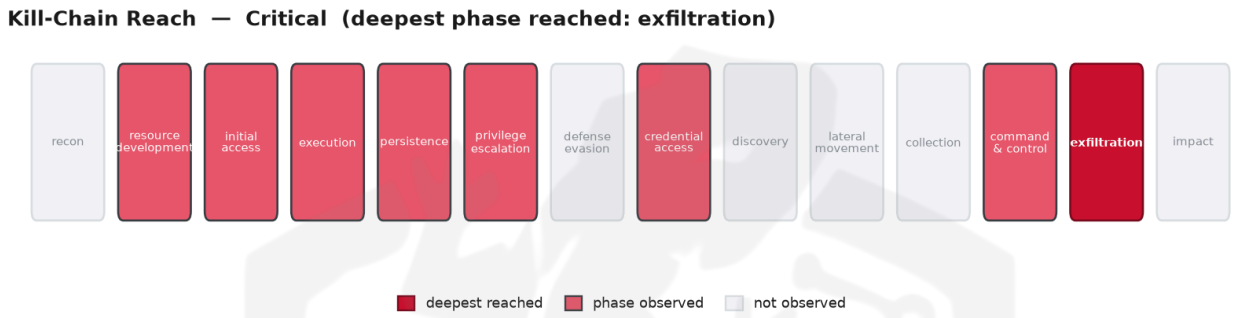
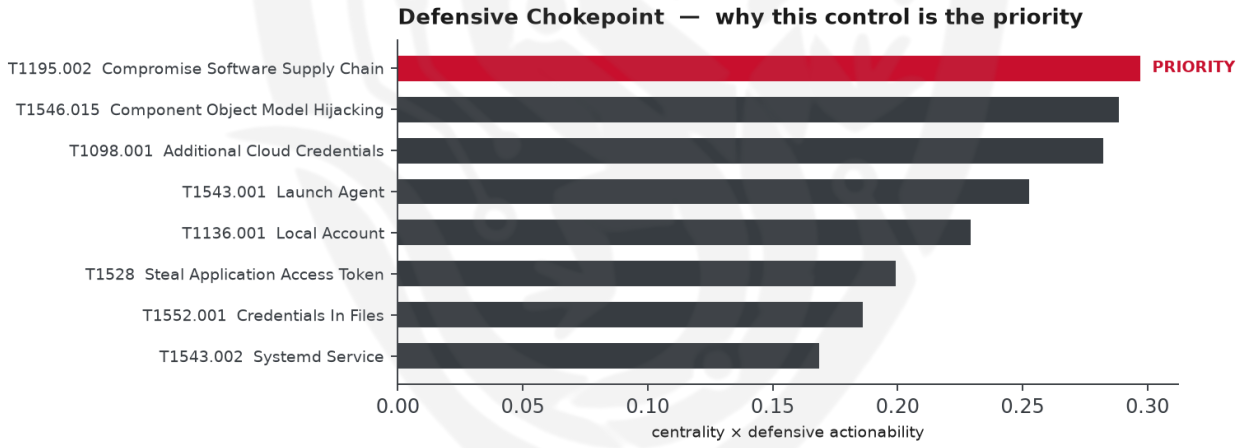
THREAT REPORT: CHAINDROP NPM WORM CAMPAIGN

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 involves the ChainDrop malware family, targeting the technology sector. The priority defensive action should be given to verifying software supply chain integrity, as the campaign poses a critical operational risk due to its potential for exfiltration. The threat actor remains unattributed, and the targeted country and central CVE are unknown.

Threat Overview

The threat actor, responsible for the ChainDrop malware family, has exploited various techniques to compromise systems, although the central CVE used is unknown. The victimology indicates that the technology sector is being targeted, with potential risks of exfiltration and compromise of software supply chain integrity.

Attack Chain and Priority Control

The observed techniques form a complex chain, including JavaScript, DNS, and Cron, among others. The priority technique is T1195.002 Compromise Software Supply Chain, which serves as a critical chokepoint in the attack chain. 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 campaign, and no corroborated malware families have been identified 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)

- T1059.007 JavaScript
- T1071.004 DNS
- T1053.003 Cron
- T1140 Deobfuscate/Decode Files or Information
- T1583.001 Domains
- T1136.001 Local Account
- T1552.001 Credentials In Files
- T1528 Steal Application Access Token
- T1098.001 Additional Cloud Credentials
- T1027 Obfuscated Files or Information
- T1546.015 Component Object Model Hijacking
- T1195.002 Compromise Software Supply Chain
- T1567.002 Exfiltration to Cloud Storage
- T1543.001 Launch Agent
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1543.002 Systemd Service
- T1105 Ingress Tool Transfer
- T1078.004 Cloud Accounts
- T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1195.002 Compromise Software Supply Chain (centrality 0.3082).

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

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3417; 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
TeamTNT	0.3417
APT33	0.3301
APT18	0.3282
TA505	0.3169
FIN7	0.3069

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	awqhnjewqjkl[.]icu	Unknown malware
URL	hxxps://npm-cache[.]com:443/router	
URL	hxxp://awqhnjewqjkl[.]icu/cdn-cgi/rum	

Type	Indicator	Context
Hash	d30b4ea6f68456672f5abb35e9dcf7d54226372b66e9d60a7ee26b7a52568e74	
Hash	35a672cf34b996b91f3e1c28cbf3a05a37e036e4	
Hash	f525d52ceb966516686b482d3dc0137028cc6a63	
Hash	54dc7ea54a1317cca0e890a2770630cf7fa6c97813e0cb9d2caa93012b350668	
Hash	9fc2570b7cef51c1b8df116d144d11ff4096357be7d2c4c6367cfc2509cf1bcc	
Hash	fd3ca4007b225fdf8de7af4345a19179d5efa8c4bb9205f88cda806e5684b1eb	
Hash	4140f7e17e6f97f83aa3472473e01add	
Hash	7bcf8d9f6834c44450eac145a967d2f2	
Hash	f92ee93a0af971a3966bfa8efa9c2625	
Hash	e65b155ce74f3f81fb7d2b5b60f8e62b36e6d69c	
Hash	b27b82afa5f15512f3856e549fb83d873fd0049759a4b62ce64c8d7d4dc2c678	

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:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 7+ groups that use Compromise Software Supply Chain, this pairing runs 2.6x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1203 Exploitation for Client Execution in an attempt to execute malicious code on the client-side, potentially by exploiting unpatched vulnerabilities in software applications, which may allow them to bypass earlier supply chain compromises and still achieve their objectives. This technique may be particularly appealing as it enables the actor to target client applications that are widely used within the organization, increasing the potential attack surface. To counter this, the mandated defensive control of patching client applications, enabling exploit mitigations such as ASLR, DEP, and CFG, and implementing application isolation would likely be effective.

Also plausible (same tactic): T1047 Windows Management Instrumentation (n=6, lift 2.2), T1569 System Services (n=3, lift 2.7)

Detection and hardening for the pivot (T1203 Exploitation for Client Execution)

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**
  - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs
  - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash
  - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
  - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
  - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015 Application Log