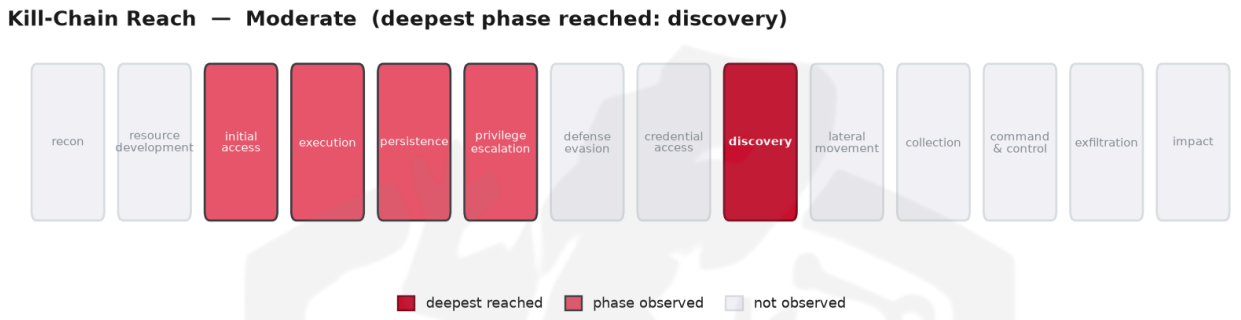
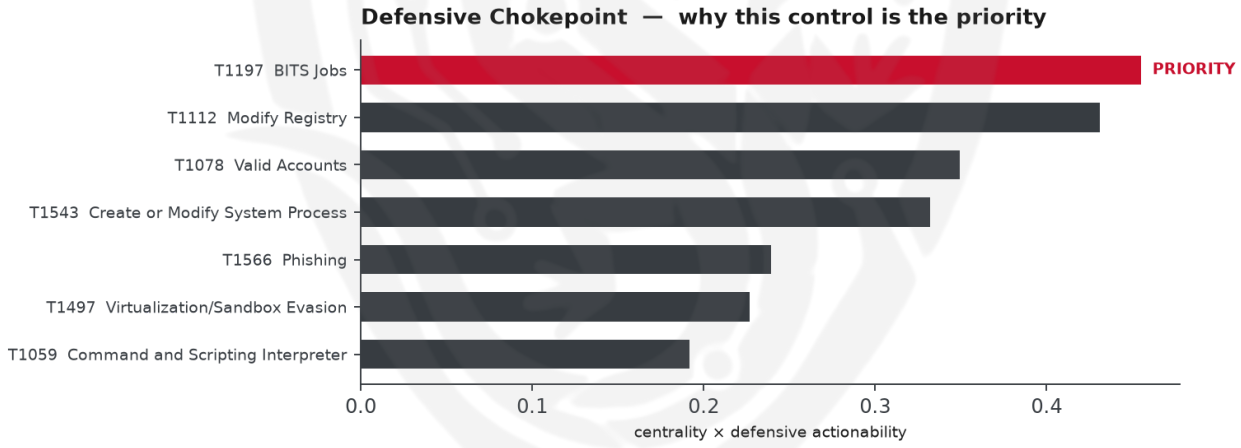
THREAT REPORT: OPERATION C-MAJOR RECRUITMENT-THEMED MALWARE CAMPAIGN

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 source attributes this activity to Operation C-Major, a threat actor leveraging malware families SheetAgent and PrivateRat to target Indian job seekers. The campaign primarily focuses on the Government, Education, and Technology sectors in India and the British Indian Ocean Territory. Priority should be given to defending against the exploitation of legitimate system features. The threat actor's use of recruitment-themed malware poses a significant risk to individuals and organizations alike.

Threat Overview

Operation C-Major is utilizing the SheetAgent and PrivateRat malware families to target individuals in the Government, Education, and Technology sectors. The reporting indicates techniques inferred from the report include Command and Scripting Interpreter, Valid Accounts, Modify Registry, BITS Jobs,

Virtualization/Sandbox Evasion, Create or Modify System Process, and Phishing. The victimology suggests a focus on Indian job seekers, with the threat actor exploiting the trust associated with recruitment processes.

Attack Chain and Priority Control

The observed techniques suggest a complex attack chain, with the threat actor leveraging various tactics to evade detection and gain access to targeted systems. The priority technique is T1197 BITS Jobs, which is the graph chokepoint. The lead control is to Apply the specific MITRE ATT&CK mitigation for this technique; add host/network detections and least-privilege controls around it.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this campaign, and no malware families have been corroborated by abuse.ch. Additionally, AbuseIPDB has not flagged any indicators with a confidence level 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, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1059 Command and Scripting Interpreter - T1078 Valid Accounts - T1112 Modify Registry - T1197 BITS Jobs - T1497 Virtualization/Sandbox Evasion - T1543 Create or Modify System Process - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1197 BITS Jobs (centrality 0.4789).
- Operational risk: Moderate (score 0.435, reaches discovery).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.2965; 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
Saint Bear	0.2965
Suckfly	0.2857
Threat Group-1314	0.2857
APT19	0.2673
TA459	0.2673

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	6bcf91af52b9577ba81cbae9368f91f8
Hash	6f2fd5cb3901d6818316423ac72da5e8
Hash	90682a7c53132750b1517f80cab2281c
Hash	081747ca2a2f4be07b52ab1da0c76b8e508248a7
Hash	a154f9bff1999be4a42ffc4cbfc686e64a163997
Hash	c1a691fdd339709439774e9402b71a4b4ba50f42
Hash	2b33b5185e93e1655eb27dbaa025d7ee088627db3d640fe4709be705646b189c
Hash	434243e615b93a1b948c26ad55902bd78f9fa18e42375c15790634375c1ad3f4
Hash	70fe7576f20f5dd6a3d872753c922f1394d91487f5eabb417b240b83c22e31b2
Hash	b928e523b51187b932e48a65d36ce3d0c39ee9d409d493b90f98cf3d1e0e73b0
Hash	c4859db541b2bd0d266bbc44fafb5a767c862a57a3633a949dfaeebdf88ed529
Hash	cf3f1bceb83fa3acefbabae4bdc275347cfe03dd7fc770052a33baef204a89f7
Hash	ee9dd2a180aea75af5c0eda16b83681c0a5fed451bfad6d5b3af85c3b62fa210
Hash	fd2ac3a761f66dc6954014532795f9108f65739f23e4b294d4563673b7996881

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:** T1197 BITS Jobs (execution)
- **Observed here:** T1197 BITS Jobs was the only execution technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1053 Scheduled Task/Job (execution)
- **Basis:** of the 4+ groups that use BITS Jobs, this pairing runs 2.3x above base rate, a disproportionately-coupled move rather than the obvious one.

The Operation C-Major actors could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious code at a scheduled time, potentially leveraging the Windows Task Scheduler to blend in with legitimate system activity, which may allow them to bypass initial detection. This technique in particular could be appealing as it enables the actors to execute tasks with elevated privileges, which would likely be necessary to achieve their objectives. To counter this, the defensive control would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1569 System Services (n=3, lift 6.0), T1203 Exploitation for Client Execution (n=3, lift 2.5)

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