

FULCRUMSEC

Financially motivated data-extortion group active since September 2025, breaching cloud environments through exposed credentials and API keys. Uses AI to mine stolen data for leverage, with no ransomware or encryption involved.

The Threat Thespians No encryption used Cloud-native extortion

RISK RATING
High

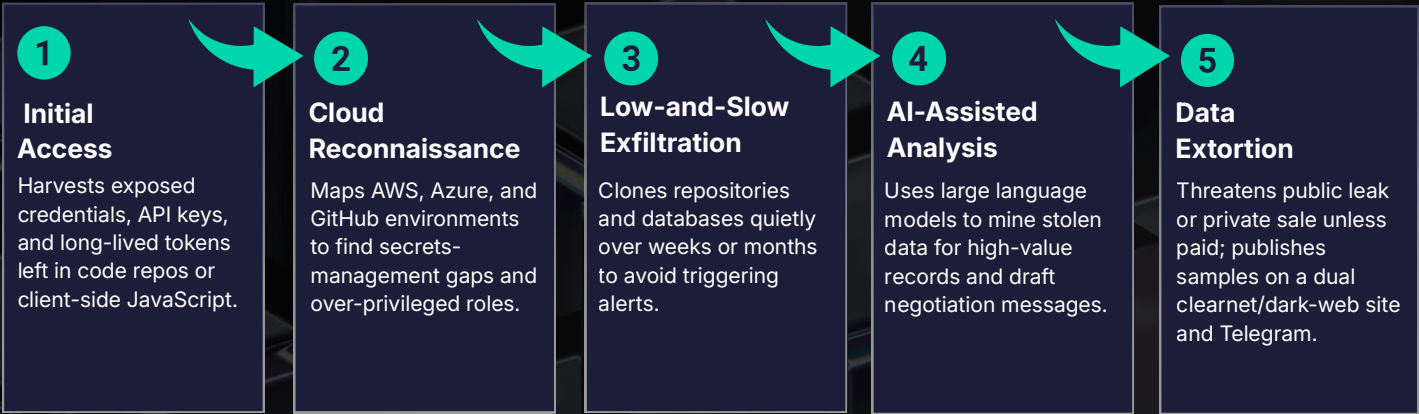
ACTIVE SINCE
2025

MOTIVATION
Data extortion only, no ransomware

PRIMARY VECTOR
Exposed cloud credentials, API keys, tokens

CLAIMED VICTIMS
25+ across 11 countries

ATTACK CHAIN



MITRE ATT&CK MAPPING

ID	TECHNIQUE
T1552.001	Credentials in files (exposed API keys/tokens in code)
T1078.004	Valid cloud accounts (over-privileged IAM roles)
T1213	Data from information repositories (source code, wikis)
T1530	Data from cloud storage (S3, Azure Blob, Redshift)
T1567.002	Exfiltration to cloud storage
T1591	Gather victim org information (AI-assisted data mining for leverage)

SECTOR BY SECTOR Summary



Technology & Business Services

Its most consistent hunting ground, where cloud misconfigurations are common and credential debt runs high.



Healthcare & Pharmaceuticals

Its highest-profile hit to date, targeting proprietary drug data and AI models rather than patient records for leverage.



Legal & Professional Services

Exploited weak cloud hygiene at a major legal data provider, exposing records tied to government and judicial staff.

ORIGIN & EVOLUTION

Active since September 2025 and compared by researchers to LAPSUS\$ and Karakurt for its pure data-extortion style, with no ransomware or encryption involved at any point. Also known as The Threat Thespians, it has claimed roughly 25 victims across 11 countries, reading more like target-of-opportunity credential hunting than a sector focus.

THREAT LANDSCAPE CONTEXT

Operates with no ransomware ties at all, closer in structure to LAPSUS\$ and Karakurt than to any RaaS operation. Its victim list spans pharma, legal, and aviation with no consistent sector thread, suggesting opportunistic credential hunting rather than a targeted campaign.

SIGNATURE TRADecraft

Harvests exposed credentials, API keys, and long-lived tokens left in code repositories or client-side JavaScript, then clones data quietly over weeks to avoid triggering alerts. Its defining trait is using large language models to mine the stolen data for high-value records and draft negotiation messages, then choosing between a private sale or a public leak-site posting depending on which nets more value.

ANALYST OUTLOOK

FulcrumSec's zero-malware model makes it resistant to traditional EDR and antivirus defenses entirely, since there's no executable to detect. Expect its victim list to keep growing wherever secrets management and IAM hygiene lag behind cloud adoption.

NOTABLE INCIDENTS

Novo Nordisk

2026

Claimed roughly 1.3TB of stolen data including drug IP, AI models, and clinical trial records, demanding \$25M after harvesting an exposed GitHub token from client-side JavaScript.

LexisNexis

Exploited a React2Shell vulnerability to breach the legal data provider, exposing records tied to government and judicial staff.

Manchester Airports Group

Breached the aviation group through cloud credential exposure, extending the group's reach beyond its initial pharmaceutical and legal targets.