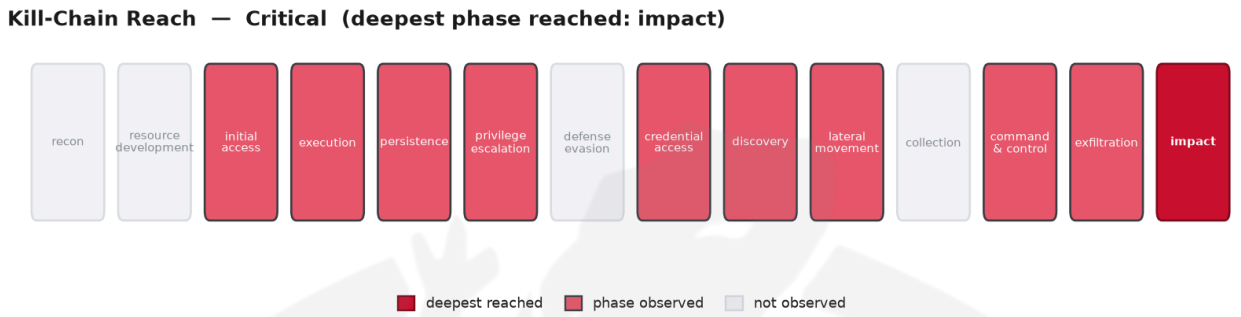
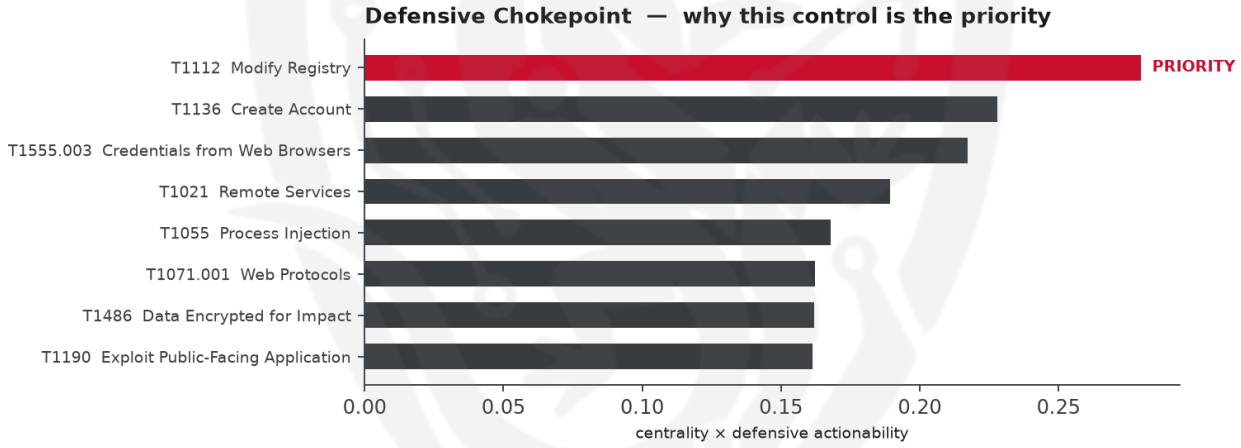
THREAT REPORT: DRAGONFORCE

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 that has been exploiting CVE-2023-52271 to target organizations in the United States of America. The actor utilizes various malware families, including Backdoor.Turn and DragonForce, to gain unauthorized access and exfiltrate sensitive data. Priority should be given to patching the exploited vulnerability and monitoring sensitive registry keys for modification. The threat actor's ability to stay hidden by weaponizing Microsoft Teams relays poses a significant risk to affected organizations.

Threat Overview

DragonForce, the observed threat actor, employs the Backdoor.Turn and DragonForce malware families to exploit the CVE-2023-52271 vulnerability, primarily targeting organizations in the United States of America. The actor's tactics involve a range of techniques, including OS credential dumping, domain

account manipulation, and exfiltration over web services. The victimology of this campaign is focused on exploiting public-facing applications and impairing defenses to maintain access and evade detection.

Attack Chain and Priority Control

The observed attack chain involves a series of techniques, including exploit public-facing application, process injection, and modify registry. The priority technique is T1112 Modify Registry, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the recommended priority control is to: Patch CVE-2023-52271 on all affected systems as the top priority, then: Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users.

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted on Data Campus Limited. Additionally, abuse.ch has corroborated the presence of the WikiLoader malware family, which is linked to this activity. However, according to AbuseIPDB, there are no 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)

- T1003 OS Credential Dumping
- T1087.002 Domain Account
- T1190 Exploit Public-Facing Application
- T1567 Exfiltration Over Web Service
- T1055 Process Injection
- T1021 Remote Services
- T1112 Modify Registry
- T1555.003 Credentials from Web Browsers
- T1562.006 Impair Defenses: Indicator Blocking
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1071.001 Web Protocols
- T1136 Create Account
- T1018 Remote System Discovery
- T1574.002 Hijack Execution Flow
- T1569.002 Service Execution
- T1090.001 Internal Proxy

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2943).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4029; 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	0.4029
APT41	0.3866
Medusa Group	0.3615
Wizard Spider	0.3413
APT39	0.3343

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: WikiLoader.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	62[.]164[.]177[.]25	AbuseIPDB 0% (NL) · AS215929 Data Campus Limited
Domain	comunidadesparentais[.]com[.]br	
Domain	glanz-gmbh[.]de	
Domain	mysimerp[.]net	

Type	Indicator	Context
Domain	professionalhomebasedbusiness[.]com	
Domain	projetosmecanicos[.]com[.]br	
Domain	safefire[.]jo	
Domain	socialbizsolutions[.]com	
Domain	turnkeyaiagents[.]com	
URL	hxxp://192[.]36[.]27[.]51/TechSupV18Fix3[.]zip	
Hash	8a4033425d36cd99fe23e6faef9764fbf555f362ebdb5b72379342fbbe4c5531	
Hash	ecb1d69999a730760b3c5654920f0ef6	
Hash	b4ddb0adf94e28b53e392900c5ff2f538616441b	
Hash	048e18416177de2ead251abdf4d89837f6807c6aba4d5b1debe49adfdecbf05c	
Hash	65ab49119c845801f29a57e8aa177146b2ffbd289d4278109b146f933380f951	
Hash	6bbf10bcbef7ac5102b54c81137859891a3802dbacd888be90f990d50e18b0b4	
Hash	6f9fbe29f8cc2788e2bc9d631e0eea2a8e9837076837b55838005a0e654f0a9e	
Hash	821da79d727351dd67ce5df7950e9a3de6647a3cf474bb3a093f67507fed92a6	
Hash	8284c8676cc22c4b2e66826ac16986da7ddecba1f2776b16771be17bfdc45dc2	
Hash	82b37a92589dfd4d67ca87eb9e52ac8e682e8e60d2211f59074cd5ccc693013b	
Hash	9335f61f8ad276d94455c5b6876fea48152c3cea759f2598c8108ee461fa5759	

Type	Indicator	Context
Hash	aea26980059ef2ad11e99556a4edfa1f8ec769fa9f06aa573b81bedf319954b5	
Hash	cd078957167e1af4de39aecdb981cd14156fa81d5a9c6ac51e74ae5b6199a12a	WikiLoader
Hash	ce66b8221446c9b6d83f0ce6382f430e519601641e5daaaf1ca7a8a8806cb0b0	
Hash	d0da2832ae1e13a98f7ce7e33a66c1b0d9797b81f69ece134e4462ea55ac923e	
Hash	d20a3c928761fe00ac522eeb474612b5804cd9108453ea8591106d5d4428428e	
Hash	e45b18c93d187aac5c4486f57483bc87580e15def82a312bfb377ff16eb96b22	
Hash	f174c19902523dcf005fa044b6598403a5e5c0a5982398d1bc0dcc5ec1cd351b	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.