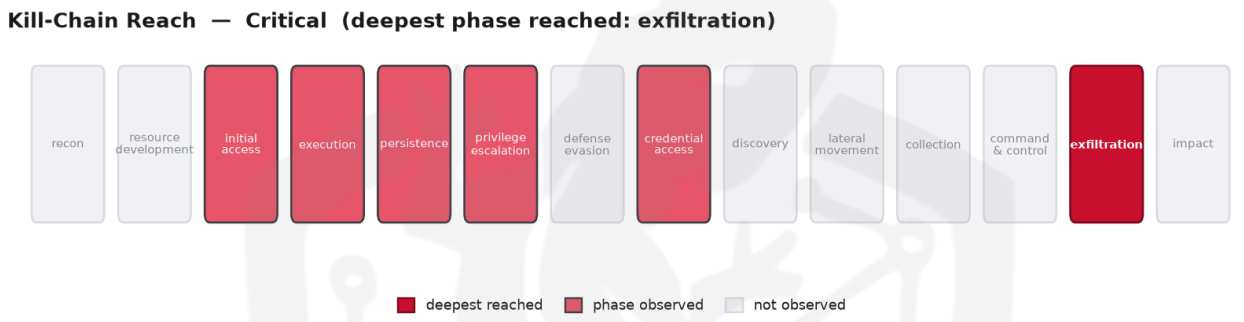
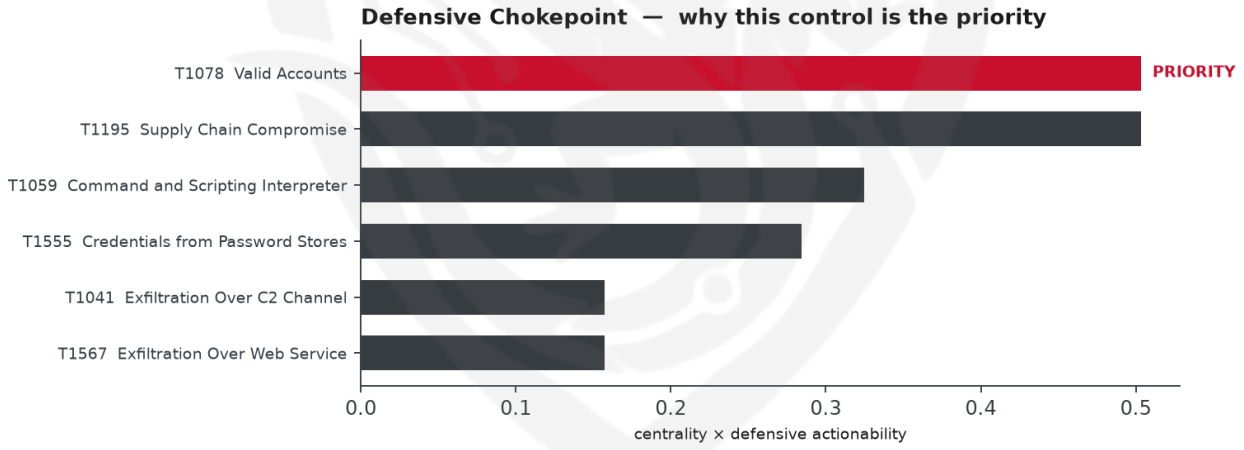
THREAT REPORT: SHAI-HULUD TARGETING INTERCOM CLIENTS WITH CREDENTIAL HARVESTING

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

Shai-Hulud has been observed targeting technology sector organizations by exploiting the Intercom-client version 7.0.4 to harvest GitHub credentials. The activity involves credential theft and exfiltration over command-and-control channels. Priority defensive action is to enforce multi-factor authentication on all accounts, disable dormant and over-privileged accounts, and monitor for impossible-travel and anomalous logons.

Threat Overview

The threat actor Shai-Hulud deployed a credential-harvesting technique against Intercom-client@7.0.4, focusing on technology sector victims. No specific malware family or CVE is identified in the source report.

The activity is characterized by supply-chain compromise and exfiltration over web services.

Attack Chain and Priority Control

The observed attack chain includes supply-chain compromise, use of valid accounts, command and scripting interpreter, credential extraction from password stores, and exfiltration over C2 channels and web services. The priority technique is **T1078 Valid Accounts**.
Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

Abuse.ch corroborates the presence of Shai-Hulud in the malicious activity. No high-confidence IP indicators were reported, and hosting providers or ASNs were not observed.

Technical Appendix

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

Observed Techniques (ATT&CK, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1041 Exfiltration Over C2 Channel - T1059 Command and Scripting Interpreter - T1078 Valid Accounts - T1195 Supply Chain Compromise - T1555 Credentials from Password Stores - T1567 Exfiltration Over Web Service

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.5033).
- Operational risk: Critical (score 0.843, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3086; 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
Suckfly	0.3086
Threat Group-1314	0.3086
Stealth Falcon	0.281
ZIRCONIUM	0.252
Akira	0.25

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	zero[.]masscan[.]cloud	Shai-Hulud

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:** T1078 Valid Accounts (initial-access)
- **Observed here:** T1078 Valid Accounts 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:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 29+ groups that use Valid Accounts, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

Shai-Hulud could pivot to T1047 Windows Management Instrumentation to maintain access and evade detection, as this technique allows them to leverage the existing Windows Management Instrumentation (WMI) framework to execute commands and gather information, potentially exploiting the trust associated with legitimate WMI activity. This technique may be particularly appealing to Shai-Hulud given the prior

use of valid accounts, as WMI can be used to interact with the system in a way that blends in with normal administrative activity. To counter this potential pivot, the mandated defensive control is to monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1053 Scheduled Task/Job (n=31, lift 1.4)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command