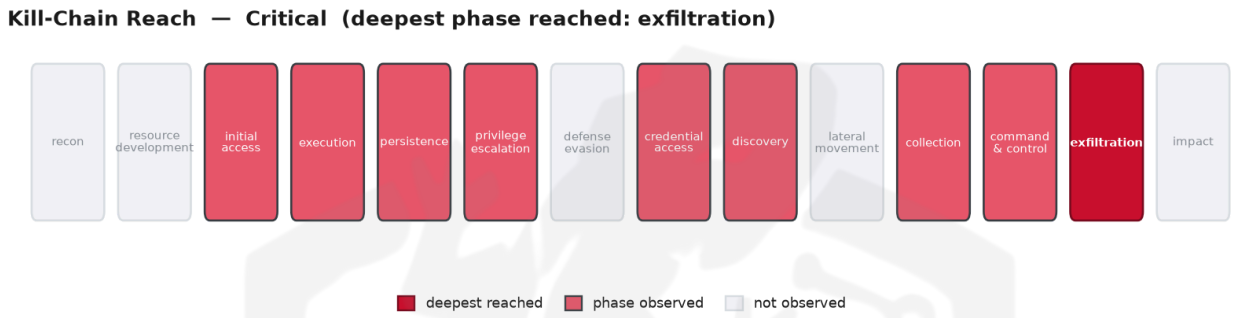
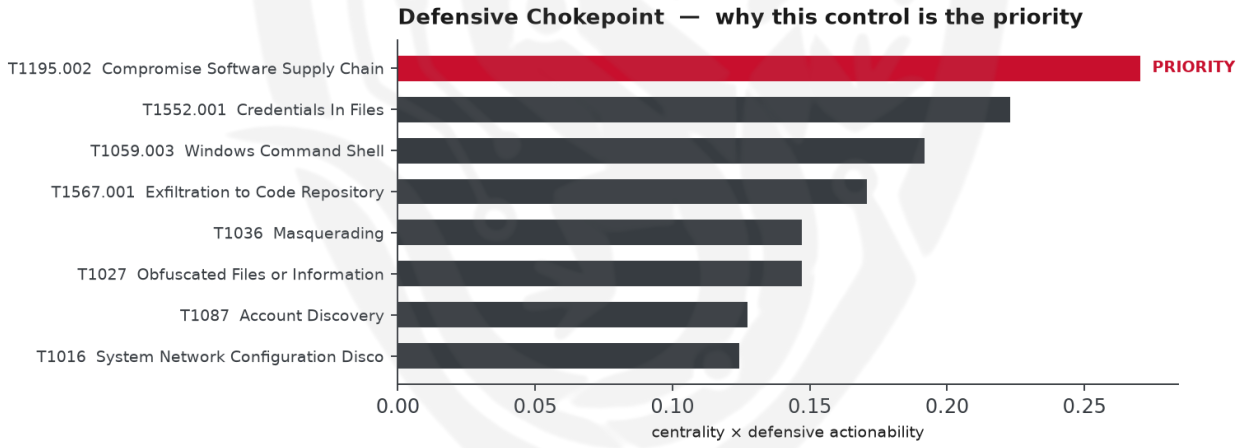
THREAT REPORT: SHAI-HULUD'S CHAINDROP NPM PACKAGE COMPROMISE

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 source attributes this activity to Shai-Hulud, who has been observed compromising over 400 npm packages with the CHAINDROP worm. The targeted sector is Technology, with the threat actor leveraging various techniques to achieve their goals. Priority should be given to verifying software supply chain integrity to mitigate the risks associated with this campaign. The lack of specific CVE information and targeted country data limits the scope of defensive actions, but addressing the software supply chain is crucial.

Threat Overview

Shai-Hulud is the threat actor behind the CHAINDROP malware family, which has been used to compromise numerous npm packages. Although the central CVE is insufficient, the malware has been

observed utilizing various techniques, including JavaScript, malicious file execution, and symmetric cryptography, to name a few. The victimology points to the Technology sector, indicating a focused effort by the threat actor.

Attack Chain and Priority Control

The observed techniques form a complex chain, starting from initial access and moving through various stages, including system information discovery, automated collection, and eventually, exfiltration to code repositories. The priority technique identified is T1195.002, Compromise Software Supply Chain, which serves as a critical chokepoint in the attack chain. To counter this, 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 specific information available on the hosting providers or ASNs observed in this campaign. Additionally, abuse.ch has not corroborated any known malware families, and AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. This lack of corroboration highlights the need to rely on the primary techniques and controls to mitigate the threat.

Technical Appendix

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

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

- T1059.007 JavaScript
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1119 Automated Collection
- T1553.001 Gatekeeper Bypass
- T1082 System Information Discovery
- T1036 Masquerading
- T1016 System Network Configuration Discovery
- T1087 Account Discovery
- T1552.001 Credentials In Files
- T1567.001 Exfiltration to Code Repository
- T1027 Obfuscated Files or Information
- T1195.002 Compromise Software Supply Chain
- T1059.003 Windows Command Shell
- T1070.004 File Deletion
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1078.004 Cloud Accounts

Analytical Scores

- Priority technique (graph chokepoint): T1195.002 Compromise Software Supply Chain (centrality 0.2705).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4623; 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
APT18	0.4623
RedCurl	0.4304
Tropic Trooper	0.4193
OilRig	0.4058
Metador	0.4051

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	awqhnjewqjkl[.]icu	Unknown malware
Hash	35a672cf34b996b91f3e1c28cbf3a05a37e036e4	
Hash	f525d52ceb966516686b482d3dc0137028cc6a63	

Type	Indicator	Context
Hash	54dc7ea54a1317cca0e890a2770630cf7fa6c97813e0cb9d2caa93012b350668	
Hash	9fc2570b7cef51c1b8df116d144d11ff4096357be7d2c4c6367cfc2509cf1bcc	
Hash	fd3ca4007b225fdf8de7af4345a19179d5efa8c4bb9205f88cda806e5684b1eb	
Hash	4140f7e17e6f97f83aa3472473e01add	
Hash	7bcf8d9f6834c44450eac145a967d2f2	
Hash	f92ee93a0af971a3966bfa8efa9c2625	
Hash	e65b155ce74f3f81fb7d2b5b60f8e62b36e6d69c	

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:** T1195.002 Compromise Software Supply Chain (initial-access)
- **Observed here:** T1195.002 Compromise Software Supply Chain 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:** T1053 Scheduled Task/Job (execution)
- **Basis:** of the 10+ groups that use Compromise Software Supply Chain, this pairing runs 2.7x above base rate, a disproportionately-coupled move rather than the obvious one.

Shai-Hulud could pivot to T1053 Scheduled Task/Job to maintain persistence and execute malicious code at a later time, potentially leveraging the technique's ability to blend in with legitimate system activity, which may allow them to bypass defenses that are focused on immediate, in-your-face attacks. This technique in particular may be appealing to Shai-Hulud because it enables them to schedule tasks that can run under the context of a legitimate system process, which would likely increase the chances of evasion. To counter this potential move, the defensive control would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1203 Exploitation for Client Execution (n=7, lift 2.6), T1047 Windows Management Instrumentation (n=6, lift 2.2)

Detection and hardening for the pivot (T1053 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**

    - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
    - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
    - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
    - Restrict schtasks/at to administrators; disable the legacy at.exe
    - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File