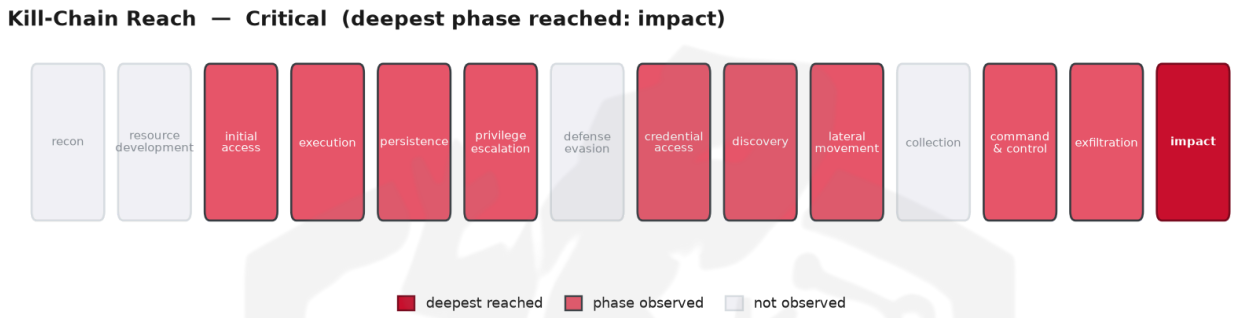
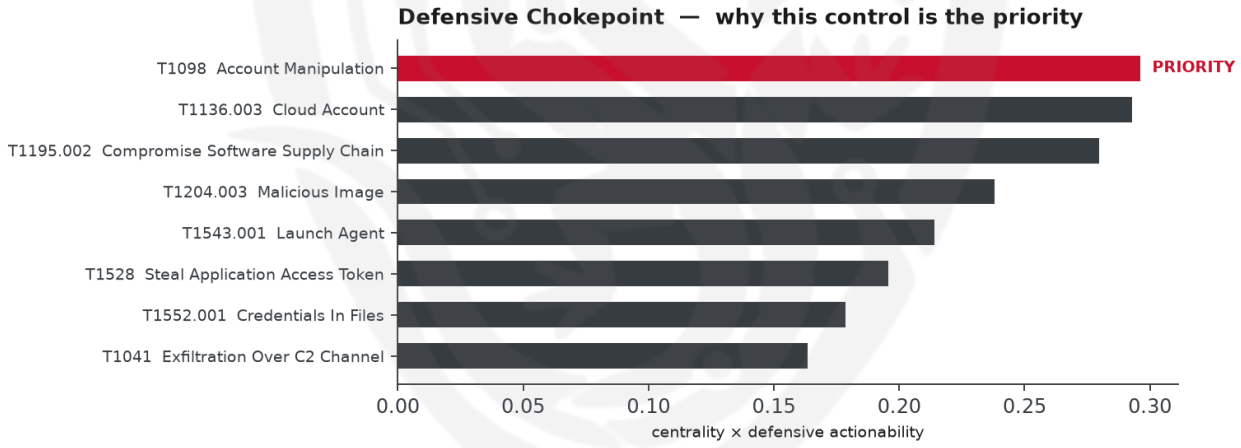
THREAT REPORT: SHAI-HULUD-STYLE NPM WORM HITS TECHNOLOGY SECTOR

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 been targeting the technology sector, leveraging various techniques to compromise systems. The priority defensive action should be to alert on privilege and group changes, as well as credential additions to accounts. This is crucial in preventing further exploitation and minimizing the impact of the attack. Given the operational risk band is Critical, immediate attention is required to mitigate potential damage.

Threat Overview

The threat actor, whose identity is currently insufficient to determine, is utilizing a range of techniques including system owner/user discovery, standard encoding, and JavaScript to carry out their objectives. The targeted sector is technology, indicating a focused approach on compromising systems within this

industry. The absence of specific malware families and central CVEs highlights the need for a broad defensive strategy.

Attack Chain and Priority Control

The attack chain involves multiple techniques, starting from system information discovery and moving through to exfiltration over C2 channels, with a significant emphasis on account manipulation. The priority technique identified is T1098 Account Manipulation, which serves as a critical chokepoint in the attack chain. To counter this, the priority control is to "Alert on privilege/group changes and credential additions to accounts (Event ID 4738/4670); review conditional-access changes."

Infrastructure and Corroboration

While specific hosting providers or ASNs are not observed, corroboration from abuse.ch indicates the involvement of the Shai-Hulud malware family. However, AbuseIPDB does not flag any indicators with a confidence level of 80% or higher, suggesting that the malicious infrastructure may not be widely recognized or reported at this time.

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
- T1132.001 Standard Encoding
- T1059.007 JavaScript
- T1552.005 Cloud Instance Metadata API
- T1082 System Information Discovery
- T1552.001 Credentials In Files
- T1528 Steal Application Access Token
- T1041 Exfiltration Over C2 Channel
- T1136.003 Cloud Account
- T1098 Account Manipulation
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1204.003 Malicious Image
- T1195.002 Compromise Software Supply Chain
- T1496 Resource Hijacking
- T1543.001 Launch Agent
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1550.001 Application Access Token
- T1078.004 Cloud Accounts

Analytical Scores

- Priority technique (graph chokepoint): T1098 Account Manipulation (centrality 0.3119).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3105; 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
Daggerfly	0.3105
TeamTNT	0.3055
APT33	0.3032
HAFNIUM	0.3024
APT19	0.3007

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Shai-Hulud.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
Domain	git-tanstack[.]com	Shai-Hulud
Hash	2ec78d556d696e208927cc503d48e4b5eb56b31abc2870c2ed2e98d6be27fc96	Shai-Hulud
Hash	b82e54923f7e440664d2d75bd31588ca	
Hash	e7d582b98ca80690883175470e96f703ef6dc497	

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:** T1098 Account Manipulation (persistence)
- **Observed here:** T1098 Account Manipulation was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1505 Server Software Component (persistence)
- **Basis:** of the 8+ groups that use Account Manipulation, this pairing runs 2.4x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1505 Server Software Component to maintain their objective by exploiting vulnerabilities in server software components, such as web servers or database management systems, which may allow them to execute malicious code or gain elevated privileges. This technique may be particularly appealing as a follow-up to T1098 Account Manipulation, as it could enable the actor to leverage compromised accounts to install or manipulate server software components. To counter this potential move, the mandated defensive control of integrity-monitoring web-server directories for web shells and restricting server module/plugin installation should be implemented.

Also plausible (same tactic): T1542 Pre-OS Boot (n=3, lift 7.1), T1133 External Remote Services (n=10, lift 3.4)

Detection and hardening for the pivot (T1505 Server Software Component)

- **Telemetry:** Web server logs; File integrity monitoring on web roots; EDR
- **Detect:**
  - New/modified files in web-accessible directories (aspx/php/jsp)
  - w3wp.exe / httpd spawning cmd.exe, powershell.exe or whoami
  - Anomalous POSTs to newly created endpoints in web access logs
- **Harden:**
  - File integrity monitoring on web roots; least-privilege service accounts
  - Remove dev tooling from production web servers; WAF in front
- **MITRE:** M1047 Audit, M1018 User Account Management, M1042 Disable or Remove Feature · DS0022 File, DS0009 Process, DS0015 Application Log