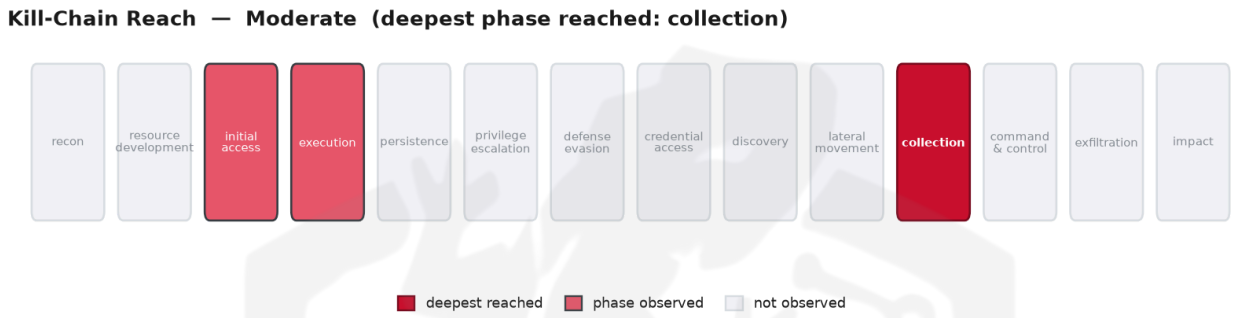
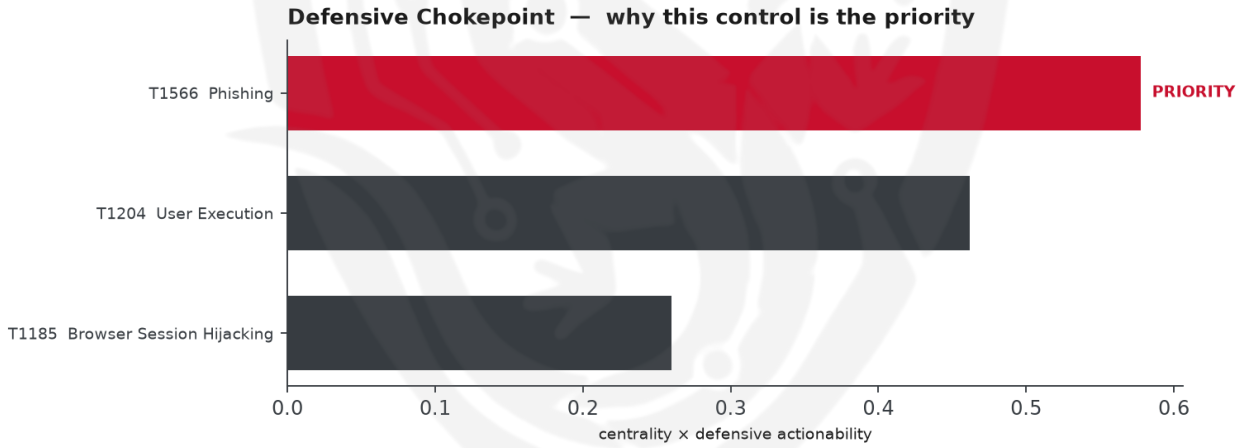
THREAT REPORT: GLOBAL PROCUREMENT-THEMED AITM PHISHING CAMPAIGN

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 is targeting the Education, Government, and Finance sectors through a procurement-themed AiTM phishing campaign. The reporting indicates techniques inferred from the report include browser session hijacking, user execution, and phishing. Priority should be given to hardening against social-engineering delivery to mitigate the threat. The campaign's operational risk band is moderate, reaching the collection stage.

Threat Overview

The threat actor, whose identity is not specified, is engaging in a phishing campaign targeting multiple sectors. The techniques inferred from the report include browser session hijacking, user execution, and

phishing, with phishing being the priority technique. The victimology suggests a focus on Education, Government, and Finance sectors.

Attack Chain and Priority Control

The observed techniques form a chain that starts with phishing, potentially leading to browser session hijacking and user execution. The priority technique is T1566 Phishing, which is the graph chokepoint. To mitigate this threat, the lead control is to: Harden against social-engineering delivery across email, links and voice/callback lures: attachment sandboxing and link rewriting, block macro-enabled Office docs from the internet zone, train users to verify unexpected requests out-of-band, deploy a report-phish button, and enforce phishing-resistant MFA.

Infrastructure and Corroboration

The campaign's infrastructure is not directly attributed to specific hosting providers or ASNs. However, abuse.ch corroborates the presence of the IClickFix malware family. According to AbuseIPDB, there are no 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. - T1185 Browser Session Hijacking - T1204 User Execution - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.5774).
- Operational risk: Moderate (score 0.416, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5774; 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
APT30	0.5774
TA459	0.4082
AppleJeus	0.4082
APT12	0.3849
Mofang	0.3849

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: IClickFix.
- 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
Domain	sohantraders[.]com	
Domain	satoriestate[.]com	
Domain	company[.]com	IClickFix
Domain	duemineral[.]uk	
Domain	assessmentevaluationreport[.]com	
Domain	barifurniture[.]net	
Domain	consistenthostinghub[.]de	
Domain	corporatetermscompliance[.]com	
Domain	designenhancessatisfaction[.]de	
Domain	employeehandbookcompliance[.]com	
Domain	esignidentification[.]com	
Domain	evergreenhostingoptions[.]de	
Domain	innovativegrowthstrategy[.]de	

Type	Indicator	Context
Domain	q1evaluationperformance[.]net	
Domain	reliablecontinuitysolutions[.]de	
Domain	solidhostingservices[.]de	
Domain	sustainablegrowthlaunch[.]de	
Domain	testserveren[.]com	
Domain	usersatisfactionlab[.]de	
Domain	vresortsliving[.]com	
Domain	ajgroupuae[.]usersatisfactionlab[.]de	

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:** T1566 Phishing (initial-access)
- **Observed here:** T1566 Phishing 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 Phishing, 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 maintain their objective by leveraging vulnerabilities in client applications, such as browsers or Office software, which may be exposed if the initial phishing attempt was intended to establish a foothold. This technique may be particularly appealing as it could allow the actor to execute malicious code on the client-side, potentially bypassing some of the restrictions imposed by the blocked phishing attempt. To counter this potential pivot, the mandated defensive control of patching client applications, enabling exploit mitigations such as ASLR, DEP, and CFG, and implementing application isolation would likely be effective.

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