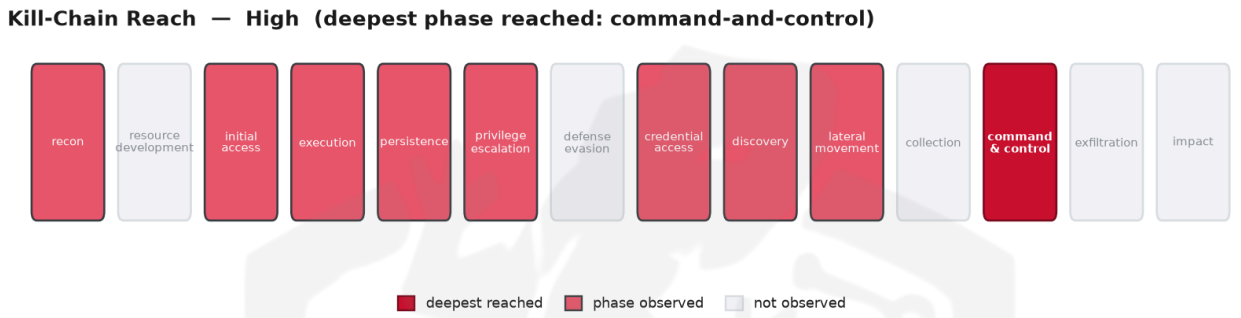
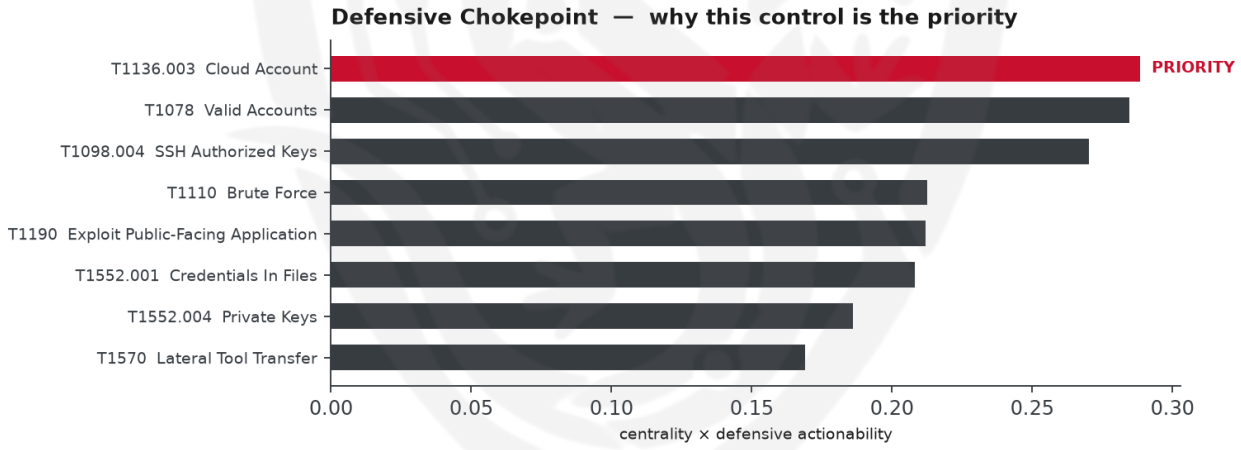
THREAT REPORT: UNKNOWN_ADVERSARY NADMESH CAMPAIGN

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 linked to the NadMesh malware family, which exploits the CVE-2016-0638 vulnerability, primarily targeting the technology sector. The threat actor's identity remains unknown due to insufficient data. Priority should be given to patching the CVE-2016-0638 vulnerability on all affected systems to prevent further exploitation. The campaign's impact is considered high, reaching command-and-control levels.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, utilizes the NadMesh malware family to exploit the CVE-2016-0638 vulnerability. The victimology of this campaign is focused on the technology

sector, although specific country targets are unknown due to insufficient data. The malware's ability to exploit this vulnerability allows for significant control over compromised systems.

Attack Chain and Priority Control

The attack chain involves multiple techniques, including boot or logon initialization scripts, external remote services, and exploit public-facing application vulnerabilities. The priority technique identified is T1136.003 Cloud Account, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority action is to: Patch CVE-2016-0638 on all affected systems as the top priority, then: Alert on new local/domain account creation (Event ID 4720/4728); enforce approval workflow for account provisioning.

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted on providers such as SKN Subnet & Telecom Ltd. While there are no malware families corroborated by abuse.ch, indicators have been flagged with a confidence level of up to 68% by AbuseIPDB, although none reach the 80% confidence threshold. These corrobations are based on third-party data and serve to enrich the understanding of the campaign's infrastructure without overriding the primary source information.

Technical Appendix

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

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

- T1037 Boot or Logon Initialization Scripts
- T1133 External Remote Services
- T1543.003 Windows Service
- T1053.003 Cron
- T1190 Exploit Public-Facing Application
- T1595.002 Vulnerability Scanning
- T1552.004 Private Keys
- T1098.004 SSH Authorized Keys
- T1552.001 Credentials In Files
- T1136.003 Cloud Account
- T1110 Brute Force
- T1027.005 Indicator Removal from Tools
- T1078 Valid Accounts
- T1573 Encrypted Channel
- T1570 Lateral Tool Transfer
- T1095 Non-Application Layer Protocol
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1046 Network Service Discovery

- T1552.007 Container API

Analytical Scores

- Priority technique (graph chokepoint): T1136.003 Cloud Account (centrality 0.3037).
- 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 0.3556; 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
TeamTNT	0.3556
Rocke	0.3266
APT41	0.323
Ember Bear	0.3203
APT3	0.3012

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 68%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	209[.]99[.]186[.]235	AbuseIPDB 68% (CH) · AS402253 SKN Subnet & Telecom Ltd
Domain	cdnorigin[.]net	
Hash	ca024acead8f54cfe5b07ac4bdf7fcea	
Hash	31c69b3e12936abca770d430066f379ec1d997ec	

Type	Indicator	Context
Hash	fc4109f5dd1d30b65dd60e57dc639ac1d313bfa5241e36e61fbc4aabc1cda482	

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:** T1136.003 Cloud Account (persistence)
- **Observed here:** the threat actor used T1078 Valid Accounts here as an alternative persistence technique.
- **Projected pivot:** T1078 Valid Accounts (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to using T1078 Valid Accounts by attempting to leverage compromised or stolen credentials to maintain access to the target environment, potentially exploiting weak password policies or unsecured account configurations. This could allow the actor to bypass the blocked cloud account control and continue their campaign. The defensive countermeasure would be to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Detection and hardening for the pivot (T1078 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