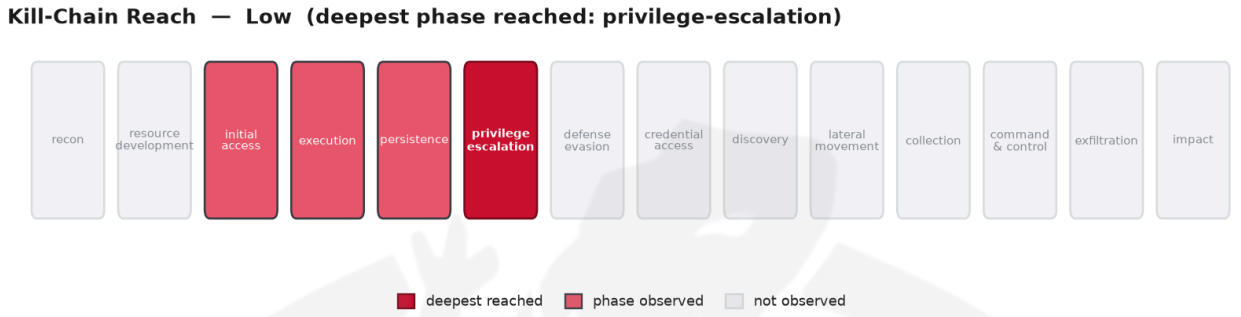
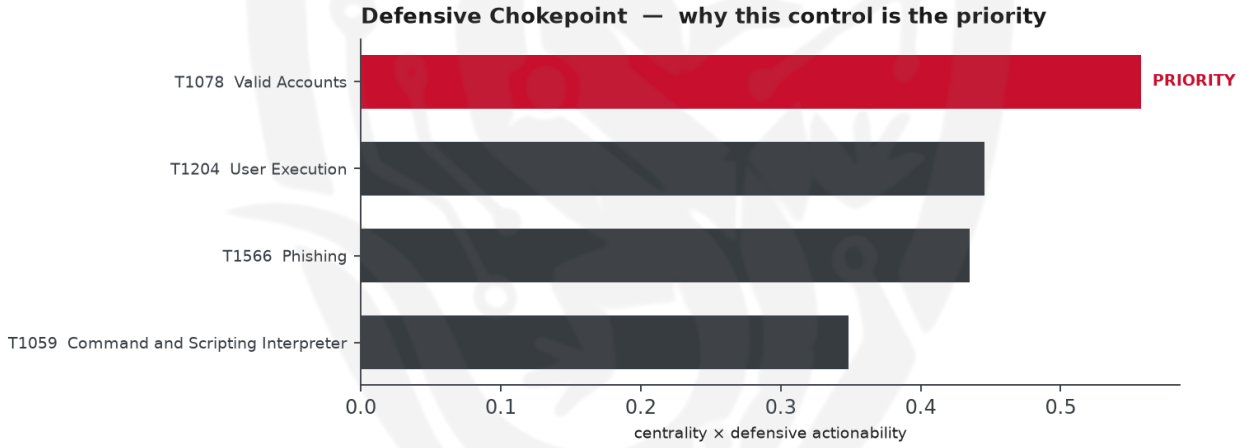
THREAT REPORT: BABADEDA LOADER CAMPAIGN

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, associated with the BabaDeda Loader, has been identified as a potential threat, although the threat actor remains unattributed. The campaign's targets and sectors affected are currently unknown. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate potential damage. The threat is characterized by a low operational risk band, reaching privilege-escalation levels.

Threat Overview

The threat actor, responsible for the BabaDeda Loader campaign, utilizes various techniques, including those inferred from the report such as command and scripting interpreter, valid accounts, user execution, and phishing. The central vulnerability exploited is currently unknown. The victimology of this campaign is also unclear due to insufficient data.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including command and scripting interpreter, valid accounts, user execution, and phishing, which ultimately lead to potential privilege escalation. The priority technique identified is the use of valid accounts (T1078). To counter this, the priority control is to "Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons."

Infrastructure and Corroboration

Although the hosting providers and ASNs observed are not available, third-party corroboration from abuse.ch indicates the presence of the Arechclient2 malware family. However, according to AbuseIPDB, there are no 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, 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. - T1059 Command and Scripting Interpreter - T1078 Valid Accounts - T1204 User Execution - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.5573).
- Operational risk: Low (score 0.276, reaches privilege-escalation).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5303; 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
TA459	0.5303
APT30	0.5
TA577	0.4523
Nomadic Octopus	0.4523
Gallmaker	0.4523

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Arechclient2.
- 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	cirealci[.]com	
Domain	humansbad2026[.]com	
URL	hxxp://91[.]92[.]243[.]161:3038	
URL	hxxp://89[.]124[.]81[.]216:9000/wbinjget?q=B2E581C85432BD4DF6A59A00CBDA1CB3	
URL	hxxp://94[.]26[.]83[.]190:6600/t36umsn9/DataRescueCommunity	
URL	hxxp://95[.]163[.]152[.]190/linguist[.]zip	
URL	hxxp://humansbad2026[.]com/track[.]php?d=	
Hash	b2e581c85432bd4df6a59a00cbda1cb3	
Hash	2efaac26a7e8c4efaaf643f19cb8b978	
Hash	3c32116f5e98f5920c2d9f2b19755077	
Hash	bf43af6116053819ebd41ee1deb40f85446c774d	
Hash	c11d639851e27293cddac5eec891e909cc641821	
Hash	0c0dc13805564d986b5eac6c5e8c90d336256fbb7f8a0c52180f1f5c690fe203	

Type	Indicator	Context
Hash	1e1d25391cf825d9607f652249e33cf1d2b98f260b587a1b1b33710e2ea6b91f	
Hash	2afa7b6f825ae82c0121117b2966c57d825e7f1cfecaef36e638f66a08060db6	
Hash	3b4208ec304b60ba9d0ca74838ad7031224a32c36d6e1fa7c616a5ecf5074a5b	
Hash	3e881c9663db5c80a0093f4b0f7008aa1e73866c57aa672e53b38274df4c2807	
Hash	425501b6428e19536be925b4a286f73ae94270bc23ac516832ea27ba6c875998	
Hash	5c6144b1bb4c195a4dcd7ebac8c427852c7e15cb5b4f5217dda0cfb39a90062a	Arechclient2
Hash	71f19394bf15ae47b668fcbe13d0fe4d46d8c06ce004eeccf82c8d1770bba558	
Hash	7eb345c26a1b827e7b2ef5b7881cb406b04b056ebc36cc92e3f7643decd2671f	
Hash	809d030d1fd65c909260b4b33bff9c99f775aea332d944ad1f64b4e5e81a6d60	
Hash	91255813151e6fb3d2a45e088490214c110ff035bbd1ee01ff430782868c77b3	
Hash	9677584602ae15bdd20d91b9a14768a17c126107739e3853d969ff4e02e10e71	
Hash	9a736f4812b485f9cf5b1332a791b205b5135a4b3a0c41f473ad9cc9fbe2d75c	
Hash	a8a2148d6cf70d06a9c2ecded8b1a21f982cf11ffc9774442209f536a66a8630	Arechclient2
Hash	c92950568a2b757d4ee0bad84b33f5b3414f0d5fdf3d3f5b06e7d304a7ccf1a1	
Hash	d79a454beabcd59459c350c71598bffd6badb6a8905b0e9fa3c1ee22cbef7d7e	
Hash	dcd612f1d86ff5c9b43f1a3d0baea16b9c08e4b844bcd82564c720ee1caafe3c	
Hash	e38550a29e4ff48d8cd4df5ab34a88b9b28f23d50e66129c896689cd334849a9	
Hash	fa25acfac32c557f809ab544764d4348f31cf9909ad9d512883d6cba8369ba88	

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.

The actor could pivot to T1047 Windows Management Instrumentation to maintain access and evade detection, as this technique allows them to leverage the existing Windows management infrastructure to execute commands and gather information, potentially exploiting the same valid account credentials that were previously used. This technique may be particularly appealing to the actor because it enables them to blend in with legitimate administrative activity, making it more challenging to distinguish between benign and malicious behavior. To counter this potential move, 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