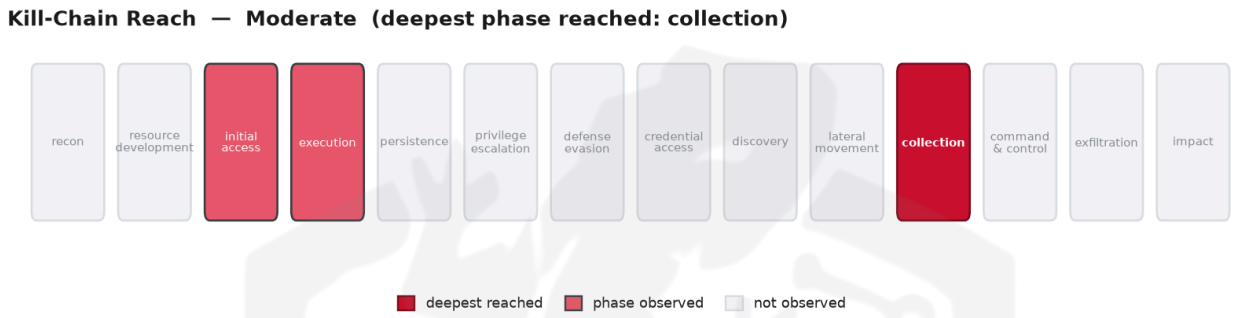
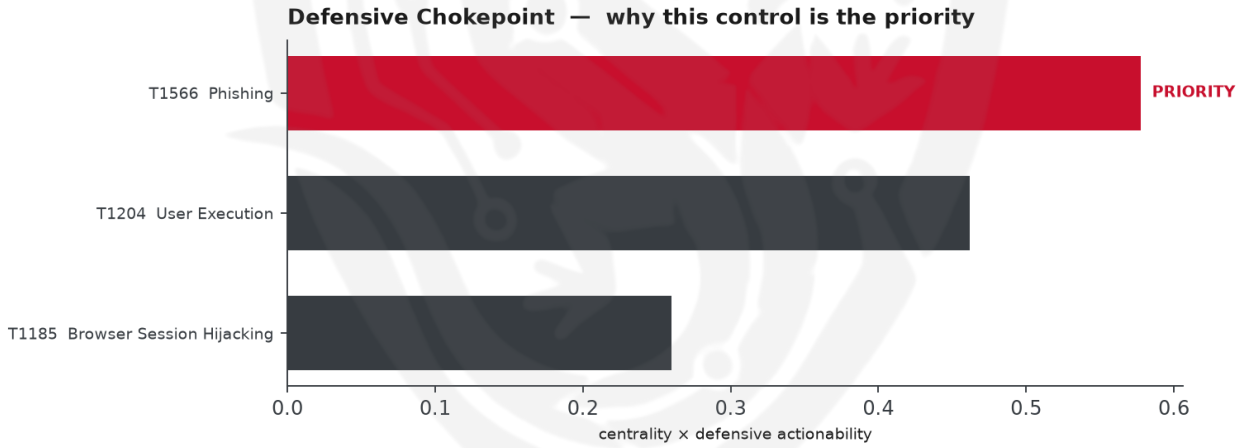
THREAT REPORT: O-UNC-038 OPERATION FAKE KICKOFF

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 O-UNC-038, a threat actor targeting various sectors including Human Resources, Aerospace, and Finance, among others. The actor's techniques, inferred from the report, involve social engineering tactics to harvest work credentials. Priority should be given to defending against social-engineering delivery methods. The threat actor's campaign poses a moderate operational risk, reaching the 'collection' stage.

Threat Overview

O-UNC-038, the observed threat actor, is involved in an operation aimed at harvesting work credentials, primarily targeting sectors such as Human Resources, Aerospace, Technology, and several others. The malware families and central CVE used in this operation are not specified due to insufficient data.

However, techniques inferred from the report include browser session hijacking, user execution, and phishing.

Attack Chain and Priority Control

The attack chain involves several techniques, including browser session hijacking, user execution, and phishing, with the latter being the priority technique, specifically T1566 Phishing. This technique serves as a critical point in the attack chain. To mitigate this threat, the priority action 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

There is no specific information available on the hosting providers or ASNs observed in this operation. Additionally, no malware families have been corroborated by abuse.ch, and 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. - 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%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator
Domain	fifahr-careers[.]com
Domain	adidas-hiring[.]com

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 adversary, O-UNC-038, could pivot to T1203 Exploitation for Client Execution in an attempt to execute malicious code on the client-side, potentially by exploiting vulnerabilities in commonly used software, which may allow them to bypass the blocked phishing attempt and still achieve their objective. This technique may be particularly appealing as it could enable the adversary to leverage existing vulnerabilities in client applications, such as Office or browsers, to gain execution and maintain access. To

counter this potential pivot, the mandated defensive control of patching client applications, enabling exploit mitigations like 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