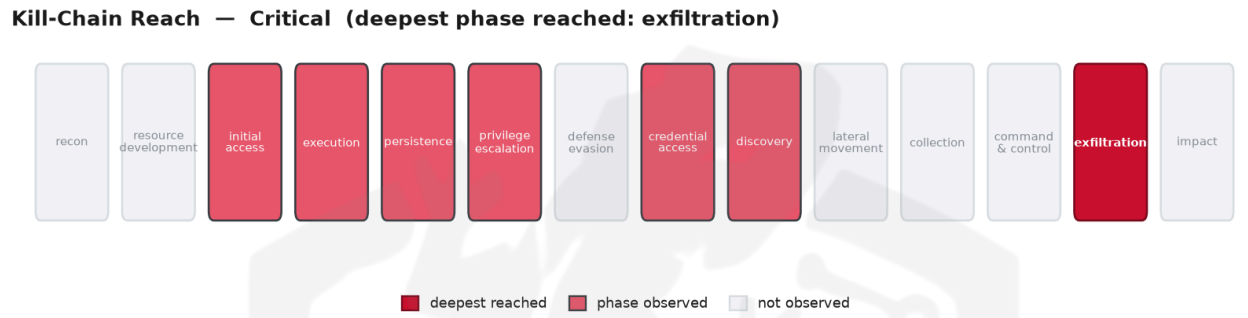
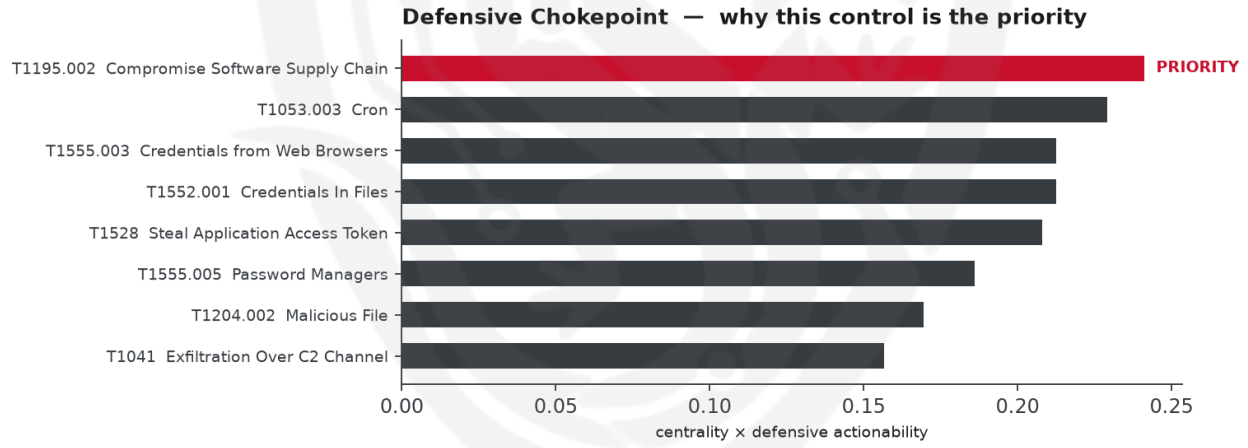
THREAT REPORT: UNKNOWN_ADVERSARY COMPROMISES JSCRAMBLER NPM PACKAGE

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 the jscrambler npm package in a supply chain attack, targeting the technology sector. The threat actor's identity and motivations are unknown, but the attack's impact is significant. Priority should be given to verifying software supply chain integrity to prevent further compromise. The attack's ability to reach exfiltration stages poses a critical operational risk.

Threat Overview

The threat actor, whose identity is unknown, has compromised the jscrambler npm package, exploiting unknown vulnerabilities. The attack targets the technology sector, with the goal of stealing sensitive information and gaining unauthorized access. The observed techniques include system owner/user discovery, JavaScript execution, and web session cookie theft, among others.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including system information discovery, deobfuscation of files, and credentials theft. The priority technique is T1195.002 Compromise Software Supply Chain, which is the graph chokepoint. To mitigate this threat, the priority control is to Verify software supply chain integrity (signing, SBOM); pin and monitor third-party dependencies and update channels.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this attack, and no malware families have been corroborated by abuse.ch. Additionally, 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, expert-tagged by source)

- T1033 System Owner/User Discovery
- T1059.007 JavaScript
- T1539 Steal Web Session Cookie
- T1548.003 Sudo and Sudo Caching
- T1204.002 Malicious File
- T1053.003 Cron
- T1555.005 Password Managers
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1555.003 Credentials from Web Browsers
- T1552.001 Credentials In Files
- T1528 Steal Application Access Token
- T1041 Exfiltration Over C2 Channel
- T1027 Obfuscated Files or Information
- T1195.002 Compromise Software Supply Chain
- T1567.002 Exfiltration to Cloud Storage
- T1027.002 Software Packing
- T1543.002 Systemd Service
- T1078.004 Cloud Accounts
- T1552.007 Container API

Analytical Scores

- Priority technique (graph chokepoint): T1195.002 Compromise Software Supply Chain (centrality 0.2413).

- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3526; 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
Threat Group-3390	0.3526
ZIRCONIUM	0.3499
Malteiro	0.3468
Molerats	0.3402
MuddyWater	0.3314

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
Hash	a41a523ef9517aab37ed6eea0ec881821bdcb7aefcb5c5f603adc7907f868c86
Hash	a742de963f14a92d24ebcbc7b44ac867e23a20d31d1b0094a13a4f83287f4e60
Hash	b7ca95d1b23c8e67416a25cedf741de0917c2096bbc9d24649eea7853d054903
Hash	bba32ddeab075a5e5015eec50f5d2af364c95b848732c714aea6b6baf78f49f0
Hash	c8fd47d36bdf7c825378593ab82ed8c24d1dc52e26b507812393e24e1d5201fd
Hash	fbbcf4d8f98168f78f5c0c47a9ae56d59ec8ac84a7c9ca6b797fedfb8d62d2bd

---

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:** T1195.002 Compromise Software Supply Chain (initial-access)
- **Observed here:** the threat actor used T1078.004 Cloud Accounts here as an alternative initial-access technique.
- **Projected pivot:** T1078.004 Cloud Accounts (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to T1078.004 Cloud Accounts by attempting to leverage compromised credentials or exploit weak authentication mechanisms to gain unauthorized access to cloud-based resources, which may allow them to maintain their objective despite the blocked software supply chain compromise. This technique could be used to establish a new foothold or persist in the environment, potentially leading to further malicious activity. To counter this, the organization would likely enforce the mandated defensive control: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Detection and hardening for the pivot (T1078.004 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