

Scattered Spider

Financially motivated eCrime collective, active since 2022. Specialises in help-desk social engineering to take over enterprise identity and cloud environments, then extorts victims via data theft and, increasingly, ransomware.

UNC3944

Octo Tempest

Muddled Libra

Scatter Swine

Oktapus

Storm-0971

Starfraud

RISK RATING

Critical

ACTIVE SINCE

2022

MOTIVATION

Financial extortion

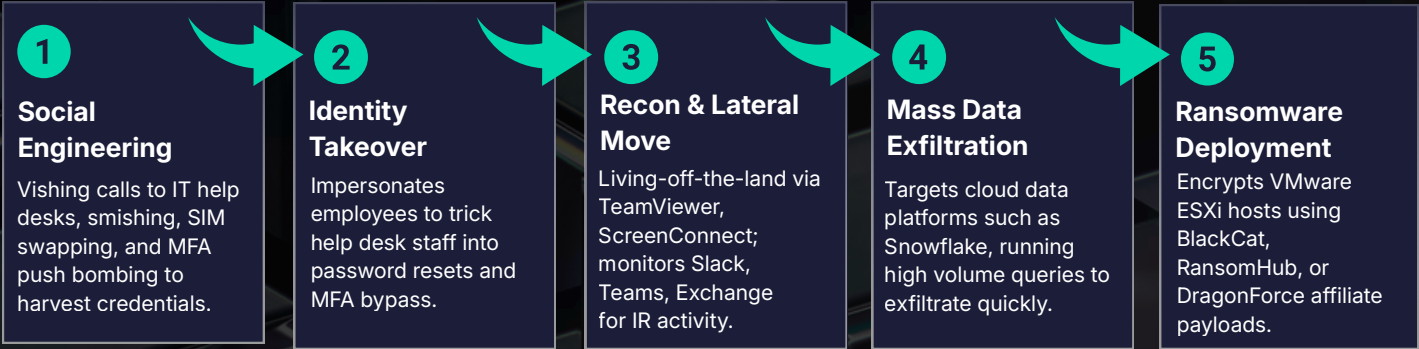
PRIMARY VECTOR

Help desk social engineering

RANSOMWARE TIES

BlackCat, RansomHub, DragonForce

ATTACK CHAIN



MITRE ATT&CK MAPPING

ID	TECHNIQUE
T1566	Phishing (email & SMS/smishing)
T1621	MFA request generation (push bombing)
T1111	Hardware token/SIM swap MFA interception
T1567	Exfiltration over web service (Snowflake & cloud)
T1486	Data encrypted for impact (VMware ESXi)
T1114	Email collection to monitor IR response

SECTOR BY SECTOR Summary



Retail

Breached major UK retailers by tricking help desk staff into resetting passwords, no malware required.



Insurance

Pivoted to US insurers using the same help desk playbook, knocking several carriers offline.



Transport

Moved into airlines through third-party IT contractors, hitting carriers on two continents.

ORIGIN & EVOLUTION

Emerged in 2022 as a loose, English-speaking collective with overlapping LAPSUS\$ membership, cutting its teeth on SIM-swapping and tech intrusions against Twilio, Cloudflare, and Okta. Gained global notoriety in September 2023 after parallel attacks on MGM Resorts and Caesars Entertainment, the incident that led CrowdStrike to coin its name. Despite steady arrests since 2024, it operates as a decentralized, revolving collective: new members replace jailed ones, and the tradecraft persists industry-wide.

SIGNATURE TRADECRAFT

The group's core weapon is the phone call, not malware. Help desk vishing and SIM swapping get initial access; MFA push bombing and password resets do the rest. Once inside, it lives off legitimate tools like TeamViewer, ScreenConnect, and AnyDesk, moves through Okta and Active Directory, then exfiltrates at scale through cloud platforms such as Snowflake before handing off to its ransomware partner of the moment.

THREAT LANDSCAPE CONTEXT

Scattered Spider shares members with LAPSUS\$, the group behind its earliest SIM-swapping and tech-company intrusions. Since 2023 it has cycled through three ransomware-as-a-service platforms as an affiliate: first ALPHV/BlackCat, then RansomHub, now DragonForce, switching each time a platform collapsed or offered a better split. The pattern shows a collective that outsources encryption entirely and stays loyal only to whichever brand pays best.

ANALYST OUTLOOK

Four years of arrests have not stopped this group, because vishing and help desk social engineering need no malware and no infrastructure of their own. Expect the tradecraft to keep resurfacing under new names even as individual members are jailed.

NOTABLE INCIDENTS

Qantas

June to July 2025

Vished an offshore, third-party contact centre rather than Qantas itself, bypassing MFA to reach around 6M customer records. Core systems and payment data were never touched.

Marks & Spencer

April 2025

Talked the service desk into a password reset, pulled the domain's credential file, then encrypted the estate: the first hit of its kind on an FTSE 100 firm. 46 days of online outage, a £300M profit hit.

MGM Resorts

September 2023

Vished the help desk using LinkedIn-sourced employee details, then deployed ransomware. MGM refused to pay: a 10-day shutdown and over \$100M in lost EBITDA.