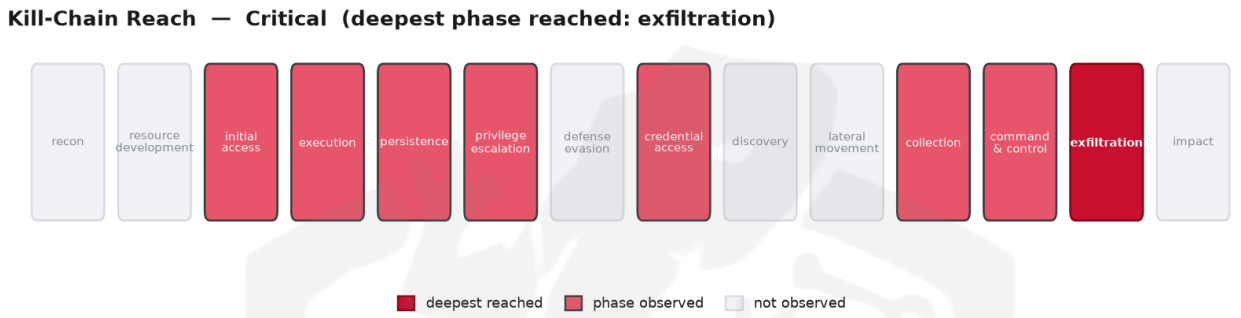
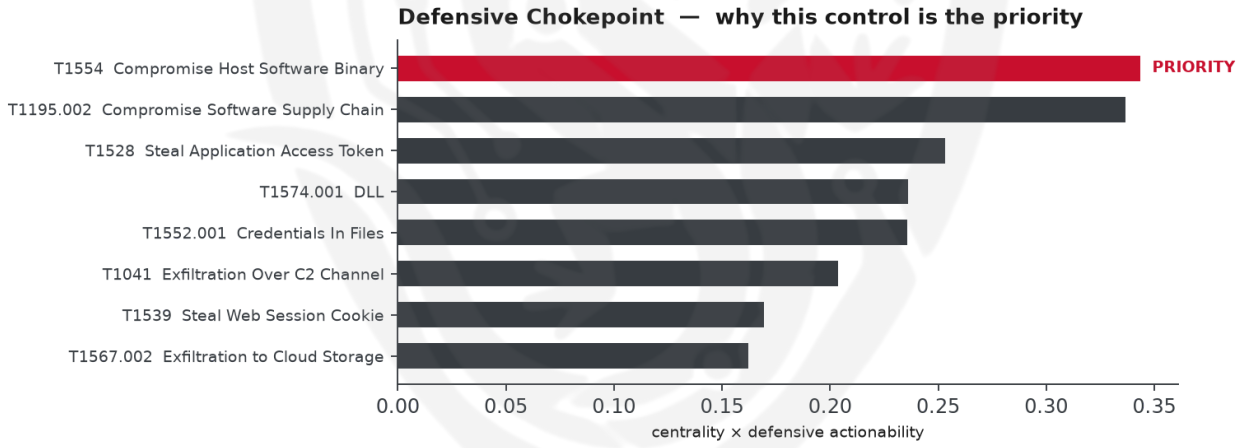
THREAT REPORT: UNKNOWN_ADVERSARY COMPROMISED INJECTIVE SDK NPM PACKAGE

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 has compromised an Injective SDK npm package, resulting in the exfiltration of wallet keys and mnemonics, primarily targeting the technology sector. The threat actor's identity and motivations are currently unknown. Priority should be given to defending against the compromise of host software binaries. The operational risk band for this threat is critical, as it reaches the level of exfiltration.

Threat Overview

The observed cluster of activity has been identified as compromising an Injective SDK npm package, although the specific malware families and central CVE used are currently unknown. The techniques

employed include standard encoding, JavaScript, stealing web session cookies, and exfiltration over C2 channels, among others. The victimology of this threat is focused on the technology sector.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including compromising host software binaries, stealing application access tokens, and exfiltrating data to cloud storage. The priority technique is T1554 Compromise Host Software Binary, which serves as a chokepoint in the attack chain. To mitigate this, the recommended control is to Apply the specific MITRE ATT&CK mitigation for this technique; add host/network detections and least-privilege controls around it.

Infrastructure and Corroboration

There is currently no information available on the hosting providers or ASNs observed in relation to this threat. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence level of 80% or higher.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1132.001 Standard Encoding
- T1059.007 JavaScript
- T1539 Steal Web Session Cookie
- T1574.001 DLL
- T1552.001 Credentials In Files
- T1528 Steal Application Access Token
- T1041 Exfiltration Over C2 Channel
- T1554 Compromise Host Software Binary
- T1195.002 Compromise Software Supply Chain
- T1567.002 Exfiltration to Cloud Storage
- T1213 Data from Information Repositories
- T1071.001 Web Protocols
- T1078.003 Local Accounts

Analytical Scores

- Priority technique (graph chokepoint): T1554 Compromise Host Software Binary (centrality 0.3618).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.2926; 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
MuddyWater	0.2926
Daggerfly	0.2789
Velvet Ant	0.2744
APT19	0.27
LuminousMoth	0.2694

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	testnet[.]archival[.]chain[.]grpc-web[.]injective[.]network
URL	hxxps://testnet[.]archival[.]chain[.]grpc-web[.]injective[.]network
Hash	103c4e6181151c1bcfedc41506cd1815458c38375d08a8fcd9981dbe0b965ce0
Hash	9a59eb454f3ca3fe91214136ee5edd417cc47a80e6f169b52099d6561944baf9

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:** T1554 Compromise Host Software Binary (persistence)
- **Observed here:** the threat actor used T1078.003 Local Accounts here as an alternative persistence technique.

- **Projected pivot:** T1078.003 Local Accounts (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to utilizing local accounts, as seen in T1078.003, to maintain access and achieve their objectives, potentially by exploiting weak passwords or leveraging existing account credentials. This technique may allow the actor to bypass some security controls and continue their campaign. The defensive countermeasure would be to enforce the mandated control, which includes Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Detection and hardening for the pivot (T1078.003 Valid Accounts)

- **Telemetry:** Windows Security (logon events); Azure AD / IdP sign-in logs; VPN and remote-access logs; Proxy / DLP / data-egress volume telemetry
- **Detect:**
  - Security 4624/4625 (logon success/fail), 4768/4769 (Kerberos TGT/TGS), 4776 (NTLM)
  - Impossible-travel, new-geo, and off-hours sign-ins from the IdP
  - Service or dormant accounts logging on interactively
  - Under valid credentials the identity signal goes quiet: baseline per-account data-egress volume and alert on peer-group and historical deviation (the real exfiltration tell)
- **Harden:**
  - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
  - Least-privilege review; separate admin from daily-driver accounts
  - Set per-account and per-partner egress baselines with DLP thresholds on sensitive stores
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account