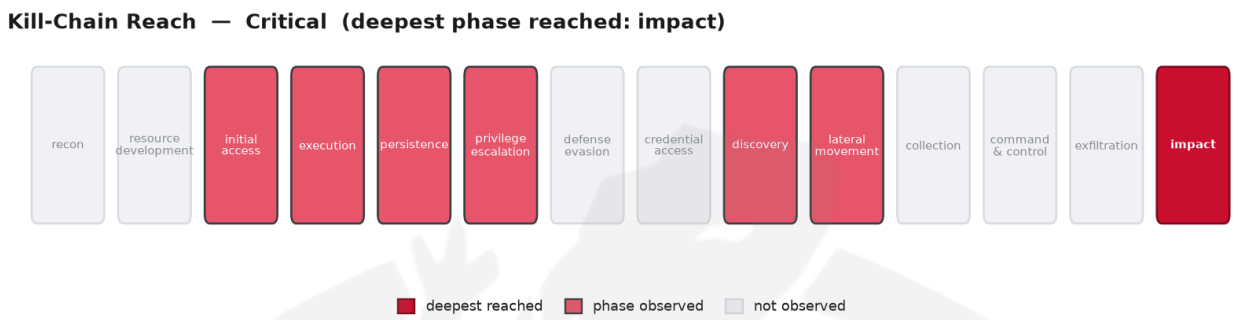
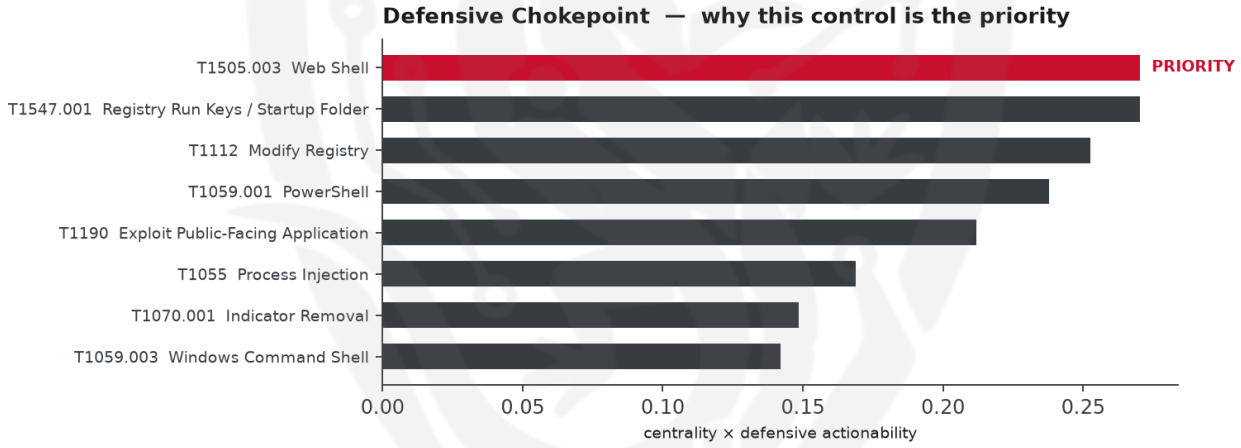
THREAT REPORT: 4BID

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 4BID, a threat actor exploiting the CVE-2023-44976 vulnerability to target various sectors including healthcare, government, manufacturing, and aerospace in countries such as Belarus, Egypt, Kazakhstan, Russian Federation, Syrian Arab Republic, and United Arab Emirates. The actor is utilizing multiple malware families, including BlackReaperRAT, Warp RAT, and Sliver, among others. Priority should be given to patching the exploited vulnerability and monitoring web-server directories for web shells. The threat actor's activities pose a critical operational risk, reaching the impact level.

Threat Overview

4BID, the attributed threat actor, is using a range of malware families including BlackReaperRAT, Warp RAT, Sliver, Havoc, Mythic Apollo, AdaptixC2, BlackSalt, ClearWater, Blackout Locker, GhostDriver, ValleyRAT, and ABCDoor to exploit the CVE-2023-44976 vulnerability. The targeted sectors include

healthcare, government, manufacturing, and aerospace, with a focus on countries in the Middle East and Eastern Europe. The actor's techniques include system owner/user discovery, service stop, and exploit public-facing application, among others.

Attack Chain and Priority Control

The observed techniques used by 4BID form a complex attack chain, involving initial system discovery, service manipulation, and exploitation of public-facing applications. The priority technique identified is T1505.003 Web Shell, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority action is to: Patch CVE-2023-44976 on all affected systems as the top priority, then: Integrity-monitor web-server directories for web shells; restrict server module/plugin installation.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with the malicious activity. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB 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)

- T1033 System Owner/User Discovery
- T1489 Service Stop
- T1543.003 Windows Service
- T1082 System Information Discovery
- T1190 Exploit Public-Facing Application
- T1055 Process Injection
- T1112 Modify Registry
- T1505.003 Web Shell
- T1070.001 Indicator Removal
- T1083 File and Directory Discovery
- T1057 Process Discovery
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1059.003 Windows Command Shell
- T1070.004 File Deletion
- T1021.001 Remote Desktop Protocol
- T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1505.003 Web Shell (centrality 0.2846).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4951; 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
FIN10	0.4951
BlackByte	0.4774
Medusa Group	0.4734
Tropic Trooper	0.4364
APT18	0.433

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	008cd423ca45134d3343f66cced1d104
Hash	038cab0c60c53cf12f048272014024c0
Hash	06bed0a0906e52c764b3b7016d6a4428
Hash	08c069f133ac27cbc02a0ed79e4e87ba
Hash	09d0517a1f69feff8186655ae3b567e0
Hash	0b1870d57221eec6f3bbef648e71a724

Type	Indicator
Hash	0c32bfdf83ecebe3a1399d261dc8ff57
Hash	10824d14c814524155f2b529cf5fee43
Hash	129225b3e93c17f131bcc2a982ffb09a
Hash	1344e6bc51cea35befb4adff7a25899b
Hash	1742a9fa35e253614b76ac0f687ba02e
Hash	1c0924f5711a24821921de5ad822213b
Hash	1d09499cb2d7d70df903b60602a58887
Hash	1e1edf879b2dc6c9892a22bfa5985db1
Hash	1ff222457f5e0e32adfa8341f260dde7
Hash	242038139842ec79ec1044c64eb0804a
Hash	26100db3f56880110a92a2b4742d6eaf
Hash	2d5533fb65ebb50a5a5fd53e62d73b9a
Hash	2db94ee3ec69988588702bd77999a5d4
Hash	2f40bcee90abed0898e92521da17e52d
Hash	36b3be503c6e34613ff50cb28e0f3ddb
Hash	389a1bbdbf5c91bd1c179227f5ae0923
Hash	3a9b0875fc692944c180b165a83a0d17
Hash	3b974ff986445e5944c51179d19bd6be
Hash	3d9cbc944f9a9e127550ffb4e8394965
Hash	3ee38b944e5c83922f99641846f7db0c
Hash	4c8a0531653b5398a35c6b1b80ff1350
Hash	5398b7eaa94f0ee570b1c5642b559047
Hash	53ba13cc6066adfd67f8098c0a5b8dde
Hash	54a308f734095d54ae0e1c86c849a2d8
Hash	555a6722436d7cf7de396e0c57d32a27

Type	Indicator
Hash	56be07e46fd452315008ed246ebbf52b
Hash	56d1de3159adbfda20aca593c99901f9
Hash	579e8bbd6a5bcca89b5acd6fb5db32db
Hash	5e81f72614db42615489266be11b1d09
Hash	60f8b115aec8a13b0069efc84fc645f5
Hash	61647db645f7cc221046999ef1dbe1d1
Hash	62123c39477389d500e74e82782adea5
Hash	68e310de44c3165ffffa25bc495d6fc5
Hash	6cf548445c39aff844be96d73c89e376