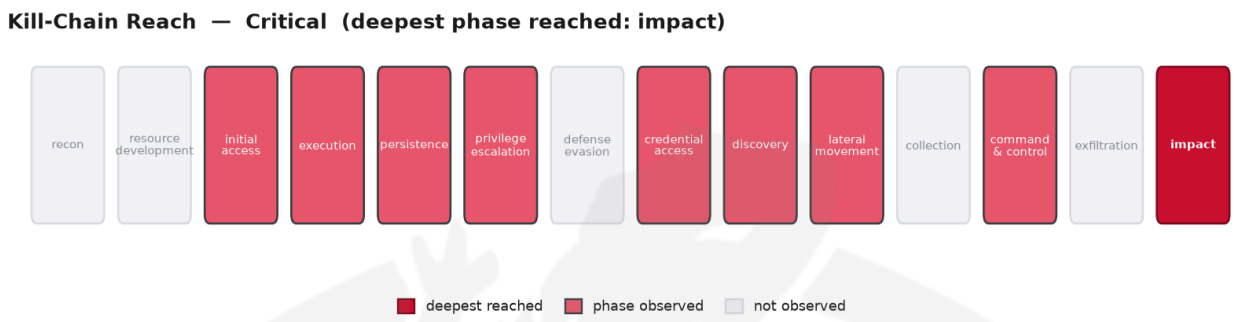
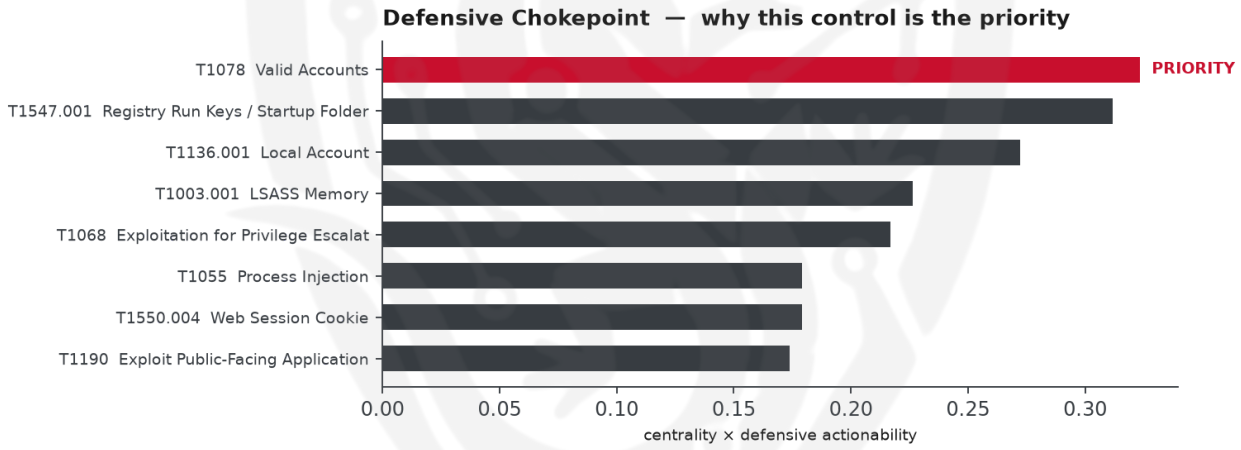
THREAT REPORT: DRAGONFORCE

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 DragonForce, a threat actor exploiting the CVE-2025-5777 vulnerability to deploy DragonForce ransomware. The targeted country and sectors are not specified due to insufficient data. Priority should be given to patching the CVE-2025-5777 vulnerability on all affected systems to prevent further exploitation. The threat actor utilizes various techniques, including valid accounts and process injection, to gain access and encrypt data.

Threat Overview

The threat actor, DragonForce, is associated with the malware families DragonForce, Mimikatz, and Impacket. The central vulnerability exploited is CVE-2025-5777, which is used to gain access to systems and deploy ransomware. The victimology is not well-defined due to insufficient data on targeted countries and sectors.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving system information discovery, exploit of public-facing applications, and remote access tools. The priority technique is T1078 Valid Accounts, which serves as a chokepoint in the attack chain. To mitigate this threat, the recommended priority control is to: Patch CVE-2025-5777 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

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 a confidence level of 80% or higher by AbuseIPDB, 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)

- T1543.003 Windows Service
- T1082 System Information Discovery
- T1190 Exploit Public-Facing Application
- T1219 Remote Access Tools
- T1055 Process Injection
- T1136.001 Local Account
- T1070.001 Indicator Removal
- T1003.001 LSASS Memory
- T1547.001 Registry Run Keys / Startup Folder
- T1078 Valid Accounts
- T1068 Exploitation for Privilege Escalation
- T1486 Data Encrypted for Impact
- T1550.004 Web Session Cookie
- T1059.003 Windows Command Shell
- T1018 Remote System Discovery
- T1021.001 Remote Desktop Protocol
- T1569.002 Service Execution

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.3235).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.517; 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
BlackByte	0.517
Silence	0.427
Wizard Spider	0.417
APT41	0.4103
Blue Mockingbird	0.4057

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	doauthentication[.]do
Domain	vpts[.]us
Domain	opa[.]tlsd[.]shop
Domain	relay[.]dltsolutions[.]top
Domain	relay[.]eurofin[.]digital
URL	hxxp://relay[.]eurofin[.]digital:8041
Hash	c4fcae3847946173bf0b3cedf5d97a9e3d18090023842f942ba544fa7fda180d
Hash	c84739655ce1af0a0269138263d47567418f69e0f75e249f8e23bc21802209e2
Hash	eb083365dc70d0294e8c4f55a2e78be0edb0f3497f2a06a70c9f474dafab48d8