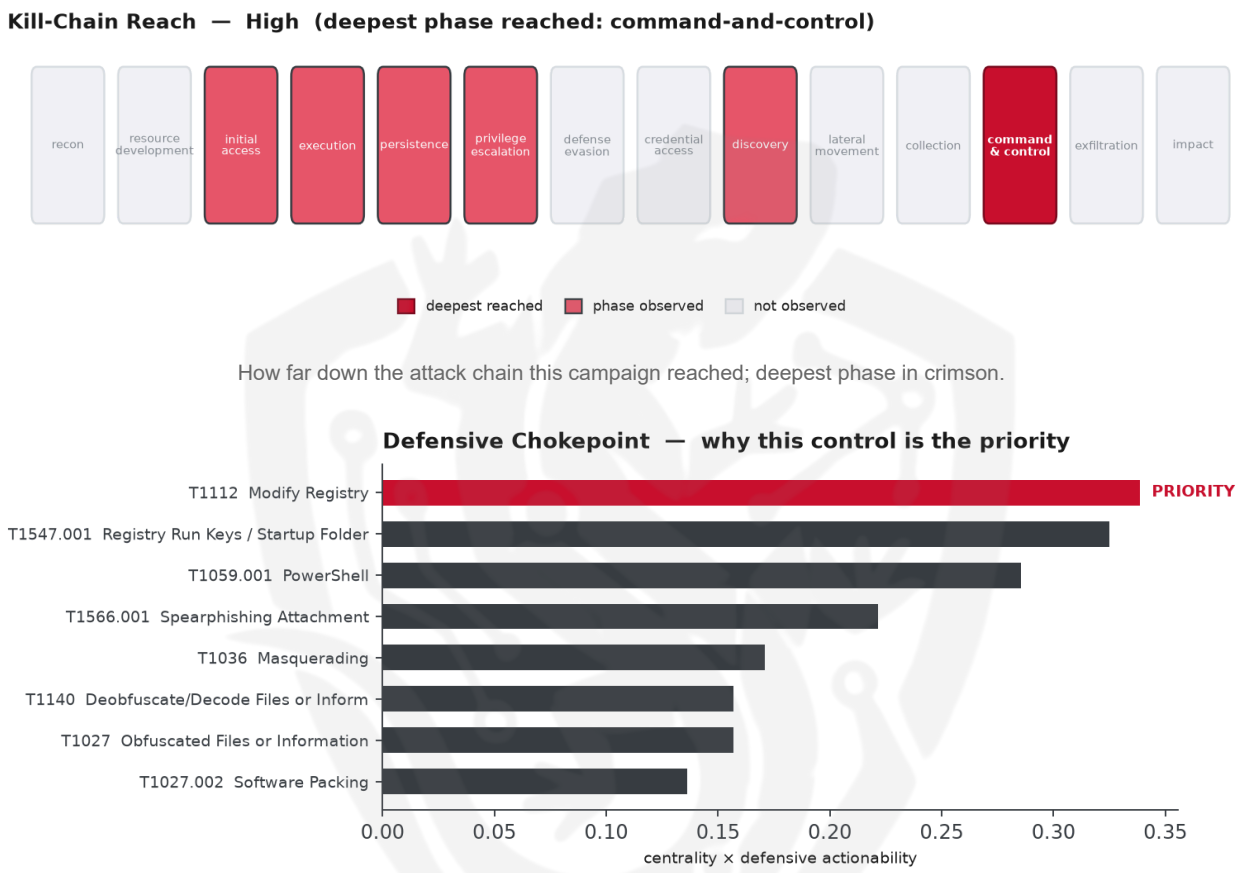
THREAT REPORT: SIDECOPY

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 SideCopy, a threat actor that has been observed targeting the British Indian Ocean Territory and India, specifically the defense sector. The actor utilizes the pdfdocs RAT malware family to carry out their operations. Priority should be given to monitoring sensitive registry keys for modification and restricting registry-edit tools for unprivileged users. The threat actor's activities pose a high operational risk, reaching the level of command-and-control.

Threat Overview

SideCopy, the observed threat actor, employs the pdfdocs RAT malware family to target the defense sector in the British Indian Ocean Territory and India. Although the central CVE is insufficient, the actor leverages various techniques, including boot or logon autostart execution, malicious files, and spearphishing attachments. The victimology suggests a focused effort on compromising defense-related systems.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including boot or logon autostart execution, malicious files, and spearphishing attachments, ultimately leading to the modification of registry keys. The priority technique is T1112 Modify Registry, which serves as a chokepoint in the attack chain. To mitigate this threat, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

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 no indicators have been flagged with an AbuseIPDB confidence of 80% or higher, 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)

- T1547 Boot or Logon Autostart Execution
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1036 Masquerading
- T1112 Modify Registry
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1204.001 Malicious Link

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3566).
- 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 0.6736; 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
Windshift	0.6736
APT19	0.5833
Nomadic Octopus	0.5685
Molerats	0.5657
LazyScripter	0.5594

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
Hash	ad7e4f47f9ddb2f97c8818d89374a82278922bac1bc41209ecd0b5ad027dcb45
Hash	b3007c3b0f140df374a6756215bde55409124822203d309dcc82e10aa8115a91
Hash	db1cb4aaee4ad2f1b2907b2c2d3393544a6a05f9a4d8819eb0078606402c416c
Hash	e9f8a7e6275c263d2a1c9c5c9725addbf484c77c1aa8387093c16f50ebdc11ab

---

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:** T1112 Modify Registry (persistence)
- **Observed here:** SideCopy used T1547 Boot or Logon Autostart Execution here as an alternative persistence technique.
- **Projected pivot:** T1547 Boot or Logon Autostart Execution (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The SideCopy actor could pivot to using T1547 Boot or Logon Autostart Execution to maintain persistence, potentially by adding entries to the startup folder or Run keys, if they were previously relying on modifying the registry to achieve their objectives. This would likely involve exploiting legitimate system features to automatically execute their malware upon boot or logon. The defensive countermeasure to mitigate this potential pivot would be to baseline and monitor autostart locations (Run keys, startup folders); alert on new persistence entries.

Detection and hardening for the pivot (T1547 Boot or Logon Autostart Execution)

- **Telemetry:** Sysmon (registry + process); EDR autostart/ASEP inventory
- **Detect:**
  - Sysmon 13 (registry value set) on Run/RunOnce keys under HKLM & HKCU ...\CurrentVersion\Run*
  - Sysmon 11 for shortcuts/scripts created in Startup folders
  - Periodic ASEP (autostart extensibility point) diff against a known-good baseline
- **Harden:**
  - Restrict write access to autostart registry keys and Startup folders
  - Application control to block unsigned autostart binaries
- **MITRE:** M1047 Audit, M1038 Execution Prevention · DS0019 Service, DS0024 Windows Registry, DS0022 File