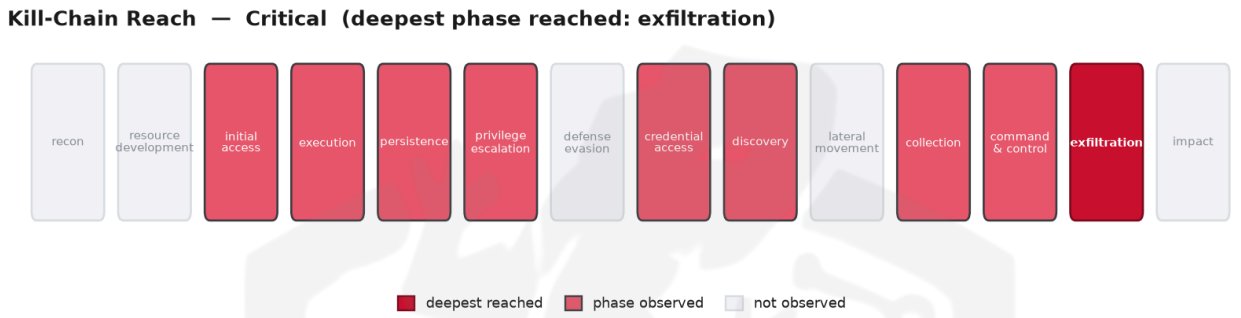
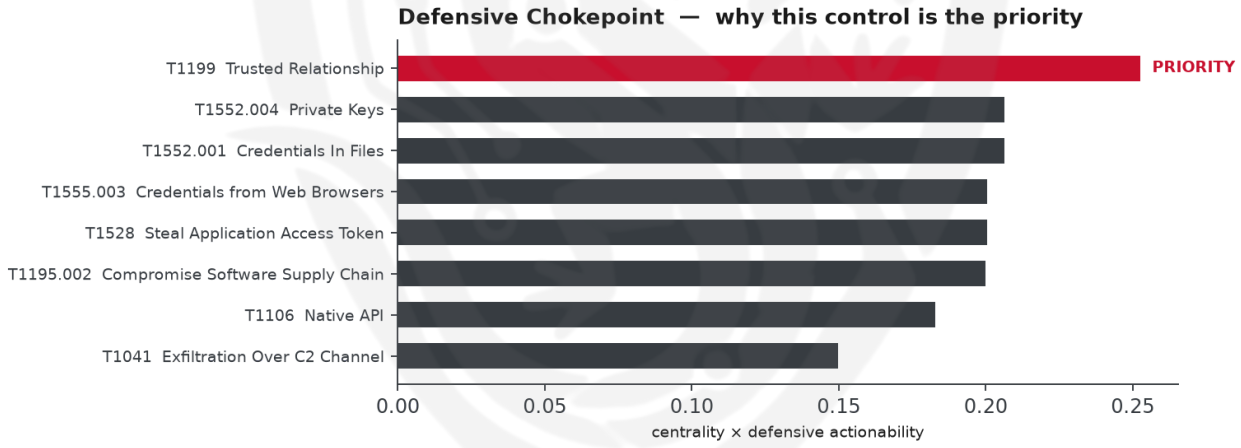
# THREAT REPORT: UNKNOWN_ADVERSARY SUPPLY CHAIN COMPROMISE

## 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 supply chain compromise, leveraging GitHub Actions to target the technology sector. The malware families Miasma and M-RED-TEAM have been observed in this campaign. Priority should be given to auditing and least-privileging trusted third-party connections to mitigate the risk of compromise. The threat actor's ability to establish trusted relationships is a critical concern, as it enables exfiltration of sensitive data.

## Threat Overview

The threat actor, whose identity is unknown, has been observed utilizing various techniques, including standard encoding, JavaScript, and symmetric cryptography, to compromise their targets. The malware families Miasma and M-RED-TEAM have been identified as part of this campaign, which appears to be

focused on the technology sector. The actor's goals and motivations are not well understood, but their ability to establish trusted relationships with their targets is a key aspect of their approach.

## Attack Chain and Priority Control

The observed techniques used by the threat actor can be described as a complex chain of events, including encoding and decoding files, discovering files and directories, and exfiltrating data over command and control channels. The priority technique in this chain is T1199 Trusted Relationship, which is the graph chokepoint. To mitigate this threat, the priority control is to "Audit and least-privilege trusted third-party/B2B connections; monitor partner-account activity."

## Infrastructure and Corroboration

There is no corroboration from third-party sources such as abuse.ch or AbuseIPDB, as no malware families have been corroborated and no indicators have been flagged with high confidence. As a result, there is limited information available on the hosting providers or ASNs used by the threat actor.

---

## Technical Appendix

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

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

- T1132.001 Standard Encoding
- T1059.007 JavaScript
- T1071.004 DNS
- T1555.001 Keychain
- T1573.001 Symmetric Cryptography
- T1106 Native API
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1555.003 Credentials from Web Browsers
- T1552.004 Private Keys
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1528 Steal Application Access Token
- T1041 Exfiltration Over C2 Channel
- T1199 Trusted Relationship
- T1027 Obfuscated Files or Information
- T1195.002 Compromise Software Supply Chain
- T1071.001 Web Protocols
- T1543.002 Systemd Service
- T1105 Ingress Tool Transfer
- T1078.004 Cloud Accounts

## Analytical Scores

- Priority technique (graph chokepoint): T1199 Trusted Relationship (centrality 0.2527).
- Operational risk: Critical (score 0.968, reaches exfiltration).

## Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3995; 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 |
|---|---|
| APT33 | 0.3995 |
| Stealth Falcon | 0.377 |
| APT18 | 0.3443 |
| Tropic Trooper | 0.3416 |
| TA505 | 0.3324 |

## 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 |
|---|---|
| Hash | 22bf76fe317ea6769bd38619bd440e42d119bd6b |
| Hash | 9890950adcbc2478e7a080234f053214adbad44e |
| Hash | a7e18d96efd3cdb127ef4cdcad9e3ad26c482bf2 |
| Hash | c70e105e212ff3c1daa04bb2a62507717f296b0b |
| Hash | c8cb3f6d5b90c46686d2bf531dc1a5786e27edc5 |

## 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:** the threat actor used T1078.004 Cloud Accounts here as an alternative initial-access technique.
- **Projected pivot:** T1078.004 Cloud Accounts (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to utilizing Cloud Accounts (T1078.004) to maintain access and achieve their objectives, potentially by leveraging compromised or newly created cloud accounts to bypass the blocked Trusted Relationship (T1199) control. This shift may allow the actor to continue their campaign, potentially exploiting weaknesses in cloud account security to regain a foothold. To counter this potential move, the mandated defensive control of Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons should be implemented.

**Detection and hardening for the pivot (T1078.004 Valid Accounts)**

- **Telemetry:** Windows Security (logon events); Azure AD / IdP sign-in logs; VPN and remote-access logs; Proxy / DLP / data-egress volume telemetry
- **Detect:**
  - Security 4624/4625 (logon success/fail), 4768/4769 (Kerberos TGT/TGS), 4776 (NTLM)
  - Impossible-travel, new-geo, and off-hours sign-ins from the IdP
  - Service or dormant accounts logging on interactively
  - Under valid credentials the identity signal goes quiet: baseline per-account data-egress volume and alert on peer-group and historical deviation (the real exfiltration tell)
- **Harden:**
  - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
  - Least-privilege review; separate admin from daily-driver accounts
  - Set per-account and per-partner egress baselines with DLP thresholds on sensitive stores
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account