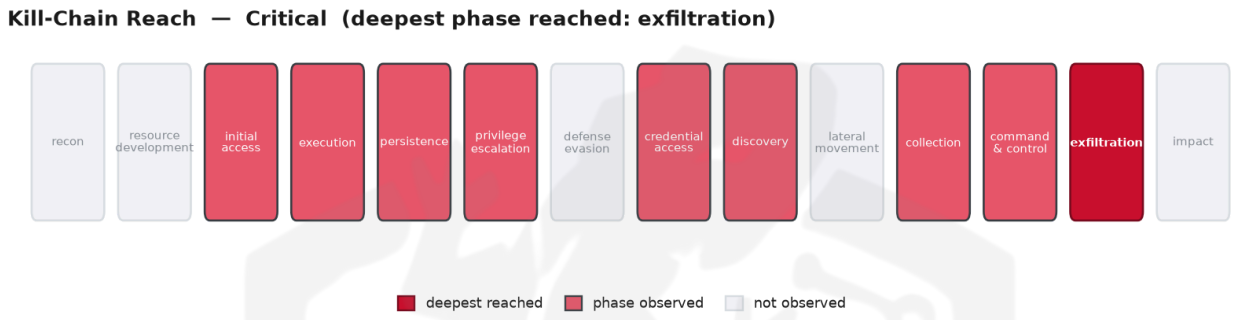
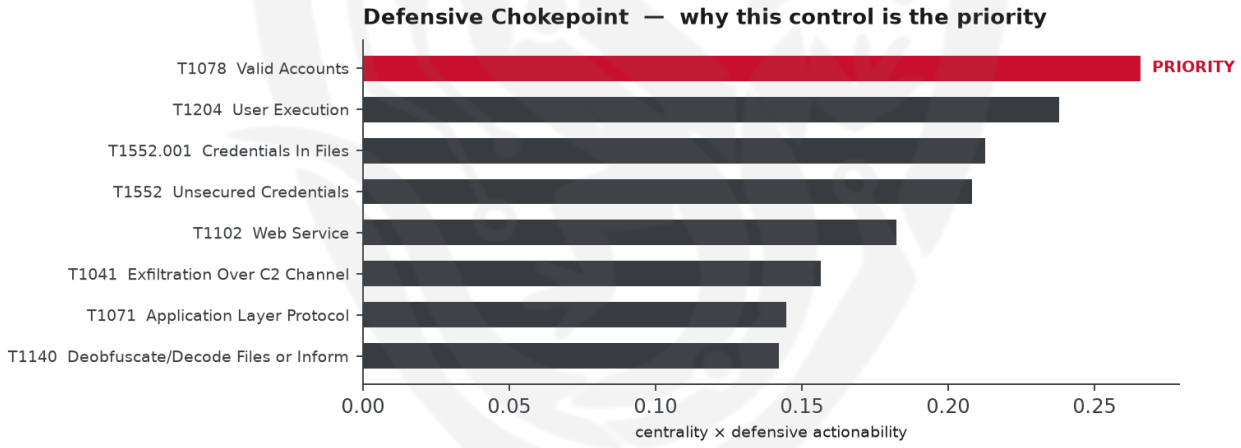
THREAT REPORT: ARMORED LIKHO TARGETS TELEGRAM AND EAVESDROPPING

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 Armored Likho, a threat actor utilizing various malware families, including Still Sync, Still Audio, and AquilaRAT, to target government, IT, education, and technology sectors. The actor's primary objective appears to be eavesdropping and data exfiltration. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The targeted country and central CVE remain unknown due to insufficient data.

Threat Overview

Armored Likho, the attributed threat actor, employs a range of malware families to exploit vulnerabilities and gain access to sensitive information. The malware families used include Still Sync, Still Audio, and

AquilaRAT. The victimology indicates that government, IT, education, and technology sectors are being targeted, although the specific country and central CVE exploited are not known.

Attack Chain and Priority Control

The observed techniques used by Armored Likho form a complex attack chain, involving techniques such as Sharepoint exploitation, audio capture, and system process modification. 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 Armored Likho's activities is hosted by various providers, including Evoxt Sdn. Bhd., Regxa Company for Information Technology Ltd, Informacines Sistemos IR Technologijos UAB, and Namecheap Inc. However, according to abuse.ch, there are no corroborated malware families, and AbuseIPDB has not flagged any 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, expert-tagged by source)

- T1213.002 Sharepoint
- T1123 Audio Capture
- T1543 Create or Modify System Process
- T1564 Hide Artifacts
- T1082 System Information Discovery
- T1071 Application Layer Protocol
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1552 Unsecured Credentials
- T1102 Web Service
- T1552.001 Credentials In Files
- T1204 User Execution
- T1041 Exfiltration Over C2 Channel
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1132 Data Encoding
- T1213 Data from Information Repositories
- T1071.001 Web Protocols

- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2658).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3558; 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
APT19	0.3558
VOID MANTICORE	0.3356
Tropic Trooper	0.3287
RedCurl	0.3175
Rocke	0.3162

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	213[.]252[.]244[.]123	AbuseIPDB 0% (LT) · AS61272 Informacines Sistemos IR Technologijos UAB
IP	159[.]198[.]37[.]74	AbuseIPDB 0% (US) · AS22612 Namecheap Inc.
IP	23[.]26[.]237[.]250	AbuseIPDB 0% (NL) · AS149440 Evoxt Sdn. Bhd.
IP	23[.]27[.]24[.]30	AbuseIPDB 0% (PL) · AS149440 Evoxt Sdn. Bhd.

Type	Indicator	Context
IP	145[.]223[.]69[.]143	AbuseIPDB 0% (FR) · AS215311 Regxa Company for Information Technology Ltd
IP	145[.]223[.]68[.]66	AbuseIPDB 0% (FR) · AS215311 Regxa Company for Information Technology Ltd
URL	hxxps://srwinservice[.]com	
URL	hxxps://tg4service[.]com:443	
Hash	c1d1ee16b92e6a138ffa048855f75d7d	
Hash	17674b250d8b422a50a86c9ff207186d	
Hash	62801f6223e860a7cca271522e303b2d	
Hash	68f0365d2fa8c828d012d8859e52a773	
Hash	4bd7c352ae277b0e38d07beedd4dd507	
Hash	d4bc09fb10ea2a5dc0bcbeeda5e5afdd	
Hash	2ca8adbab98ebe305eacf272cf48f5a0	
Hash	3ac41b097236a7723821848ae31ef141	
Hash	439255736797bc88bd19f282449e0436	
Hash	17b6f4984930165939680a09d91989ad82bc57e2	
Hash	724f6ca2ea66dbf117c7eea42c99760716ec75b9	
Hash	b9258c816724cb074258df485dfbc5b08141cdcb	
Hash	dd1f41f6f8e995fb482070d6689f4238505aac78	

Type	Indicator	Context
Hash	31349d61da780d59a8a27e2762405632726d88135a08ac5dda05849c62dfd551	
Hash	404eb4ada6e161210611f1c8275f126ec24aad37c380ead130cf15667023d249	
Hash	4eb6126f7e23d9155df280b944a98da10a79f1067f39990cf019f25feef75712	
Hash	5fc1251e474eae9253362a08095e989edc2b63de21d76052a2c849efc6792c3f	

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.

Armored Likho could pivot to using T1047 Windows Management Instrumentation to maintain their access and evade detection, as this technique allows them to leverage the existing Windows management infrastructure to execute commands and gather information, potentially bypassing the restrictions imposed by the blocked T1078 Valid Accounts technique. This technique may be particularly appealing to Armored Likho due to its ability to blend in with legitimate administrative activity, making it harder to detect. To counter this potential move, the mandated 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), 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