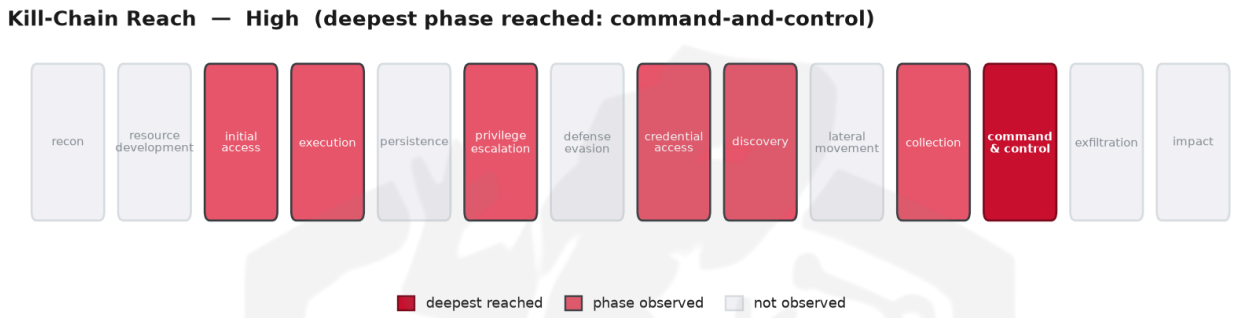
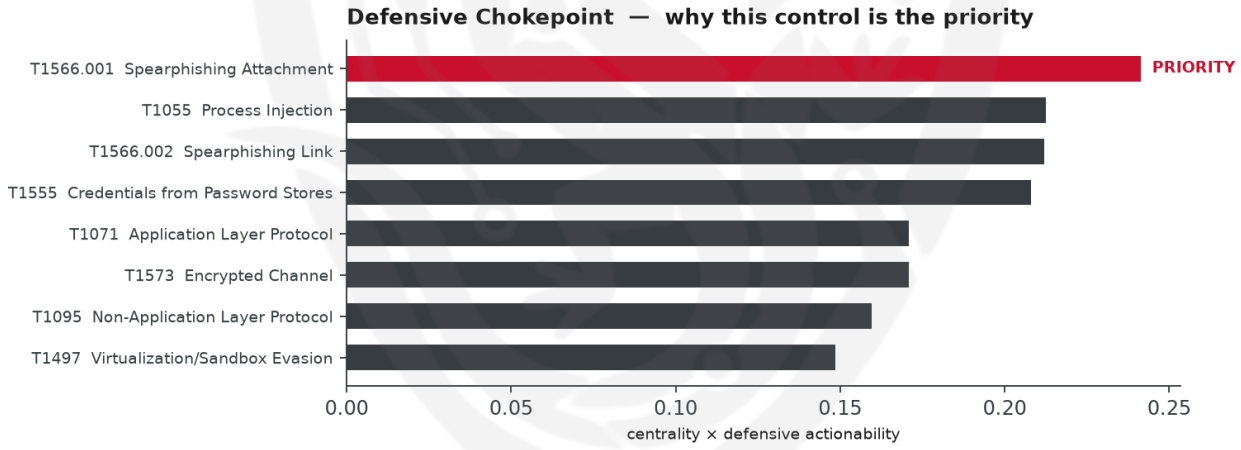
THREAT REPORT: INDIAN TAXPAYERS TARGETED BY PHISHING AND MALWARE CAMPAIGNS

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 is targeting Indian taxpayers, leveraging various techniques to compromise systems. The threat actor is exploiting multiple vulnerabilities, with a focus on spearphishing attachments. Priority should be given to defensive actions that block malicious email attachments and executable contents at the gateway. The campaign's operational risk band is considered high, as it reaches command-and-control levels.

Threat Overview

The threat actor, whose identity is not specified, is utilizing a range of techniques, including keylogging, stealing web session cookies, and spearphishing, to target individuals in the British Indian Ocean Territory and India. The malware families and central CVE used in the campaign are not specified. The actor's

techniques include system information discovery, application layer protocol, and credentials theft from password stores.

Attack Chain and Priority Control

The observed techniques form a complex chain, with the priority technique being T1566.001 Spearphishing Attachment, which serves as a chokepoint in the attack chain. To mitigate this threat, the priority 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 observed hosting provider or ASN associated with this campaign, and no malware families have been corroborated by abuse.ch. Additionally, 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)

- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1071 Application Layer Protocol
- T1555 Credentials from Password Stores
- T1055 Process Injection
- T1016 System Network Configuration Discovery
- T1497 Virtualization/Sandbox Evasion
- T1573 Encrypted Channel
- T1095 Non-Application Layer Protocol
- T1012 Query Registry
- T1518.001 Security Software Discovery
- T1027.002 Software Packing
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer
- T1204.001 Malicious Link

Analytical Scores

- Priority technique (graph chokepoint): T1566.001 Spearphishing Attachment (centrality 0.2413).
- 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 0.5381; 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
Darkhotel	0.5381
Windshift	0.5204
TA2541	0.5144
Elderwood	0.5095
PLATINUM	0.5064

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
Domain	laoshunfa[.]xyz
Domain	gov-xnui[.]com
Domain	gova[.]lat
Domain	indiaaba[.]com
Domain	apeal[.]lol
Domain	audet[.]club
Domain	bcgovtop[.]lol

Type	Indicator
Domain	ckoming[.]study
Domain	clerk[.]lat
Domain	fsyahsxd[.]xin
Domain	gisudyawz[.]ink
Domain	gova[.]bar
Domain	govj[.]one
Domain	govtocki[.]shop
Domain	ingovtop[.]click
Domain	kcsueaw[.]xin
Domain	konimqh[.]study
Domain	laiuatexqw[.]cc
Domain	lzaiwugsa[.]ink
Domain	oder[.]autos
Domain	qaksdiuw[.]xin
Domain	sfinmgov[.]club
Domain	tarif[.]lol
Domain	tzawccsw[.]xin
Domain	xcvgyuraw[.]live
Domain	zasudtytw[.]xin
Domain	zixhasda[.]xin
Domain	zuytyarws[.]xin
Domain	zxizusuy[.]xin
Domain	zytsyxbwa[.]live
Domain	22[.]laoshunfa[.]xyz
URL	hxxp://gova[.]lat/1[.]html

Type	Indicator
URL	hxxp://govj[.]one/index[.]html
Hash	2d85a7a16d1eb86dfd92b00f6267733d
Hash	538ad8e0ad1fec0ecc54f9e120ac6ff9
Hash	dff2b7a23882445b4e354199bf38554f
Hash	7479fbc27320ae246db9030cca80809ec63de0e9
Hash	667b37eafb9ec5131ed4f017ed429a47dca3adf626b2fc85fc6424b1e17ff6e1

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 initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 38+ groups that use Spearphishing Attachment, this pairing runs 1.6x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1203 Exploitation for Client Execution to keep their objective after the block, as this technique may allow them to execute malicious code on the client-side by exploiting vulnerabilities in commonly used software, potentially bypassing the initial spearphishing attachment block. This technique in particular could be appealing as it would likely enable the actor to leverage existing vulnerabilities in client applications, such as browsers or office software, to gain execution. The defensive countermeasure to mitigate this potential pivot would be to patch client applications, enable exploit mitigations, and implement application isolation.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=43, lift 1.3), T1106 Native API (n=18, lift 1.6)

Detection and hardening for the pivot (T1203 Exploitation for Client Execution)

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**
  - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs
  - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash

    - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
    - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
    - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015 Application Log