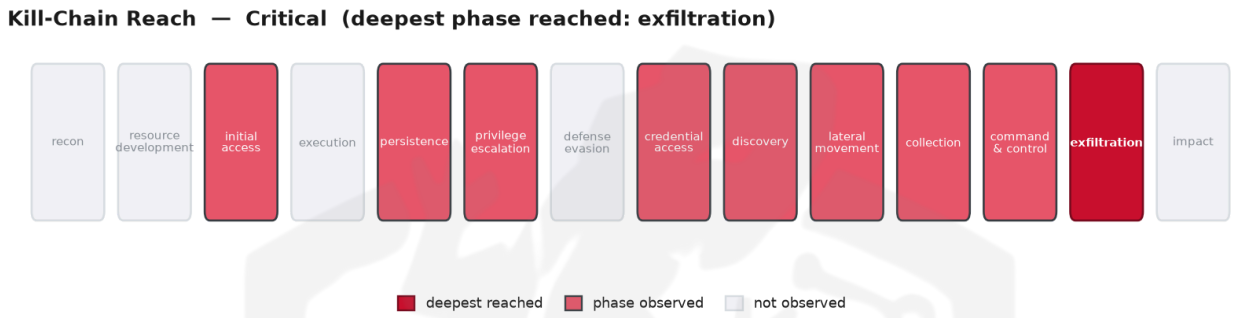
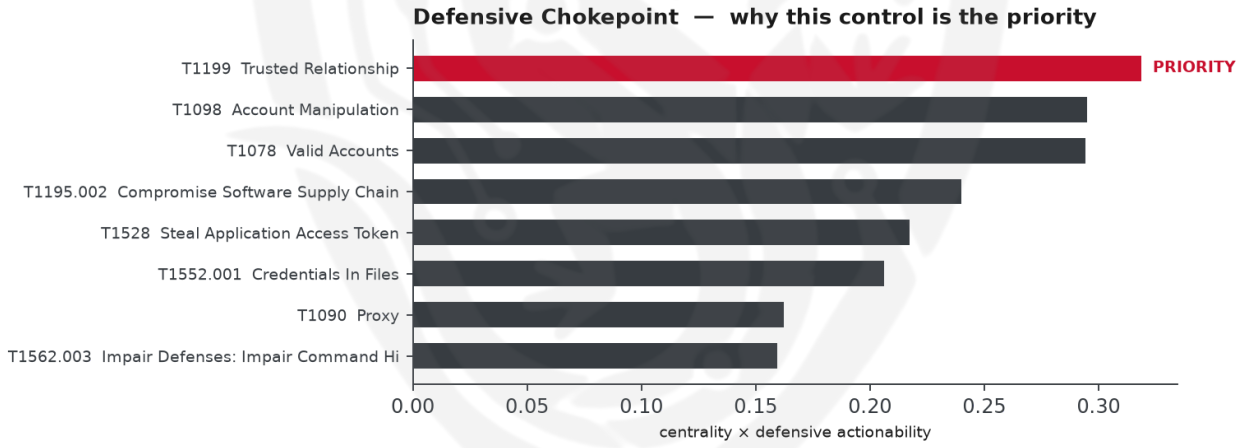
THREAT REPORT: SHAI-HULUD AND MIASMA MALWARE CAMPAIGN

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 involves the Shai-Hulud and Miasma malware families, targeting unspecified sectors and countries. The threat actor is exploiting various techniques to compromise software dependencies and exfiltrate data. Priority should be given to auditing and least-privileging trusted third-party connections to mitigate the risk. The campaign's ability to impair defenses and exfiltrate data over web services makes it a critical operational risk.

Threat Overview

The threat actor, utilizing the Shai-Hulud and Miasma malware families, is exploiting multiple techniques, including compromising software dependencies and development tools, exploiting public-facing applications, and exfiltrating data over web services. The victimology and targeted countries are currently

unknown. The actor's techniques include account discovery, proxy usage, and stealing application access tokens, indicating a sophisticated campaign.

Attack Chain and Priority Control

The observed techniques form a complex attack chain, with the threat actor compromising software dependencies, exploiting public-facing applications, and exfiltrating data over web services. The priority technique is T1199 Trusted Relationship, which serves as a graph chokepoint. To mitigate this risk, the priority control is to "Audit and least-privilege trusted third-party/B2B connections; monitor partner-account activity."

Infrastructure and Corroboration

The malicious infrastructure is hosted on various providers, including FiberState LLC, FDCServers.net, Viettel Corporation, and China Telecom Beijing Tianjin Hebei Big Data Industry Park Branch. However, no malware families have been corroborated by abuse.ch, and 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)

- T1195.001 Compromise Software Dependencies and Development Tools
- T1190 Exploit Public-Facing Application
- T1567 Exfiltration Over Web Service
- T1552.004 Private Keys
- T1087 Account Discovery
- T1090 Proxy
- T1552.001 Credentials In Files
- T1528 Steal Application Access Token
- T1562.003 Impair Defenses: Impair Command History Logging
- T1199 Trusted Relationship
- T1098 Account Manipulation
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1195.002 Compromise Software Supply Chain
- T1562.008 Impair Defenses: Disable or Modify Cloud Logs
- T1213 Data from Information Repositories
- T1071.001 Web Protocols
- T1550.001 Application Access Token

Analytical Scores

- Priority technique (graph chokepoint): T1199 Trusted Relationship (centrality 0.3187).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3311; 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
GOLD SOUTHFIELD	0.3311
HAFNIUM	0.2824
POLONIUM	0.2767
FIN13	0.2649
Ember Bear	0.2644

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	38[.]46[.]219[.]162	AbuseIPDB 0% (US) · AS26042 FiberState LLC
IP	116[.]105[.]166[.]148	AbuseIPDB 0% (VN) · AS24086 Viettel Corporation
IP	38[.]46[.]219[.]166	AbuseIPDB 0% (US) · AS26042 FiberState LLC
IP	38[.]46[.]219[.]163	AbuseIPDB 0% (US) · AS26042 FiberState LLC
IP	23[.]237[.]196[.]170	AbuseIPDB 0% (US) · AS30058 FDCServers.net
IP	198[.]255[.]70[.]210	AbuseIPDB 0% (US) · AS30058 FDCServers.net

Type	Indicator	Context
IP	117[.]72[.]74[.]48	AbuseIPDB 0% (CN) · AS141679 China Telecom Beijing Tianjin Hebei Big Data Industry Park Branch
Domain	amutes[.]com	
Domain	abb1[.]life	

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:** T1199 Trusted Relationship (initial-access)
- **Observed here:** T1199 Trusted Relationship 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 5+ groups that use Trusted Relationship, this pairing runs 1.7x 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 maintain their objective, as this technique may allow them to leverage vulnerabilities in client applications to execute malicious code, potentially bypassing the blocked trusted relationship. This technique is particularly appealing as it could enable the actor to exploit widely used software, such as Office or browsers, to gain a foothold in the system. To counter this potential move, the mandated defensive control of patching client applications, enabling exploit mitigations like ASLR, DEP, and CFG, and implementing application isolation would likely be an effective measure.

Also plausible (same tactic): T1047 Windows Management Instrumentation (n=5, lift 1.7), T1059 Command and Scripting Interpreter (n=10, lift 1.2)

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