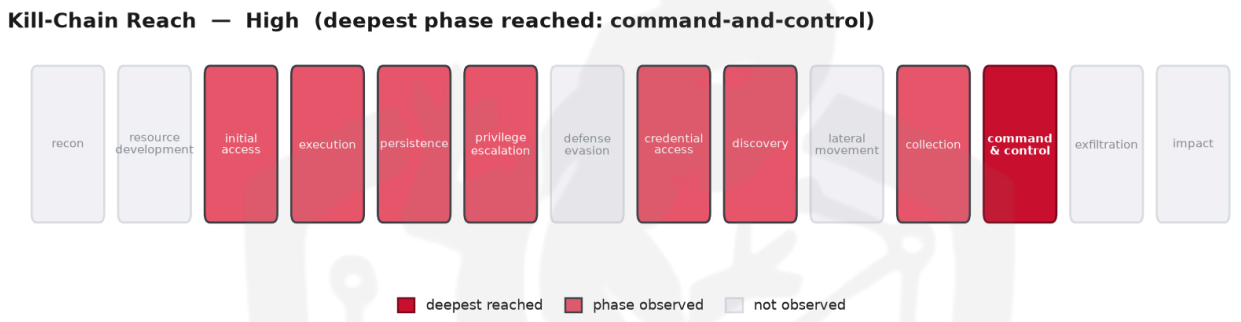
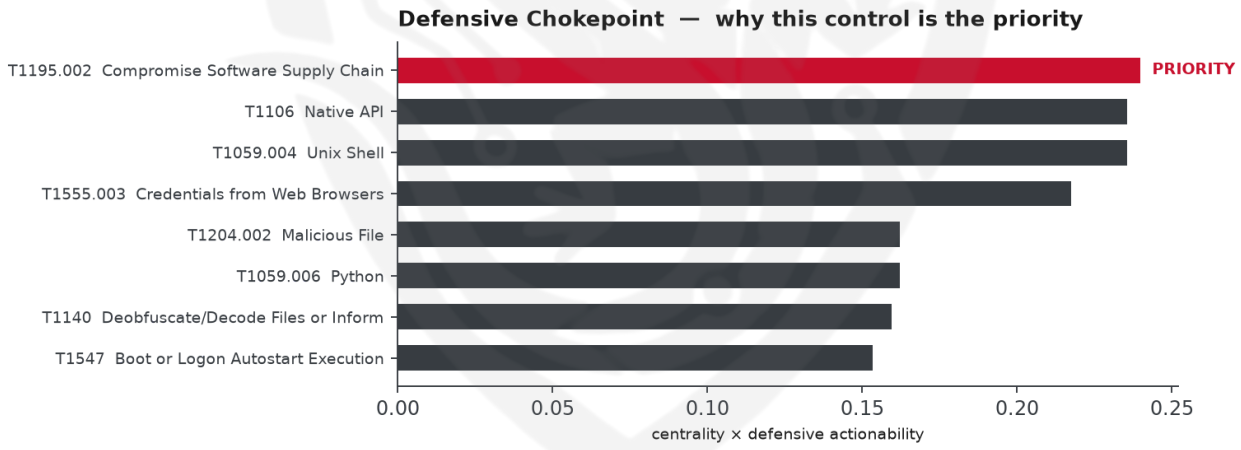
THREAT REPORT: COMPROMISED NPM BETA RELEASES DELIVER DEV#POPPER REMOTE ACCESS TROJAN

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 two Joyfill npm beta releases to deliver the DEV#POPPER Remote Access Trojan, targeting the technology sector. The priority defensive action should be given to verifying software supply chain integrity. The threat actor remains unattributed, and the targeted country is unknown. The malware campaign poses a high operational risk due to its ability to reach command-and-control levels.

Threat Overview

The threat actor, whose identity is insufficient to determine, has utilized the DEV#POPPER and OmniStealer malware families to compromise software supply chains. The central vulnerability exploited is

unknown, but various techniques have been employed, including screen capture, JavaScript execution, and system information discovery. The technology sector has been targeted, but the specific country and other details remain insufficient.

Attack Chain and Priority Control

The observed techniques form a chain that includes screen capture, JavaScript execution, and system information discovery, ultimately leading to the compromise of software supply chains. The priority technique is T1195.002 Compromise Software Supply Chain, which serves as a 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

The malicious infrastructure is hosted by Evoxt Sdn. Bhd. However, no malware families have been corroborated by abuse.ch, and no indicators have reached an 80% confidence level on AbuseIPDB, with the highest confidence seen being 0%. These findings are based on third-party enrichment and corroboration, attributed to their respective sources.

Technical Appendix

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

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

- T1113 Screen Capture
- T1059.007 JavaScript
- T1547 Boot or Logon Autostart Execution
- T1204.002 Malicious File
- T1115 Clipboard Data
- T1082 System Information Discovery
- T1106 Native API
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1560 Archive Collected Data
- T1555.003 Credentials from Web Browsers
- T1059.004 Unix Shell
- T1027 Obfuscated Files or Information
- T1195.002 Compromise Software Supply Chain
- T1059.006 Python
- T1555.004 Windows Credential Manager
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1195.002 Compromise Software Supply Chain (centrality 0.2399).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4616; 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
APT37	0.4616
Dark Caracal	0.4305
Molerats	0.417
Inception	0.3934
Windshift	0.3831

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	23[.]27[.]202[.]27	AbuseIPDB 0% (US) · AS149440 Evoxt Sdn. Bhd.
IP	198[.]105[.]127[.]210	AbuseIPDB 0% (GB) · AS149440 Evoxt Sdn. Bhd.
IP	166[.]88[.]134[.]62	AbuseIPDB 0% (GB) · AS149440 Evoxt Sdn. Bhd.
IP	23[.]27[.]13[.]43	AbuseIPDB 0% (GB) · AS149440 Evoxt Sdn. Bhd.

Type	Indicator	Context
Hash	2cfede38fb121a71a2f3607474aa8cd588a99f51b37e5e6f0d8cb789fa275032	
Hash	26351aed0397158d3a3b8cc8fd3047d4c015d264c9895f10f20f1521b974ed18	
Hash	36ff00b45e67baa7e3674b0c80f48e88737264c61e5c6b3b091200972de8157c	
Hash	adc4af90540d33cd1e98f44b51482ae9250fbeb97d6f8d7841c81b618cb2c6e6	
Hash	8e8b90dedd456ded0c5748119836e1ca1066112bc569c1b41ca70eb931d1d4dc	
Hash	5f6a92006ca2ea4b464d66fb41af777edce7296939a7c6ee491e2b3cbfe09848	
Hash	bcc93dc55bc7daedf4ca57254f0e7a7f1c40e09851eab98fe10cde801982db17	
Hash	1352ad22c99983d91e600348b7cbf58235131b1ee34cea9f09623206d5b7dea7	
Hash	67c6ef602cc850f10d935fee53fa40440df841adf081563bf4fc2631a71249ce	
Hash	c5742ea1875ecd2360022624149994909cd0546e221e4203dffd01f48de45469	
Hash	cb46f12d70824ea24ed1f8bcf45bf3f86680e02a9089aafc03b27f691be57be3	
Hash	f452f9cfa539f4a1fe25187a99a484391290d5dbaa422ba455edf6b04f81b7d1	
Hash	78f0de8682e0e894a5784eb7e95db4da6088f528918ca3107dd1e76f80a561d8	
Hash	ae7565109fd01b88d82acf7f73ab20709cbc2c9f26fdea13e429ccc87a55d4fb	
Hash	26e679eaf1e9baeb7c55eb48db482301171d4d26e1728544b23734a90dc70e1b	
Hash	b7c8c84d1729e78ca9d64d1d6dd97fe4	

Type	Indicator	Context
Hash	e147076dd588df4e2bc9db25fcc306fb34a04a55	

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.

The actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious code at a later time, potentially exploiting the fact that scheduled tasks can be used to bypass security controls and blend in with legitimate system activity. This technique may be particularly appealing as it allows the actor to execute code in the context of a legitimate process, making it harder to detect. To counter this, the defensive control of alerting on new scheduled tasks (Event ID 4698), restricting schtasks/at to admins, and baselining legitimate task creators should be implemented.

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