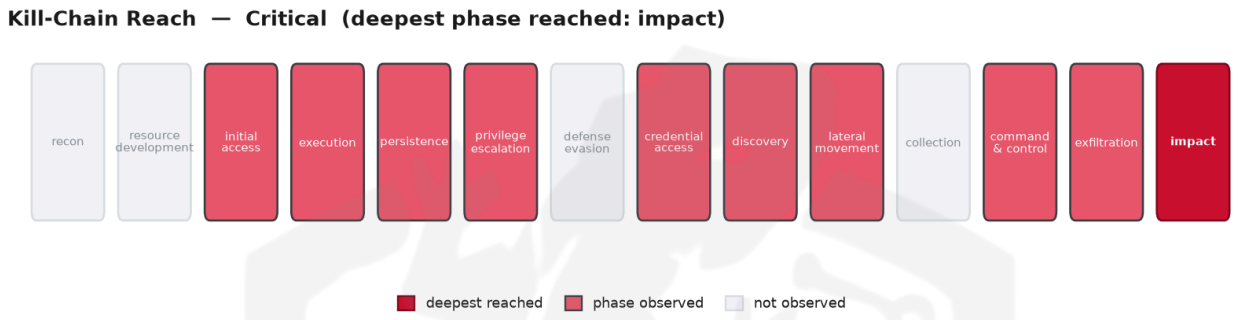
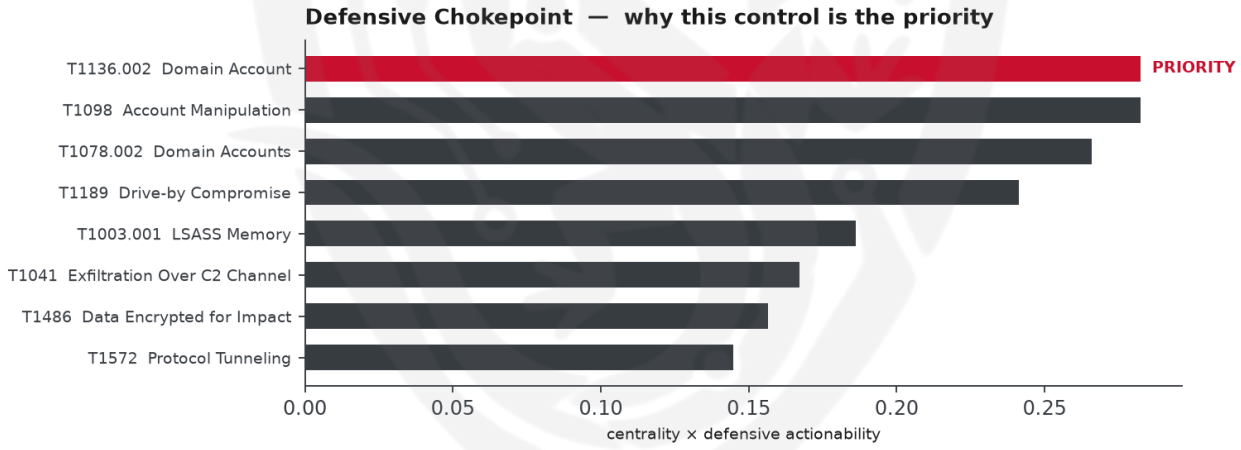
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 delivering the Akira ransomware through the Bumblebee and AdaptixC2 malware families. The threat actor's targets and motivations are not well understood, but the priority defensive action should be to monitor for new local and domain account creation. Given the operational risk band is Critical, priority should be given to enforcing approval workflows for account provisioning to mitigate potential impact.

Threat Overview

The threat actor, whose identity is not specified, is utilizing the Bumblebee and AdaptixC2 malware families to deliver the Akira ransomware. The victimology and targeted sectors are not well understood,

but the techniques used include a range of system discovery, file manipulation, and account manipulation methods.

Attack Chain and Priority Control

The observed techniques form a complex chain, starting with system owner and user discovery, followed by malicious file execution, and culminating in data encryption for impact. The priority technique is T1136.002 Domain Account, which serves as a chokepoint in the attack chain. To mitigate this, the priority control is to Alert on new local/domain account creation (Event ID 4720/4728); enforce approval workflow for account provisioning.

Infrastructure and Corroboration

The malicious infrastructure is hosted on providers such as RockHoster Private Limited and Shock Hosting LLC. The malware families Akira and BumbleBee have been corroborated by abuse.ch, providing additional context to the threat. However, according to AbuseIPDB, the indicators have a relatively low confidence level, with the highest seen being 21%.

Technical Appendix

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

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

- T1033 System Owner/User Discovery
- T1204.002 Malicious File
- T1543.003 Windows Service
- T1069.002 Domain Groups
- T1082 System Information Discovery
- T1572 Protocol Tunneling
- T1003.001 LSASS Memory
- T1016 System Network Configuration Discovery
- T1136.002 Domain Account
- T1083 File and Directory Discovery
- T1041 Exfiltration Over C2 Channel
- T1098 Account Manipulation
- T1486 Data Encrypted for Impact
- T1078.002 Domain Accounts
- T1189 Drive-by Compromise
- T1071.001 Web Protocols
- T1018 Remote System Discovery
- T1574.002 Hijack Execution Flow
- T1021.001 Remote Desktop Protocol
- T1003.003 NTDS

Analytical Scores

- Priority technique (graph chokepoint): T1136.002 Domain Account (centrality 0.2973).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4323; 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
APT3	0.4323
Medusa Group	0.4174
Ke3chang	0.4048
Wizard Spider	0.3941
Scattered Spider	0.3734

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 21%.
- Malware families corroborated by abuse.ch: Akira, BumbleBee.
- 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
IP	172[.]96[.]137[.]160	AbuseIPDB 21% (US) · AS395092 Shock Hosting LLC
IP	109[.]205[.]195[.]211	AbuseIPDB 0% (DE) · AS215381 RockHoster Private Limited
IP	193[.]242[.]184[.]150	AbuseIPDB 0% (CA) · AS215381 RockHoster Private Limited

Type	Indicator	Context
Domain	angryipscanner[.]org	
Domain	opmanager[.]pro	
Domain	2rxyt9urhq0bgj[.]org	
Domain	axiscamerastation[.]org	
Domain	ev2sirbd269o5j[.]org	
Domain	ijt0l3i8brit6q[.]org	
Domain	ip-scanner[.]org	
Hash	a14506c6fb92a5af88a6a44d273edafe10d69ee3d85c8b2a7ac458a22edf68d2	BumbleBee
Hash	a746da514c90f26a187a294fda7edc1b	BumbleBee
Hash	bcee0ab10b23f5999bcdb56c0b4a631a	BumbleBee
Hash	1b9aa401457d29405c0bcf19cbf19a7028a0d214	BumbleBee
Hash	f352cec89a56e23dae20cdd62df4d40bc7f22b5e	BumbleBee
Hash	186b26df63df3b7334043b47659cba4185c948629d857d47452cc1936f0aa5da	
Hash	18b8e6762afd29a09becae283083c74a19fc09db1f2c3412c42f1b0178bc122a	
Hash	6ba5d96e52734cbb9246bcc3decf127f780d48fa11587a1a44880c1f04404d23	BumbleBee
Hash	a6df0b49a5ef9ffd6513bfe061fb60f6d2941a440038e2de8a7aeb1914945331	BumbleBee
Hash	de730d969854c3697fd0e0803826b4222f3a14efe47e4c60ed749fff6edce19d	Akira
Hash	ca8646dfc88423bb9fffda811160cebe	BumbleBee

Type	Indicator	Context
Hash	febbaf5f08a8e0782ffcce8beef1f2b4e249a52b	BumbleBee

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:** T1136.002 Domain Account (persistence)
- **Observed here:** the threat actor used T1078.002 Domain Accounts here as an alternative persistence technique.
- **Projected pivot:** T1078.002 Domain Accounts (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The threat actor could pivot to utilizing Domain Accounts (T1078.002) to maintain access and achieve their objectives, potentially by compromising or reusing existing domain account credentials that were not previously blocked. This would likely involve attempting to use these accounts to move laterally within the network or gain elevated privileges. The defender would likely counter this by enforcing the mandated defensive control: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Detection and hardening for the pivot (T1078.002 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