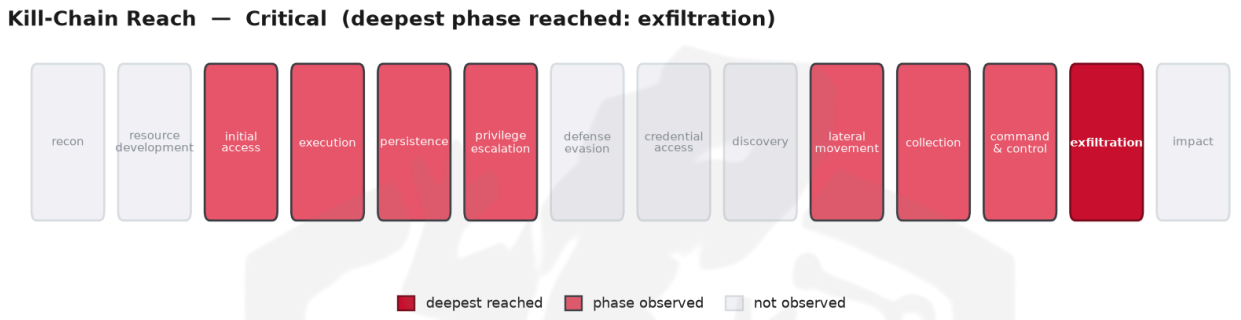
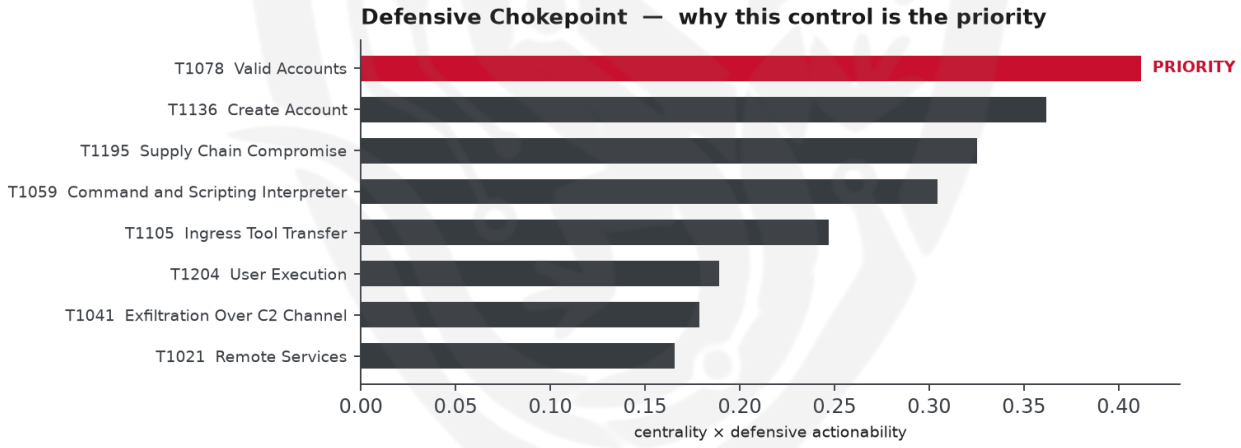
THREAT REPORT: CHAINDROP NPM ATTACK COMPROMISES TECHNOLOGY SECTOR

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 compromised hundreds of packages using the ChainDrop and Shai-Hulud malware families, targeting the technology sector. The reporting indicates techniques inferred from the report include data exfiltration and supply chain compromise. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The operational risk band is critical due to the potential for exfiltration.

Threat Overview

The threat actor, whose identity is not specified, is utilizing the ChainDrop and Shai-Hulud malware families to compromise packages in the technology sector. The reporting indicates techniques inferred from the report include data exfiltration over various channels and supply chain compromise. The

victimology suggests a focus on the technology sector, although specific country information is not available.

Attack Chain and Priority Control

The observed techniques, inferred from the report, suggest a chain of events including data exfiltration, command and scripting interpreter usage, and potential supply chain compromise. The priority technique is T1078 Valid Accounts, which is the graph chokepoint. To mitigate this threat, the priority control is: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

There is no available information on hosting providers or ASNs observed in this campaign. Additionally, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB.

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. - T1005 Data from Local System - T1021 Remote Services - T1041 Exfiltration Over C2 Channel - T1059 Command and Scripting Interpreter - T1078 Valid Accounts - T1105 Ingress Tool Transfer - T1136 Create Account - T1195 Supply Chain Compromise - T1204 User Execution - T1567 Exfiltration Over Web Service

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.4118).
- Operational risk: Critical (score 0.926, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3586; 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-1314	0.3586
Indrik Spider	0.3229
Cinnamon Tempest	0.3101
APT3	0.3046
Confucius	0.2988

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Unknown malware.
- 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	npm-cache[.]com	Unknown malware
Domain	pypi-get[.]com	Unknown malware
Domain	js-mirror[.]com	Unknown malware
Domain	go[.]getblock[.]io	
Hash	00ca0c04d247ef09f2b2acc452029345	
Hash	dbb9b09957113463bbeb420c2c4108b5	
Hash	7b0278216ac31ec18eca9eb8bc1c1261a1b26f6c	
Hash	ff7ed7a0fa1c43eed01809d076feedbaed464fc7	
Hash	14eb4ce01dd4307759887ff819359b70d7d9ff709ecde039a5abc1aac325b128	
Hash	927387d0cfac1118df4b383decc2ea6ba49c9d2f98b47098bcbcba1efc026e1f	
Hash	35a672cf34b996b91f3e1c28cbf3a05a37e036e4	
Hash	f525d52ceb966516686b482d3dc0137028cc6a63	

Type	Indicator	Context
Hash	9fc2570b7cef51c1b8df116d144d11ff4096357be7d2c4c6367cfc2509cf1bcc	
Hash	fd3ca4007b225fdf8de7af4345a19179d5efa8c4bb9205f88cda806e5684b1eb	
Hash	4140f7e17e6f97f83aa3472473e01add	
Hash	7bcf8d9f6834c44450eac145a967d2f2	
Hash	3f3f42d072bd36860ab7bd7fb5e10ac0d22c741c13c89505ccd6ec0ea572eea7	

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:** T1078 Valid Accounts (initial-access)
- **Observed here:** T1078 Valid Accounts 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:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 29+ groups that use Valid Accounts, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain access and evade detection, as this technique allows them to leverage the existing Windows infrastructure for remote management and execution, potentially exploiting the trust inherent in administrative protocols. This technique may be particularly appealing as it enables the actor to execute commands and gather information without relying on compromised credentials, which were previously obtained through T1078 Valid Accounts. To counter this potential pivot, the mandated defensive control of monitoring wmiprvse.exe child-process creation, restricting remote WMI (DCOM) at the host firewall, and enabling WMI-Activity operational logging should be implemented.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1053 Scheduled Task/Job (n=31, lift 1.4)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts

- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command