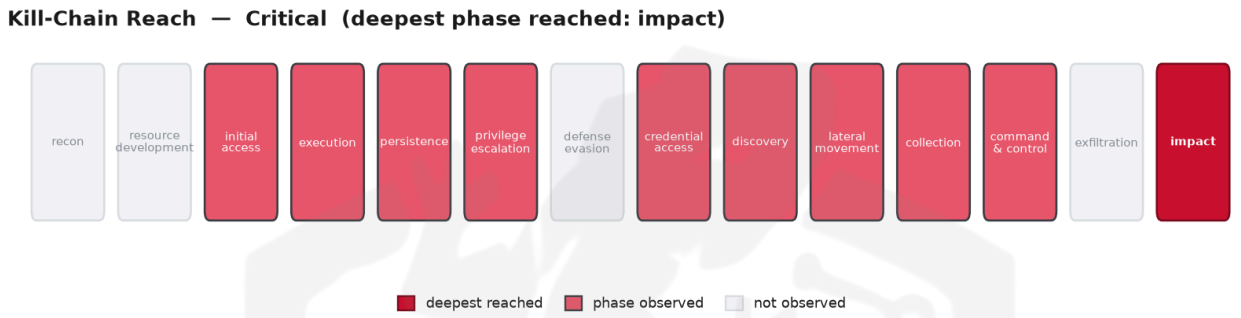
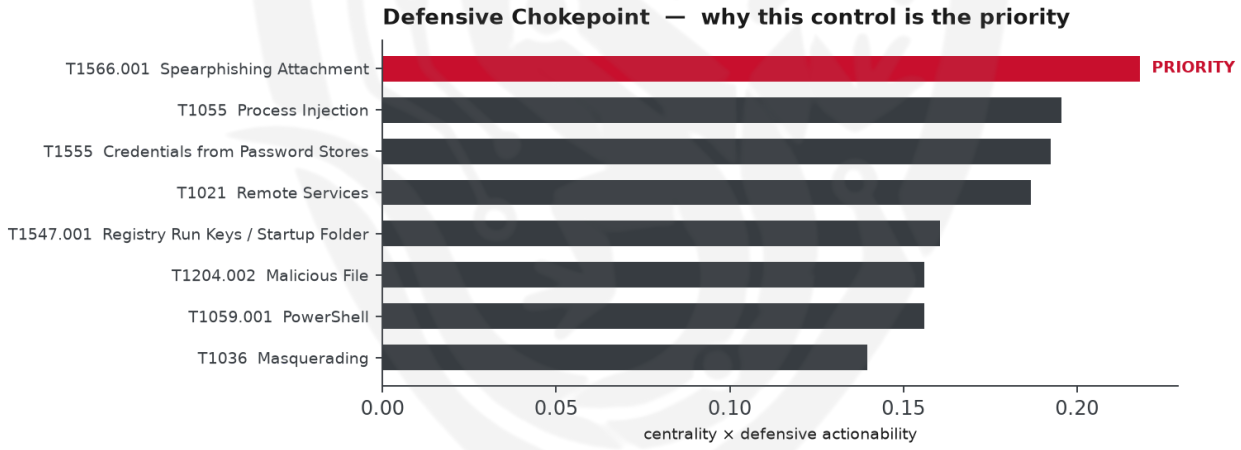
THREAT REPORT: UNKNOWN_ADVERSARY BEHIND THE REFUND CAMPAIGN

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 targeting the British Indian Ocean Territory and India, specifically the finance and government sectors, with a multi-stage .NET infection chain leading to Remcos RAT deployment. The threat actor's tactics involve various techniques to evade detection and gain control over compromised systems. Priority should be given to defensive actions that focus on email attachments and executable contents. The campaign's impact is considered critical, reaching the 'impact' level of operational risk.

Threat Overview

The threat actor, whose identity is unknown, is utilizing the Remcos RAT malware family to target victims. Although the central CVE is insufficient, the actor's techniques include screen capture, keylogging, and

bypassing user account control, among others. The targeted countries are the British Indian Ocean Territory and India, with a focus on the finance and government sectors.

Attack Chain and Priority Control

The observed techniques form a complex chain, starting with initial infection and leading to various tactics such as system information discovery, process injection, and data exfiltration. The priority technique is T1566.001 Spearphishing Attachment, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended control is to: Sandbox and detonate email attachments; block executable/script archive contents at the gateway; strip mark-of-the-web bypass; user report-phish button.

Infrastructure and Corroboration

There is no available information on hosting providers or ASNs observed in this campaign. Additionally, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with a confidence level of 80% or higher 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)

- T1113 Screen Capture
- T1056.001 Keylogging
- T1129 Shared Modules
- T1548.002 Bypass User Account Control
- T1489 Service Stop
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1036 Masquerading
- T1055 Process Injection
- T1218.003 CMSTP
- T1021 Remote Services
- T1016 System Network Configuration Discovery
- T1083 File and Directory Discovery
- T1057 Process Discovery
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1039 Data from Network Shared Drive

- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1566.001 Spearphishing Attachment (centrality 0.2182).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5311; 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
APT37	0.5311
Dark Caracal	0.5272
Inception	0.5154
Darkhotel	0.5154
Windshift	0.5052

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	07d7d21c2c0920d198efb9ea54900a80
Hash	20476f3a51dfddf3dc0603fc7858d894
Hash	2a34bdd25b404737ee5d3b52bf0b3b70
Hash	3757dccb2adae65ccdf8d5e5c948b927

Type	Indicator
Hash	7842d12d9e37c75076133be5b9904cb2
Hash	cc34d9760394104ad47877a0d57e9c63

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:** T1566.001 Spearphishing Attachment (initial-access)
- **Observed here:** T1566.001 Spearphishing Attachment was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1189 Drive-by Compromise (initial-access)
- **Basis:** 27 of 170 documented groups that use Spearphishing Attachment also use Drive-by Compromise (conditional 0.28, lift 1.5, i.e. ~1.5x base rate). Strongest same-tactic neighbour.

The actor could pivot to T1189 Drive-by Compromise by exploiting vulnerabilities in software or plugins to compromise a user's system, potentially achieving their objective if the user visits a malicious website. This technique may be used in conjunction with social engineering tactics to increase the likelihood of a successful compromise. The defensive control to mitigate this potential pivot would be to enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.

Also plausible (same tactic): T1195 Supply Chain Compromise (n=9, lift 1.4), T1199 Trusted Relationship (n=9, lift 1.3)

- **Defensive countermeasure:** Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.