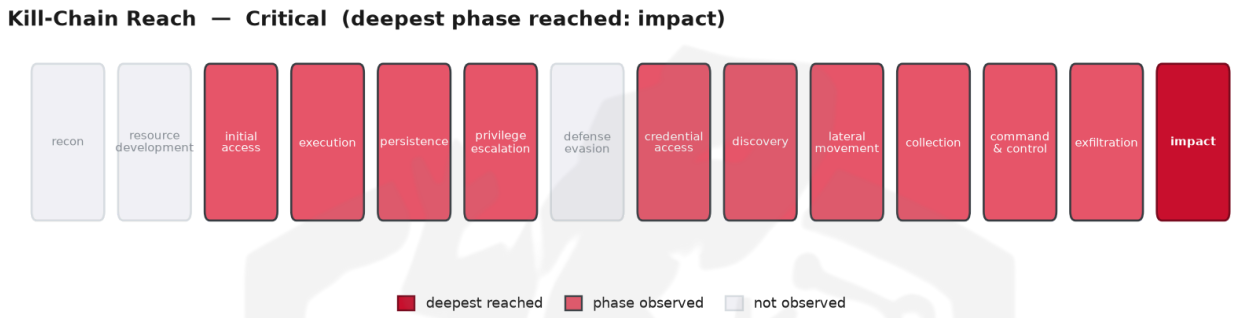
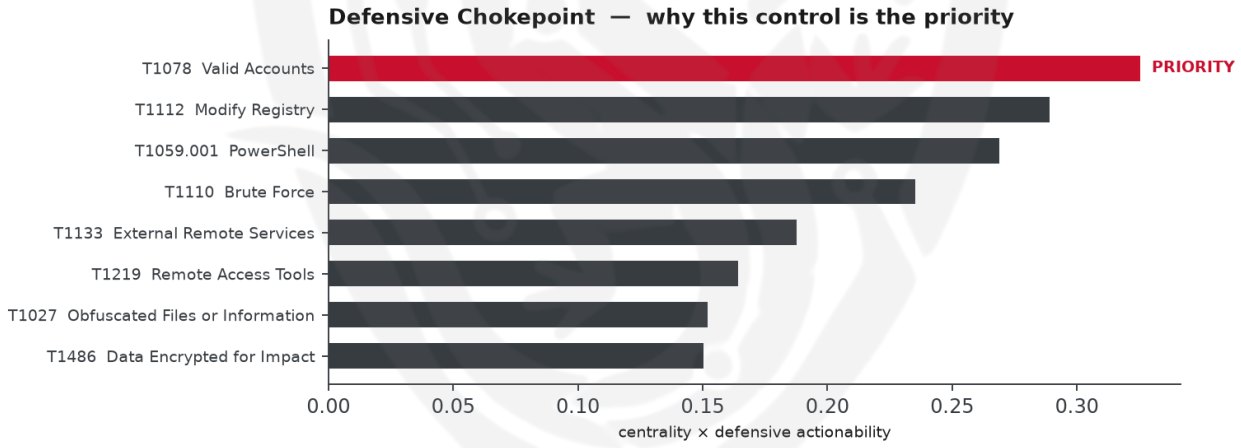
THREAT REPORT: STORM-1567 RANSOMWARE CAMPAIGN

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 source attributes this activity to Storm-1567, a threat actor utilizing Akira and AnyDesk malware families to target unknown sectors and countries. The actor's techniques include exploiting various vulnerabilities and utilizing scheduled tasks, external remote services, and remote access tools. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The threat actor's ability to encrypt data and exfiltrate it to cloud storage poses a significant risk.

Threat Overview

Storm-1567, the observed threat actor, employs Akira and AnyDesk malware families, although the central CVE exploited remains insufficiently documented. The victimology and targeted sectors are also not well-

defined, but the techniques used by the actor include scheduled tasks, archive utilities, and external remote services, indicating a sophisticated approach to gaining and maintaining access.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including scheduled tasks, external remote services, and remote access tools, ultimately leading to data encryption and exfiltration. The priority technique identified is T1078 Valid Accounts, which serves as a critical chokepoint in the attack chain. 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

The malicious infrastructure associated with this campaign is observed to be hosted by Armstrong. However, there are no malware families corroborated by abuse.ch, and no indicators have reached an 80% confidence level on AbuseIPDB, with the highest confidence seen being 0%. This information provides context but does not override the primary threat intelligence provided by the source.

Technical Appendix

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

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

- T1053.005 Scheduled Task
- T1560.001 Archive via Utility
- T1133 External Remote Services
- T1087.002 Domain Account
- T1219 Remote Access Tools
- T1112 Modify Registry
- T1083 File and Directory Discovery
- T1059.001 PowerShell
- T1110 Brute Force
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1567.002 Exfiltration to Cloud Storage
- T1018 Remote System Discovery
- T1021.001 Remote Desktop Protocol
- T1529 System Shutdown/Reboot

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.3254).

- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.6093; 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
Akira	0.6093
ToddyCat	0.4842
Fox Kitten	0.4352
Chimera	0.4238
BlackByte	0.3936

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	Context
IP	72[.]23[.]77[.]35	AbuseIPDB 0% (US) · AS27364 Arm strong
Hash	e2356c742c74cce5c6b6100162d0071a3f71e2fed2ed895c2011061a95b3299a	
Hash	61a1ad1b6a028a1833c85e6544383999	
Hash	bb6f97878c8cbf762d69717b3480658fe9157ff0	
Hash	414b9985f46714f44dd1bd63860d2a48dcfababcfe5c712a4b4f575378127a56	

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.

Storm-1567 could pivot to using Windows Management Instrumentation (T1047) to maintain access and gather information, as this technique may allow them to leverage existing Windows administrative tools and protocols to interact with systems without relying on valid accounts. This technique in particular would likely involve using WMI to execute commands or query system information, which could be a viable alternative to their previously blocked attempts at using valid accounts. To counter this potential pivot, the defensive control of monitoring wmiprvse.exe child-process creation, restricting remote WMI (DCOM) at the host firewall, and enabling WMI-Activity operational logging should be implemented.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1072 Software Deployment Tools (n=6, lift 2.3)

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