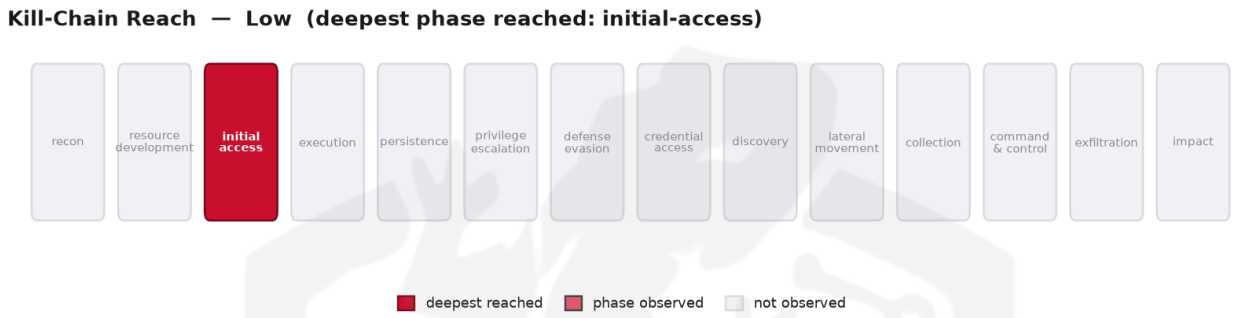
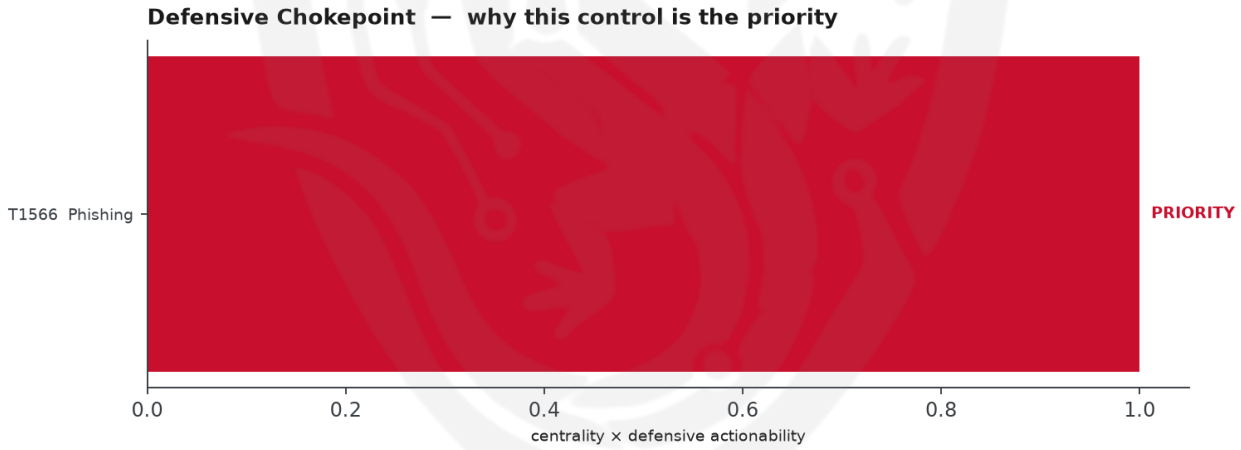
THREAT REPORT: O-UNC-066 TARGETS ENTRA PASSKEY ENROLLMENT

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-066, a threat actor targeting multiple sectors including Technology, Healthcare, and Aerospace, with a focus on Entra passkey enrollment. The techniques inferred from the report suggest a social engineering approach. Priority should be given to defending against phishing and social engineering tactics. The actor's methods pose a low operational risk but can still achieve initial access.

Threat Overview

O-UNC-066, the attributed threat actor, is involved in targeting various sectors with techniques inferred from the report as phishing. The specific malware families and central CVE used are not sufficiently detailed. The victimology spans across several industries, indicating a broad targeting strategy.

Attack Chain and Priority Control

The observed techniques, as inferred from the report, suggest a chain that likely starts with phishing, aiming for initial access. The priority technique identified is T1566 Phishing, which serves as a critical chokepoint in the attack chain. To mitigate this, the recommended priority 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

There is no specific information available on the hosting providers or ASNs used by the threat actor, as indicated by the lack of data in this area. Similarly, 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. - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 1.0).
- Operational risk: Low (score 0.117, reaches initial-access).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.7071; 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
AppleJeus	0.7071
APT30	0.5
TA459	0.3536
APT12	0.3333
Mofang	0.3333

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	deploypasskey[.]com
Domain	passkeyadd[.]com
Domain	passkeydeploy[.]com
Domain	setpasskey[.]com
Domain	assignpasskey[.]com
Domain	exampleentity[.]setpasskey[.]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:** T1204 User Execution (execution)
- **Basis:** of the 89+ 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-066, could pivot to T1204 User Execution to maintain their objective by tricking users into executing malicious files, potentially disguised as legitimate documents or applications, which may be downloaded from compromised websites or sent via email, thereby bypassing the phishing block. This technique is particularly appealing as it relies on user interaction, making it a plausible next step after a phishing attempt. The defensive countermeasure to mitigate this would be to Block execution of downloaded HTA/JS/LNK; enforce mark-of-the-web; disable Office macros from the internet; user awareness on lures.

Also plausible (same tactic): T1203 Exploitation for Client Execution (n=38, lift 1.6), T1053 Scheduled Task/Job (n=43, lift 1.3)

Detection and hardening for the pivot (T1204 User Execution)

- **Telemetry:** Endpoint process telemetry; Email/proxy logs
- **Detect:**
  - User double-clicking archive/ISO/LNK contents that spawn interpreters
  - Mark-of-the-Web on delivered files; LOLBIN execution from user temp paths
- **Harden:**
  - Block risky file types; ASR rules; user awareness training
  - Application control to stop execution from user-writable directories
- **MITRE:** M1049 Antivirus/Antimalware, M1038 Execution Prevention, M1017 User Training · DS0009 Process, DS0022 File