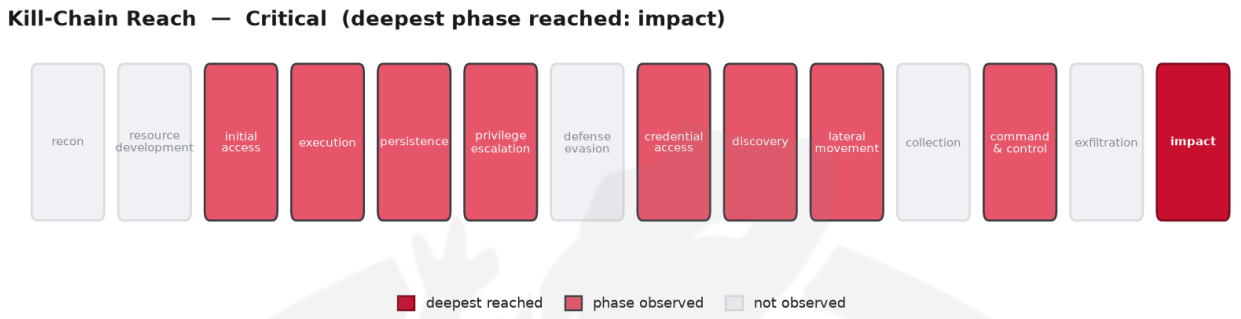
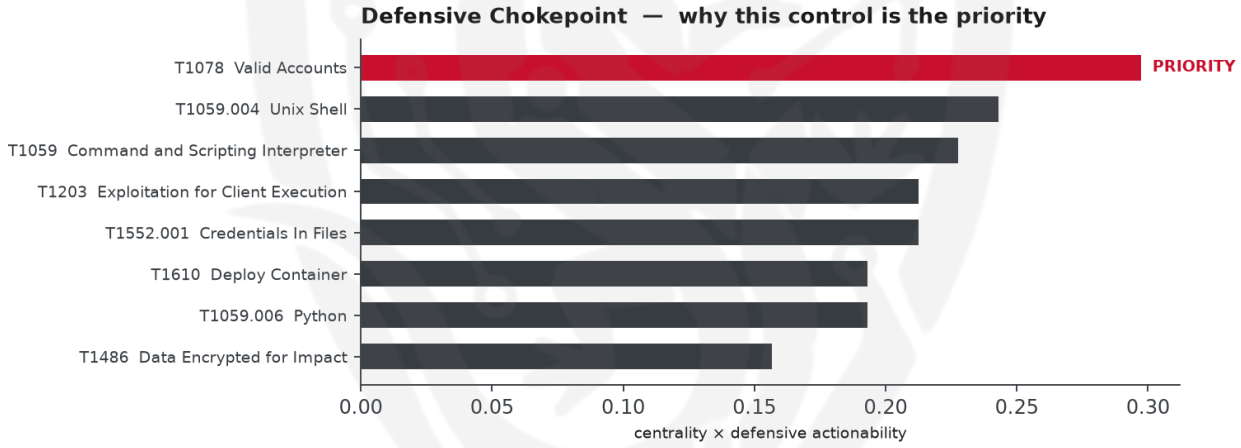
THREAT REPORT: JADEPUFFER

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 JADEPUFFER, a threat actor that has been observed deploying ENCFORGE ransomware, which is designed to destroy AI models, targeting the technology sector. The actor exploits CVE-2025-3248, a critical vulnerability that allows for significant impact. Priority should be given to patching this vulnerability on all affected systems to prevent further exploitation. The threat actor's use of valid accounts is a key technique in their attack chain, highlighting the need for robust account management and monitoring.

Threat Overview

JADEPUFFER, the observed threat actor, utilizes the ENCFORGE malware family to exploit the CVE-2025-3248 vulnerability, primarily targeting the technology sector. The actor's goal is to destroy AI models, and their tactics involve a range of techniques, including service stop, exploit public-facing application, and

remote access tools. The victimology is focused on the technology sector, although the specific targeted country is not specified due to insufficient data.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including stopping services, exploiting public-facing applications, and using remote access tools. The priority technique is T1078 Valid Accounts, which is a critical component of the actor's attack chain. To mitigate this threat, the priority control is to: Patch CVE-2025-3248 on all affected systems as the top priority, then: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

The malicious infrastructure is hosted on Dominic Scholz Trading As ITP-Solutions GmbH & Co. Kg, according to third-party observations. AbuseIPDB flags some indicators with a low confidence level, with the highest confidence seen being 14%, but no malware families have been corroborated by abuse.ch. These findings are based on third-party enrichment and do not override the source pulse.

Technical Appendix

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

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

- T1489 Service Stop
- T1190 Exploit Public-Facing Application
- T1219 Remote Access Tools
- T1611 Escape to Host
- T1021 Remote Services
- T1610 Deploy Container
- T1087 Account Discovery
- T1059 Command and Scripting Interpreter
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1059.004 Unix Shell
- T1078 Valid Accounts
- T1486 Data Encrypted for Impact
- T1203 Exploitation for Client Execution
- T1059.006 Python
- T1485 Data Destruction
- T1070.004 File Deletion
- T1046 Network Service Discovery
- T1490 Inhibit System Recovery
- T1552.007 Container API

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2973).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3742; 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
INC Ransom	0.3742
Medusa Group	0.3133
TeamTNT	0.3024
BlackByte	0.2955
Sandworm Team	0.2926

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 14%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	45[.]131[.]66[.]106	AbuseIPDB 14% (DE) · AS213250 Dominic Scholz Trading As ITP-Solutions GmbH & Co. Kg
Hash	8cb0c223b018cecef1d990ec81c67b826eb3c30d54f06193cf69969e9a8baea2	
Hash	ab9824b61587c77a8d8649545cdbdc63ed2c384e45c9aba534e3f457f96efa7a	
Hash	ea7822eac6cecef7746c606b862b4d3034856caf754c4cf69533662637905328	

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:** JADEPUFFER used T1190 Exploit Public-Facing Application here as an alternative initial-access technique.
- **Projected pivot:** T1190 Exploit Public-Facing Application (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

JADEPUFFER could pivot to exploiting a public-facing application, as seen in T1190, by identifying vulnerable services or software that may not have been properly updated or secured, which may allow them to maintain their objective despite the block on valid accounts. This exploitation could be particularly effective if the targeted application has a known vulnerability that JADEPUFFER can leverage. To counter this potential move, the mandated defensive control is to patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

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