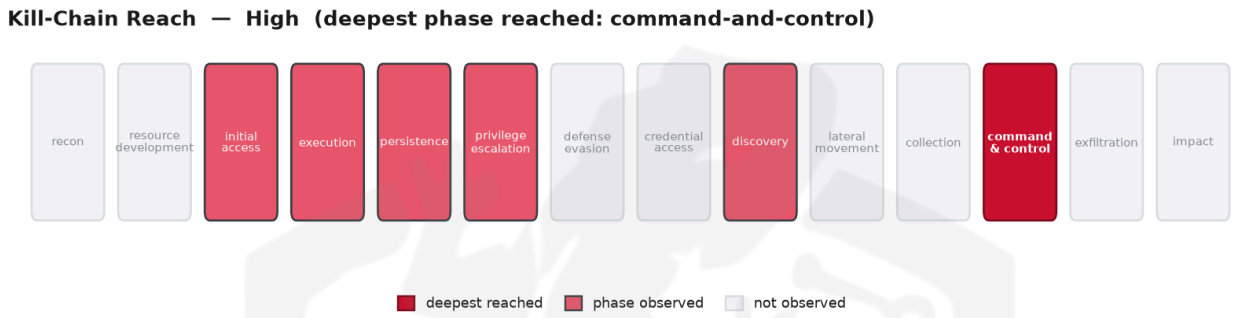
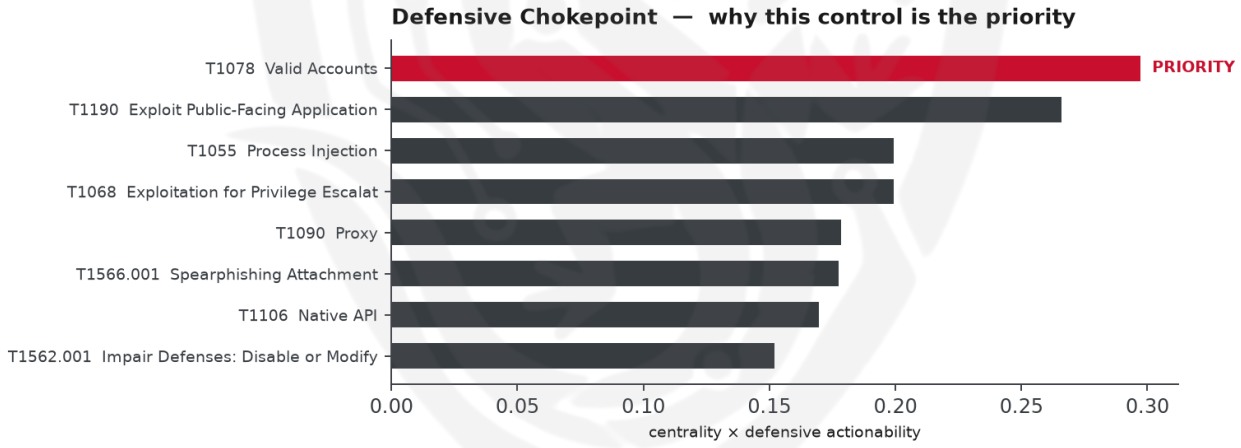
THREAT REPORT: LAZARUS USES FAKE JOB OFFERS TO DELIVER NEW ZERO DAY EXPLOIT

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 Lazarus, a threat actor that has been using fake job offers to deliver a new zero-day exploit, specifically CVE-2025-49113, to targets in various countries including Brazil, France, Germany, and India. The targeted sectors include Defense, Aerospace, and Aviation. Priority should be given to enforcing multi-factor authentication and patching the exploited vulnerability to prevent further attacks. The threat actor's use of valid accounts as a priority technique highlights the importance of account security.

Threat Overview

Lazarus, the attributed threat actor, has been observed using malware families such as MISTPEN, ForestTiger, and Olympic Destroyer to exploit the CVE-2025-49113 vulnerability. The victimology suggests

that the threat actor is targeting organizations in the Defense, Aerospace, and Aviation sectors in multiple countries. The exploited vulnerability and malware families indicate a sophisticated attack chain.

Attack Chain and Priority Control

The observed techniques used by Lazarus form a complex attack chain, including spearphishing, malicious file execution, and exploitation of public-facing applications. The priority technique, T1078 Valid Accounts, is the graph chokepoint, indicating that the threat actor is relying on compromised accounts to gain access to targeted systems. The priority control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons. In parallel, patch CVE-2025-49113 on all affected systems.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this activity. Additionally, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB, with the highest confidence seen being 0%. This lack of corroboration highlights the need to rely on the source pulse for threat intelligence.

Technical Appendix

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

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

- T1014 Rootkit
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1055 Process Injection
- T1090 Proxy
- T1083 File and Directory Discovery
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1068 Exploitation for Privilege Escalation
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1102.002 Bidirectional Communication
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow

- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2973).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4637; 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
Tropic Trooper	0.4637
Rancor	0.4593
FIN4	0.4564
APT37	0.4518
Higaisa	0.4463

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
Domain	enveil[.]online
Domain	envell[.]xyz
Domain	uxtramine[.]org
Hash	13d10bc99f7f7abe7ee0902be87920b73b2ea41bd9683dbfcad340dacbcdef79
Hash	1de949c71efcfb0ffc41f33d38833dbc4b082075b1a540fc68c18c535d7ad86c

Type	Indicator
Hash	21c3ad4838c4324bc5f081021da5fb2e9073d0c9304087811c21eb47c9e22762
Hash	231b1ef8b95bf77887d5377e2a60f649035e78f543af1b82877db36a5759d858
Hash	29e24c007549e51319ff3aee011da6f9f93568e8c85a5ad69c9e53bd3f4533a2
Hash	2b4987c07a3d9a9a5d1a9bf4efa3d1903e775090b611710edafdc92874265ca8
Hash	2db25ac41a66aa523c79e23e00443573530dd7bd82b8371bcc87bd7232e141eb
Hash	3601060c62edeeaa49def6a13be6e126e1024ce011faad4e2d9f585ccf6bd5a6
Hash	396192d92d17ace1a521f1351eeeba2825e60badd0d799cc5c338e4934b3c82c
Hash	3a02d0d798e8d35555776886d92b20ff38a101c9ef7e0eebc8ce5d259516525a
Hash	3b6378df8442e63a6ed7317075913e4720847a510d95022d4a8347b2637c245d
Hash	4c9b804d6155b29f1e27a9ffe531e10bc42a7bdab42f905b50146bf2026768d9
Hash	4dd792c9f672bbdcc8d363d745994efe90f4ffc5fdc2c059c8e379a48ad6a68a
Hash	4ebdce2f47c23ff8c9e8e80c8b5239c7a5764da31cd3ab8f0505926890adc105
Hash	4fd32432341dfcf54d0517a6bbc38e5d265be70933493e4183c2a340cdde9a2d
Hash	5278ee922838352f1480a73e971161017d643a80b7ec22bf725897dfd088696d
Hash	590fb6ae19480d694e08ee85859cad8066f2f87e7e5abba2960c6d115e1615d6
Hash	68d4fba7b1300a59cd6212c08910a260cd71b40cd9f51cac933030a68faac0bb
Hash	6da9b1e6f3315ceb77dd14a937a26cc3602bf6a7e2c2ecafb3c65ce5319837be
Hash	72dccae85e062f541fecad9ec7a18a3123e7ae5ac5d53c91709b53a46dbbd289
Hash	743172aab606974b054a64561534ae66baa3a840657f79d7c6fa18350e8d45d1
Hash	75b93a7103b0562f6497d30052c0c5cf7aa58c1bf0e9297022b74469a7f096f1
Hash	82268052f94df6f4870d02e57b18d4c54136cc7a8c8d80ad162631f99462c943
Hash	8ce6c29f92dc45b1474417cbdff4ed0c18e58fa63e3a071ee9f85aa9d2aac07c
Hash	92106b0c62a0a42678232f8273f030b2d3c8e92efce81b98b9eec70cfe98afa1
Hash	a0578a2b7821d7e2c573530648f26d7a0d98b373ab24fb7f0c792736761e542d
Hash	a45144d22cac70a45d71cf4dffa4efbc373658779a56cf1300d6ac863d6cc7e2

Type	Indicator
Hash	a673ae661593c0de9bbb815593b816a6853dad6d55ad5042d2ef1875cd13d6e7
Hash	a738059ce07c951c31ab2da3d93d8f69bff32f9b7d933dbf5943441b9cc99075
Hash	acb97cec84e08b89f41967a24e965d1fd2c51751cef158f7aa35bb4306b87b97
Hash	b4082d21070d9ddf53fde4ea22524d09e41ec9826ce63cef3c6235e458d21afb
Hash	ba96c603e44046de703c67b2c3b7e4ca974afef7b437a0244418bc4edc781bb7
Hash	c2aa28bb5e2a749c693712008276f311edd912f689371ef9e8a1ee5fb4167461
Hash	cc4e06aa378a190f71384c03023bb3d18a6d66e297d46701220e132963d2e222
Hash	d578c28c9afe7457a0d81f6701332ef8197e8f7468de654935fb29a50ea66459
Hash	db3d69b7eeda2e35e23006bf4b7e206281fce809584207214fc213f9bc30376d
Hash	ea7056f2bf36c66a61ff787ff5be975a85f534c3c5ca178791dac2504db2c619

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 here; the pivot escalates to execution, drawn from Lazarus's own documented ATT&CK repertoire.
- **Projected pivot:** T1047 Windows Management Instrumentation (execution)
- **Basis:** documented in Lazarus's own ATT&CK repertoire, and disproportionately paired with Valid Accounts across tracked groups (lift 1.8, ~1.8x base rate). Their move, not a generic one.

Lazarus could pivot to T1047 Windows Management Instrumentation to maintain their access and evade detection, as this technique would allow them to leverage the existing Windows Management Instrumentation (WMI) infrastructure to execute commands and gather information without relying on compromised credentials. By using WMI, Lazarus may attempt to create new processes or interact with the system in a way that blends in with legitimate administrative activity, making it harder to detect. To counter this, 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): T1053 Scheduled Task/Job (n=31, lift 1.4), T1203 Exploitation for Client Execution (n=17, lift 1.1)

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