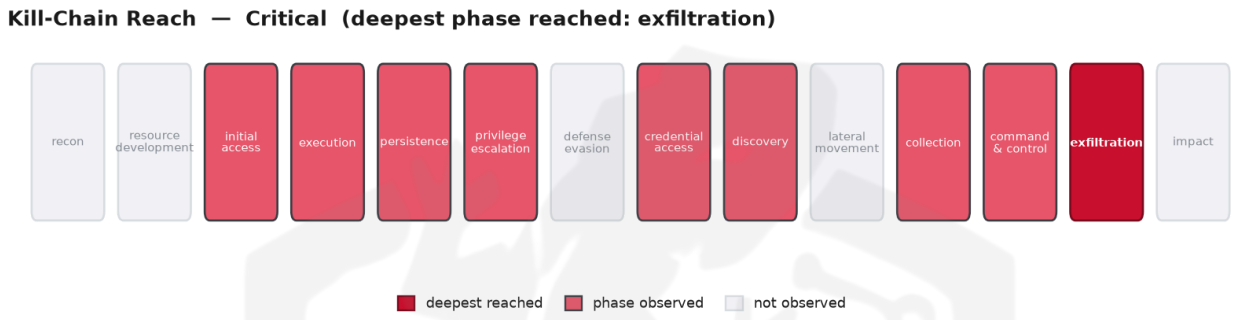
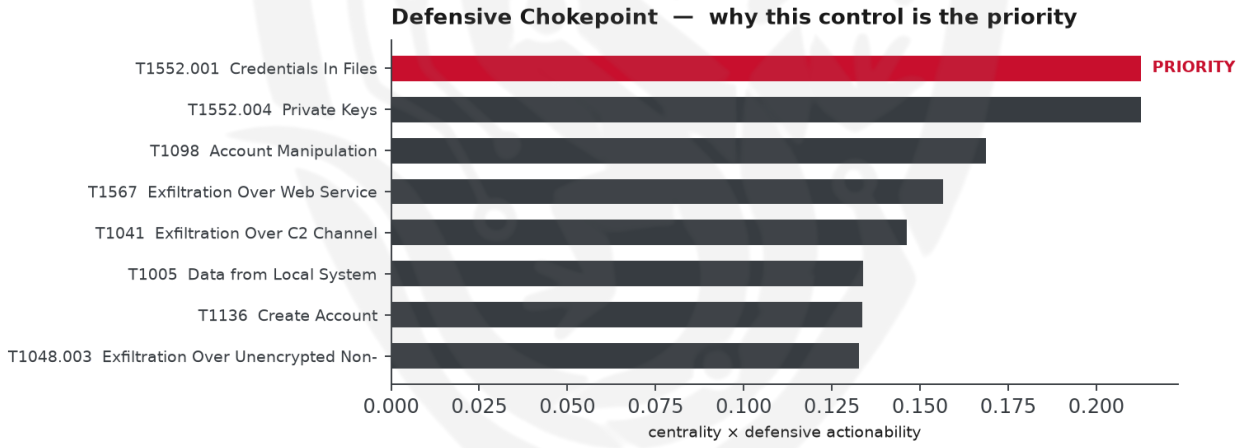
THREAT REPORT: UNKNOWN_ADVERSARY MALWARE CAMPAIGN

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 has been identified as a malware campaign targeting the technology sector, utilizing the node-ipc npm package to steal credentials. The campaign's impact is considered critical due to the potential for exfiltration of sensitive data. Priority should be given to removing secrets from code, configuration files, and registries, as well as deploying a secrets manager to mitigate the threat. The affected organizations should also scan their repositories and hosts for credentials to prevent further compromise.

Threat Overview

The threat actor, whose identity is currently unknown, is exploiting the node-ipc malware family to compromise the software supply chain and steal credentials from targeted systems. The actor is using

various techniques, including compromise of software supply chain, valid accounts, and account manipulation, to gain access to sensitive information. The primary goal of the actor appears to be the exfiltration of credentials and other sensitive data.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including compromise of software supply chain, creation of accounts, and manipulation of accounts, ultimately leading to the exfiltration of sensitive data. The priority technique in this chain is T1552.001 Credentials In Files, which is the graph chokepoint. To mitigate this threat, the priority control is to "Remove secrets from code/config/registry; deploy a secrets manager; scan repos and hosts for credentials."

Infrastructure and Corroboration

Although the hosting providers and ASNs observed are not available, the malware family has been corroborated by abuse.ch as Shai-Hulud. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, and the highest confidence seen is 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)

- T1195.002 Compromise Software Supply Chain
- T1078 Valid Accounts
- T1136 Create Account
- T1098 Account Manipulation
- T1071.004 DNS
- T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol
- T1041 Exfiltration Over C2 Channel
- T1567 Exfiltration Over Web Service
- T1005 Data from Local System
- T1552.001 Credentials In Files
- T1552.004 Private Keys
- T1087 Account Discovery
- T1082 System Information Discovery
- T1083 File and Directory Discovery
- T1119 Automated Collection
- T1074.001 Local Data Staging
- T1560.001 Archive via Utility
- T1027 Obfuscated Files or Information
- T1027.002 Software Packing
- T1059.007 JavaScript

Analytical Scores

- Priority technique (graph chokepoint): T1552.001 Credentials In Files (centrality 0.3037).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3939; 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
APT3	0.3939
Wizard Spider	0.3411
FIN13	0.3333
APT39	0.3175
APT18	0.3175

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Shai-Hulud.
- 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	sh[.]azurestaticprovider[.]net	Shai-Hulud
Domain	atlantis-software[.]net	
Domain	child[.]channel	
URL	hxxp://sh[.]azurestaticprovider[.]net:443	
Hash	96097e0612d9575cb133021017fb1a5c68a03b60f9f3d24ebdc0e628d9034144	

Type	Indicator	Context
Hash	78a82d93b4f580835f5823b85a3d9ee1f03a15ee6f0e01b4eac86252a7002981	
Hash	c2f4dc64aec4631540a568e88932b61daebbfb7e8281b812fa01b7215f9be9ea	
Hash	449e4265979b5fdb2d3446c021af437e815debd66de7da2fe54f1ad93cbcc75e	
Hash	bf9d8c0c3ed3ceaa831a13de27f1b1c7c7b7f01d2db4103bfdba4191940b0301	

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:** T1552.001 Credentials In Files (credential-access)
- **Observed here:** the threat actor used T1552.004 Private Keys here as an alternative credential-access technique.
- **Projected pivot:** T1552.004 Private Keys (credential-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to using T1552.004 Private Keys if they have access to private key files, which may allow them to maintain their objective of obtaining credentials. This technique would likely involve searching for and exploiting private key files that are not properly secured, which could provide an alternative means of authentication. The defensive countermeasure to mitigate this would be to remove secrets from code/config/registry; deploy a secrets manager; scan repos and hosts for credentials.

- **Defensive countermeasure:** Remove secrets from code/config/registry; deploy a secrets manager; scan repos and hosts for credentials.