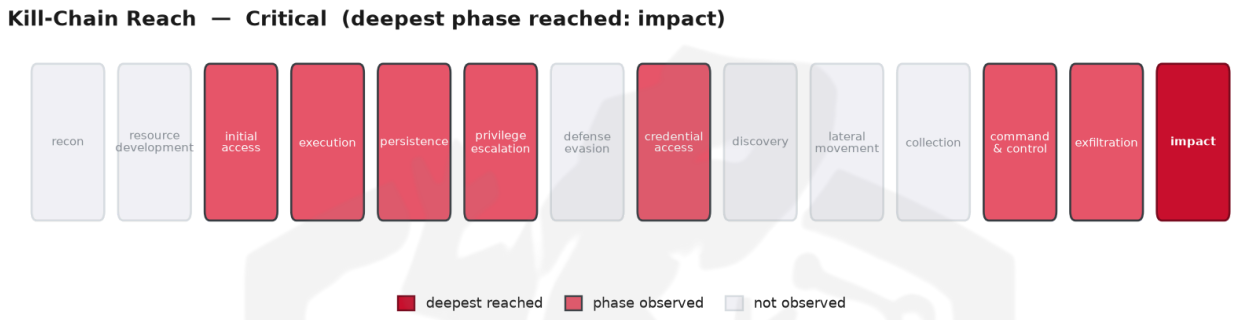
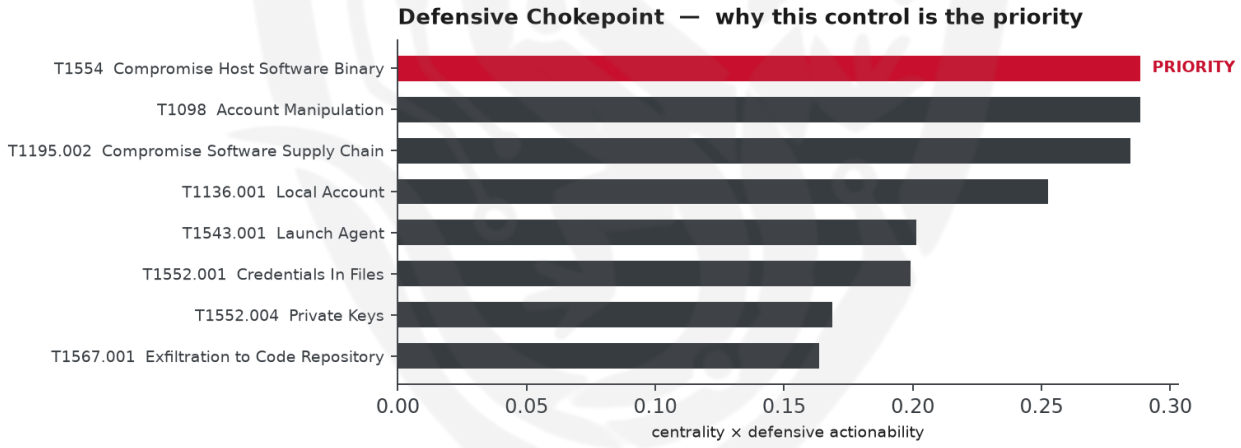
THREAT REPORT: TEAMPCP'S CHAINDROP NPM WORM

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 TeamPCP, who has been observed utilizing a range of malware families, including ChainDrop and Shai-Hulud, to target the technology sector. The threat actor's techniques include compromising software dependencies and development tools, as well as exfiltrating data to code repositories and cloud storage. Priority should be given to defending against the compromise of host software binaries. The actor's operational risk band is considered Critical, indicating a high potential impact.

Threat Overview

TeamPCP, the attributed threat actor, has been associated with multiple malware families, including ChainDrop, Shai-Hulud, Mini Shai-Hulud, Megalodian, Miasma, Phantom Gyp, and Hades. The central

vulnerability exploited is currently unknown. The threat actor targets the technology sector, with the targeted country and specific CVEs remaining insufficiently documented.

Attack Chain and Priority Control

The observed techniques employed by TeamPCP form a complex chain, involving standard encoding, JavaScript, compromise of software dependencies and development tools, and symmetric cryptography, among others. The priority technique is T1554 Compromise Host Software Binary, which serves as a critical 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 no observed hosting provider or ASN associated with this activity. Abuse.ch has not corroborated any specific malware families in this context, labeling them as unknown. 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)

- T1132.001 Standard Encoding
- T1059.007 JavaScript
- T1195.001 Compromise Software Dependencies and Development Tools
- T1552.005 Cloud Instance Metadata API
- T1573.001 Symmetric Cryptography
- T1552.004 Private Keys
- T1136.001 Local Account
- T1552.001 Credentials In Files
- T1567.001 Exfiltration to Code Repository
- T1554 Compromise Host Software Binary
- T1098 Account Manipulation
- T1027 Obfuscated Files or Information
- T1195.002 Compromise Software Supply Chain
- T1567.002 Exfiltration to Cloud Storage
- T1496 Resource Hijacking
- T1543.001 Launch Agent
- T1485 Data Destruction
- T1071.001 Web Protocols
- T1078.004 Cloud Accounts

- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1554 Compromise Host Software Binary (centrality 0.3037).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.325; 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
APT33	0.325
TeamTNT	0.3002
MuddyWater	0.2681
Rocke	0.2626
Kimsuky	0.2556

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
Domain	copilot-instructions[.]md	
URL	hxxps://npm-cache[.]com:443/router	

Type	Indicator	Context
Hash	35a672cf34b996b91f3e1c28cbf3a05a37e036e4	
Hash	f525d52ceb966516686b482d3dc0137028cc6a63	
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:** T1554 Compromise Host Software Binary (persistence)
- **Observed here:** TeamPCP used T1078.004 Cloud Accounts here as an alternative persistence technique.
- **Projected pivot:** T1078.004 Cloud Accounts (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

TeamPCP could pivot to T1078.004 Cloud Accounts by attempting to leverage compromised credentials or exploiting weak authentication mechanisms to gain access to cloud-based infrastructure, which may allow them to maintain persistence and continue their campaign objectives. This technique in particular may be appealing as it enables TeamPCP to operate from a cloud-based foothold, potentially making it more challenging for defenders to detect and respond. To counter this potential move, the mandated defensive control of Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons should be implemented.

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