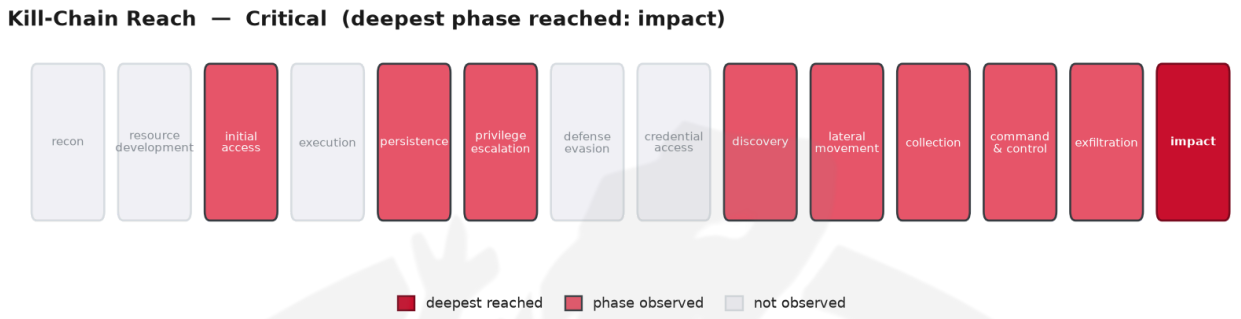
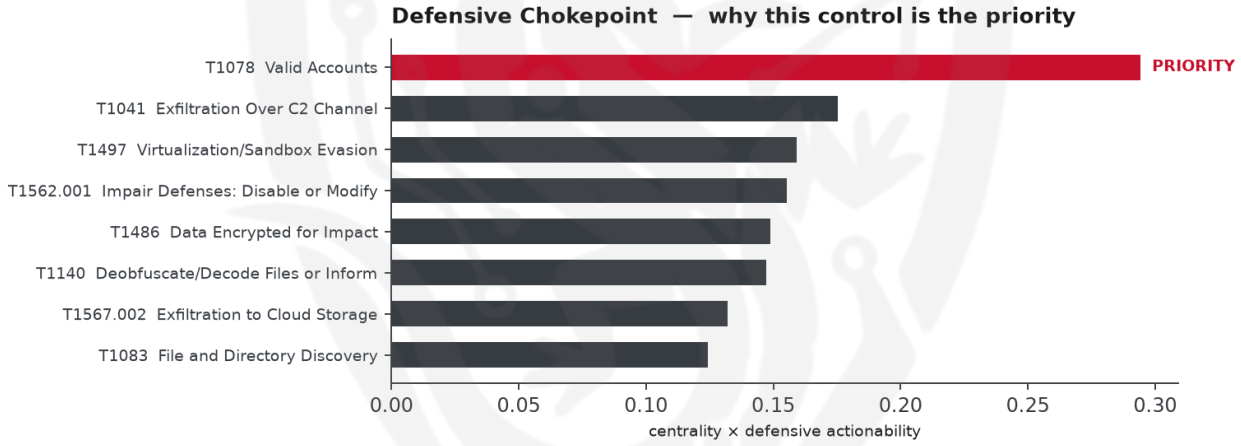
THREAT REPORT: STORM-1567

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 source attributes this activity to Storm-1567, a threat actor utilizing the Akira malware family to target unspecified countries and sectors. The actor's techniques include data exfiltration, system information discovery, and impairment of defenses. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The threat actor's actions pose a critical operational risk due to their potential impact.

Threat Overview

The threat actor, Storm-1567, is associated with the Akira malware family, although the central vulnerability exploited is not specified. The actor's techniques include archive utility, permission group discovery, local data staging, and exfiltration over command and control channels, among others. The victimology of this threat is not well-defined due to insufficient data on targeted countries and sectors.

Attack Chain and Priority Control

The observed techniques employed by Storm-1567 form a complex chain that includes initial system discovery, data staging, and eventual exfiltration. A key technique in this chain is the use of valid accounts (T1078), identified as the priority technique. To counter this, the recommended 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

There is no significant third-party corroboration or infrastructure information available for this threat, as indicated by the lack of hosting providers, corroborated malware families, and high-confidence indicators from sources like AbuseIPDB and abuse.ch.

Technical Appendix

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

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

- T1560.001 Archive via Utility
- T1069 Permission Groups Discovery
- T1074.001 Local Data Staging
- T1087.002 Domain Account
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1083 File and Directory Discovery
- T1497 Virtualization/Sandbox Evasion
- T1041 Exfiltration Over C2 Channel
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1486 Data Encrypted for Impact
- T1567.002 Exfiltration to Cloud Storage
- T1018 Remote System Discovery
- T1105 Ingress Tool Transfer
- T1021.001 Remote Desktop Protocol
- T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2943).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4496; 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
ToddyCat	0.4496
Agrius	0.4282
INC Ransom	0.4022
Akira	0.3917
APT3	0.385

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	131877a052f62750d815cf55d4c14f606a26025e3094e1b8bb18bd1668e3beaa

---

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 only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1190 Exploit Public-Facing Application (initial-access)
- **Basis:** 32 of 170 documented groups that use Valid Accounts also use Exploit Public-Facing Application (conditional 0.50, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

With T1078 Valid Accounts blocked, Storm-1567 could preserve the same objective by pivoting to T1190 Exploit Public-Facing Application, a technique commonly paired with it across tracked groups. Defensive countermeasure: Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

Also plausible (same tactic): T1133 External Remote Services (n=25, lift 2.4), T1199 Trusted Relationship (n=10, lift 2.2)

Detection and hardening for the pivot (T1190 Exploit Public-Facing Application)

- **Telemetry:** WAF / reverse-proxy logs; Web server logs; EDR on the DMZ host
- **Detect:**
  - Exploit strings and anomalous request paths in access logs; 500s spikes
  - The web/app service account spawning shells or network tools
  - Outbound connections from a server that should never initiate them
- **Harden:**
  - Patch internet-facing software fast; virtual-patch at the WAF meanwhile
  - Egress filtering from DMZ hosts; least-privilege service accounts
- **MITRE:** M1051 Update Software, M1050 Exploit Protection, M1016 Vulnerability Scanning, M1030 Network Segmentation · DS0015 Application Log, DS0009 Process, DS0029 Network Traffic