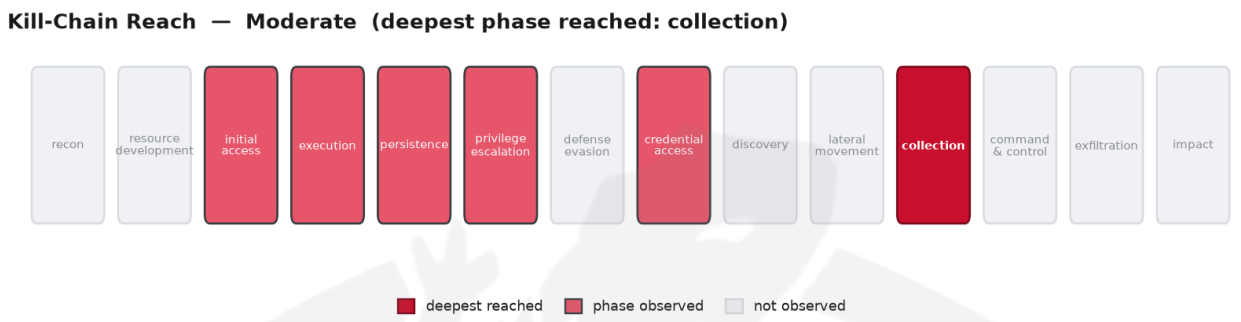
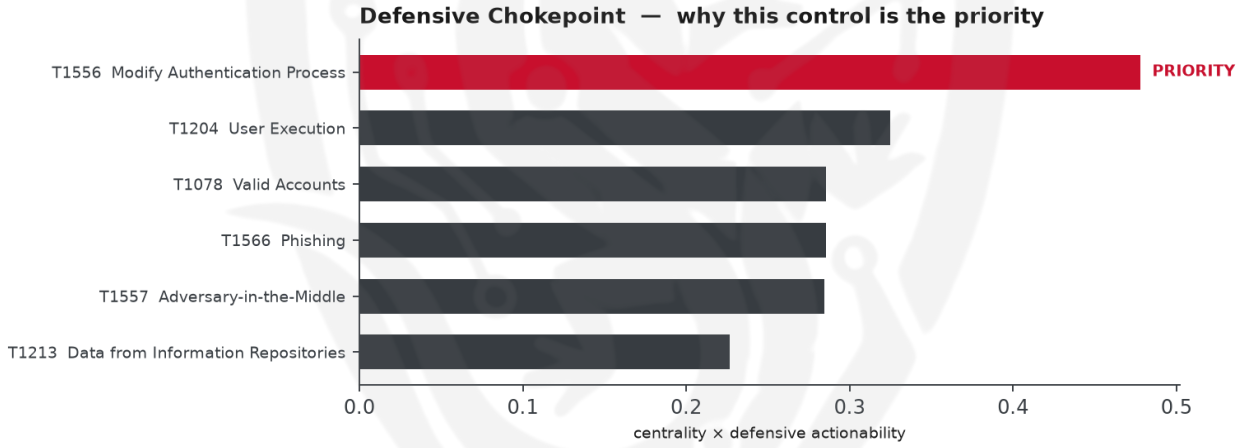
THREAT REPORT: HELIX

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

Helix has been identified as the threat actor behind a recent data-extortion campaign. The activity involves exploitation of an unspecified vulnerability and the use of an unidentified malware family. The observed tactics focus on compromising authentication processes. Priority defensive action is to protect the authentication pipeline by monitoring changes to MFA methods, federation trusts, and conditional-access policies, and by enforcing step-up approval for authentication-method registration.

Threat Overview

The source attributes the activity to Helix. The malware family and central CVE are not disclosed. The campaign targets unspecified sectors and countries, with the primary objective of extracting data from information repositories.

Attack Chain and Priority Control

The observed techniques include Valid Accounts (T1078), User Execution (T1204), Data from Information Repositories (T1213), Modify Authentication Process (T1556), Adversary-in-the-Middle (T1557), and Phishing (T1566). The priority technique is T1556 Modify Authentication Process.
Priority action: Protect the authentication pipeline: alert on changes to MFA methods, federation trusts and conditional-access policies; require step-up approval for auth-method registration; monitor for AiTM/token replay and revoke sessions on anomaly.

Infrastructure and Corroboration

The malicious infrastructure is hosted by Private Layer Inc. No additional high-confidence reputation flags or corroborated malware families were identified.

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. - T1078 Valid Accounts - T1204 User Execution - T1213 Data from Information Repositories - T1556 Modify Authentication Process - T1557 Adversary-in-the-Middle - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1556 Modify Authentication Process (centrality 0.5033).
- Operational risk: Moderate (score 0.479, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4082; 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	0.4082
TA459	0.2887

Historical Profile	Behavioural Overlap
AppleJeus	0.2887
FIN4	0.2739
APT12	0.2722

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	Context
IP	179[.]43[.]185[.]226	AbuseIPDB 0% (CH) · AS51852 Private Layer Inc
IP	179[.]43[.]185[.]230	AbuseIPDB 0% (CH) · AS51852 Private Layer Inc
IP	179[.]43[.]171[.]42	AbuseIPDB 0% (CH) · AS51852 Private Layer Inc
Domain	oskeysync[.]com	

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:** T1556 Modify Authentication Process (persistence)
- **Observed here:** T1556 Modify Authentication Process was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1098 Account Manipulation (persistence)
- **Basis:** of the 4+ groups that use Modify Authentication Process, this pairing runs 4.7x above base rate, a disproportionately-coupled move rather than the obvious one.

Having blocked the adversary's attempt to alter the authentication process, the Helix actor could pivot to T1098 Account Manipulation by creating or modifying privileged user accounts, adding them to administrative groups, or injecting new credentials into existing accounts to maintain persistence and elevate privileges without changing the authentication flow. To counter this, the SOC should monitor for privilege and group changes and credential additions to accounts (Event ID 4738/4670) and review any conditional-access policy modifications.

Also plausible (same tactic): T1133 External Remote Services (n=5, lift 3.8), T1136 Create Account (n=3, lift 2.9)

Detection and hardening for the pivot (T1098 Account Manipulation)

- **Telemetry:** Windows Security (account management); Azure AD audit logs
- **Detect:**
  - Security 4728/4732/4756 (added to security-enabled groups), 4738 (account changed), 4670 (permissions changed)
  - New credentials/keys added to accounts or app registrations in the IdP
  - MFA method added or reset outside a normal workflow
- **Harden:**
  - Alert on privileged-group changes; approval workflow for role grants
  - Monitor and restrict service-principal credential additions
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1018 User Account Management · DS0002 User Account, DS0026 Active Directory