc	
Hash	41748648b71a70431123ec48e38868ff8aad3 a7a06f5d781c2d2a4f718e7fd91	
Hash	51edd14233483bcf36e0b0f31451f28eac681f e3f2036f76c02b7ec1bb17ce33	
Hash	5d53246b0e6b681bc624739a7bead39a61fb0 7c0f4474b8170112e829c053f85	
Hash	65af5c3ba2d00967b25b9165d2d3171fa81f20 9ee0790299805bb907d492a670	
Hash	66b2b22397cea219266afb8cbbb28fe93997c 1444f642a183ac8fc9ca1fabed5	
Hash	759287052b8cc4f4ce16065857cbc9dba72aa b218e709d3419483a95092c6f96	
Hash	7dcabb6d07d52b92bbf8d659d1ed373fa780e 7839fd3d744826a56fc1cd2372f	
Hash	9136ffb749c6cec13b826cd4f25ffdcf17037588 9feba9fee28dd74c32578f52	
Hash	f36bfccf944b5d1e5e306958c1a728e38786c0 42ee4e536cc44c9d43940b1121	
Hash	f85960dee17ba587b712cd8cdf89042bcd6ba 711c3d5d548bef7c7f0988413f5	

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.

The actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious code at a later time, potentially leveraging the Windows Task Scheduler to blend in with legitimate system activity, which may allow them to bypass the initial block on registry run keys and startup folders. This technique in particular could be appealing to the actor because it enables them to schedule tasks to run under the context of a specific user or system account, which may provide the necessary privileges to achieve their objectives. To counter this potential move, the defensive control of alerting on new scheduled tasks (Event ID 4698), restricting schtasks/at to admins, and baselining legitimate task creators should be implemented.

Also plausible (same tactic): T1098 Account Manipulation (n=12, lift 2.0), T1112 Modify Registry (n=17, lift 1.7)

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