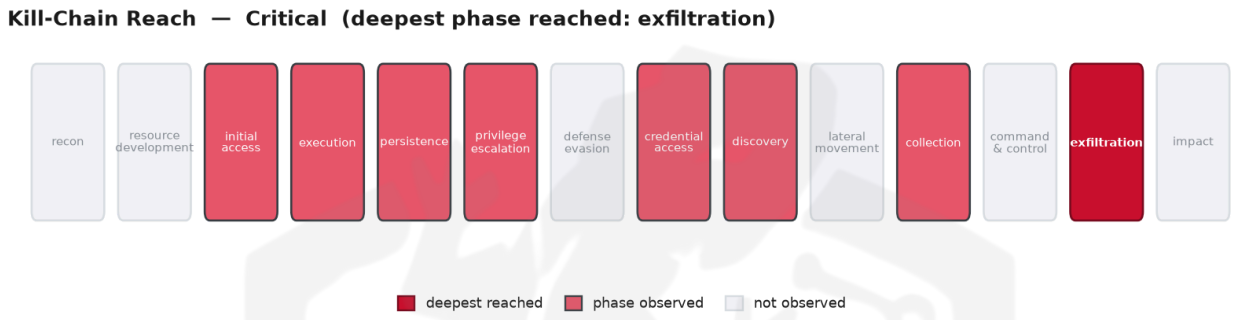
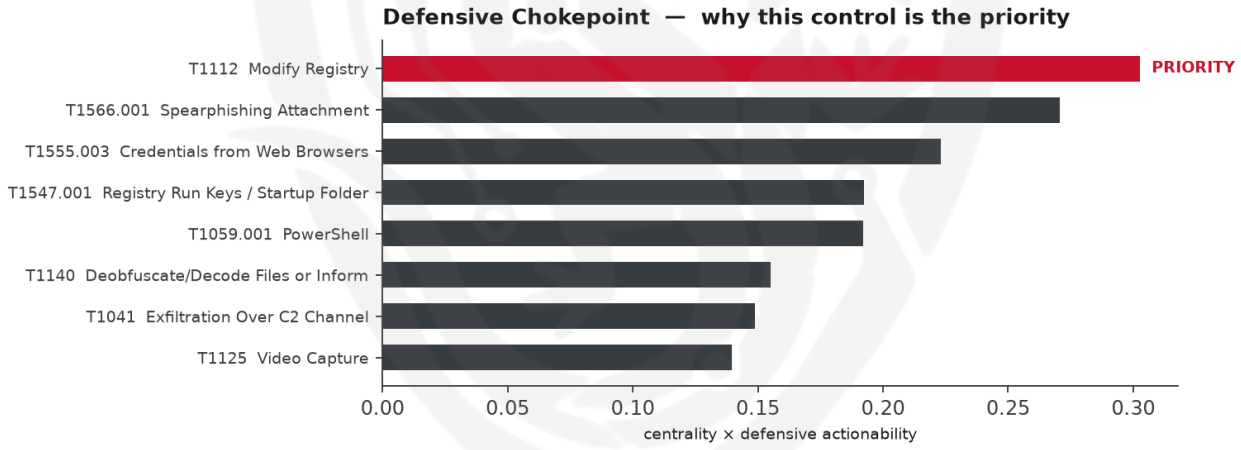
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 has been deploying a diverse set of malware payloads, including Remcos RAT, Agent Tesla, and others, targeting the finance sector in the British Indian Ocean Territory and India. The threat actor is exploiting various techniques to gain access to sensitive information. Priority should be given to monitoring sensitive registry keys for modification to prevent further damage. The campaign's ability to exfiltrate data over command and control channels poses a significant risk.

Threat Overview

The threat actor, whose identity is currently unknown, is utilizing a range of malware families, including Remcos RAT, Agent Tesla, MassLogger, and others, to target finance sector organizations. The exploited vulnerability is not specified, but the actor is using techniques such as screen capture, keylogging, and

audio capture to gather sensitive information. The victimology suggests a focus on the British Indian Ocean Territory and India.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, starting with initial access and progressing to techniques such as spearphishing attachment, file and directory discovery, and data exfiltration over command and control channels. The priority technique is T1112 Modify Registry, which serves as a chokepoint in the attack chain. To mitigate this, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The malware families used in this campaign, including Remcos and RemcosRAT, have been corroborated by abuse.ch. However, there is no available information on the hosting providers or ASNs observed, and AbuseIPDB has not flagged any indicators with high confidence.

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
- T1123 Audio Capture
- T1497.001 System Checks
- T1566.001 Spearphishing Attachment
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1112 Modify Registry
- T1555.003 Credentials from Web Browsers
- T1125 Video Capture
- T1083 File and Directory Discovery
- T1041 Exfiltration Over C2 Channel
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1564.001 Hidden Files and Directories

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3187).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4414; 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
Gorgon Group	0.4414
Molerats	0.4234
APT19	0.4082
RedCurl	0.3975
Dark Caracal	0.3974

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Remcos, RemcosRAT.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
Hash	372f19a45d0eb4c8c52117c6ae2bb8040a91bc72be8670623f957a18c2166985	Remcos
Hash	897abf678edad72998554ec18675092f	RemcosRAT
Hash	afe085b7324d72673eef749ff5f21a49	
Hash	c2e25aba8e2ad4cafdd6c633b8ca0906	
Hash	be36ef651eed6808760153200a3a2a2b7060cce5	RemcosRAT
Hash	4924369c0bdaf73b21eb992eb9db4dea	

Type	Indicator	Context
Hash	f3626a38fcf488c9eed54beb8c7c116f	

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:** T1112 Modify Registry (persistence)
- **Observed here:** the threat actor used T1547.001 Registry Run Keys / Startup Folder here as an alternative persistence technique.
- **Projected pivot:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to using T1547.001 Registry Run Keys / Startup Folder to maintain persistence, potentially by adding malicious entries to the Startup folder or Run/RunOnce registry keys, which may allow them to regain a foothold after the block on registry modifications. This technique may be used to execute malicious code automatically when a user logs in, which would likely undermine the defender's previous control. To counter this potential move, the mandated defensive 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.

Detection and hardening for the pivot (T1547.001 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