SCATTERED SPIDER

[/ ˈskæt.ərd ˈspaɪ.dər /]

Scattered Spider began with phishing and SIM swapping (2022), partnered with ALPHV/BlackCat then RansomHub, and by 2025 was deploying DragonForce ransomware on virtualized environments using fake SSO portals, dynamic DNS, and short-lived phishing kits.

IDENTITY

Attribution	: Cybercriminal collective of English-speaking actors (U.S., U.K., Canada, Europe), linked to underground network "The Community / The Comm."
Active Since	: At least 2022.
Aliases	: UNC3944, Octo Tempest, Oktapus, Muddled Libra, Scatter Swine.
Motivation	: Financially driven – extortion, ransomware, SIM swapping, credential theft, and fraud.

TTPs

Initial Access

- **Phishing & Smishing:** Fake Okta/SSO portals, short-lived phishing domains (5–30 min), dynamic DNS-based domains (e.g., mailchimp-sso[.]com, klv1.it[.]com).
- **Social Engineering:** Vishing, impersonating IT staff, MFA fatigue attacks.
- **SIM Swapping:** Hijacking numbers to intercept MFA tokens.

Execution

- **Living-off-the-Land (LotL):** Abuse of RMM tools like AnyDesk, TeamViewer, ScreenConnect, Splashtop, TacticalRMM, Tailscale VPN.
- **Commercial RATs:** Spectre RAT (latest variant with XOR encoding, HTTP C2), WarZone RAT, Raccoon Stealer, Vidar.

Persistence

- **Abuse of SSO/Federation:** Adding malicious IdPs to maintain cloud persistence.
- **Creation of Privileged Accounts:** Local/domain admin accounts.
- **VPN & RMM Persistence:** Long-term access via commercial tools.

Privilege Escalation / Defense Evasion

- **Credential Dumping:** Using Mimikatz, ADExplorer to harvest credentials and NTDS.dit.
- **Hypervisor Attacks:** VMware ESXi access, resetting root passwords.
- **LotL & Proxy Networks:** Blending in with PowerShell, PsExec; rotating IPs and device names.

Command & Control (C2)

- **Dynamic DNS Domains:** For callback and rapid infrastructure changes.
- **Third-Party Services:** Abuse of Slack, Teams, Exchange, and social media as covert C2.
- **Cloud-based Exfil:** Use of MEGA.nz, AWS S3 for exfiltration.

Discovery / Lateral Movement / Collection

- **Cloud Recon:** AWS inventory abuse, Snowflake database scans.
- **Lateral Movement:** Exploiting federated identities; VPN/RMM pivoting.
- **Collection:** Mass data access from SharePoint, cloud storage, network shares.

Exfiltration & Impact

- **Exfiltration:** Cloud services (MEGA, AWS S3), custom C2 channels.
- **Impact:** Data theft, extortion, DragonForce ransomware (hypervisor-level encryption of VMware ESXi and backups).
- **Ransom Strategy:** Double extortion – encryption + data leak threats.

Malware & Tools

- Spectre RAT (2025 variant – advanced obfuscation, expanded commands).
- WarZone RAT / AveMaria RAT.
- Raccoon & Vidar Stealers.
- DragonForce Ransomware (2025).
- Past RaaS Affiliations: ALPHV/BlackCat (2023), RansomHub (2024).

TARGET PROFILE

Target Sectors

- **Airlines & Transportation:** Qantas (6M records), Hawaiian Airlines, WestJet.
- **Cloud & SaaS Providers:** Okta, Klaviyo, HubSpot, Pure Storage.
- **Retail & Luxury:** Nike, Louis Vuitton, Audemars Piguet.
- **Financial & Insurance:** Credit Karma, Paxos, Morningstar, T-Mobile, Vodafone.
- **Media & Tech:** Twitter/X, Forbes, News Corp.
- **Critical Infrastructure:** Telecom, insurance, and government contractors.

Geographies Targeted

: **Primary:** U.S., U.K., Canada, Europe.
Global Reach: Opportunistic targeting across retail, aviation, SaaS, and finance.

THREAT ASSESSMENT

Risk Level

: Critical o Aviation attacks: Qantas, Hawaiian Airlines, WestJet breaches.

Most Recent Activity

- Business services compromised: Klaviyo, HubSpot, Pure Storage.
- Spectre RAT updated variant deployed in global campaigns.
- Troy Hunt phishing case: Mailchimp-sso[.]com attack linked to Scattered Spider.
- DragonForce ransomware used against VMware ESXi.
- One of the most dangerous and adaptive groups in 2025.

Evolution

- **2022** – SIM swapping & phishing (Okta portals).
- **2023** – RaaS affiliation with ALPHV/BlackCat, MGM Resorts breach.
- **2024** – RansomHub partnership, U.S. indictments/arrests but resilient operations.
- **2025** – Hypervisor-level ransomware (DragonForce), Spectre RAT upgrades, aviation + SaaS sector expansion.

NOTABLE OPERATIONS

2025 (Jul): Qantas data breach – 6M customers impacted; also Hawaiian Airlines & WestJet targeted.

2025 (Mar): Phishing attack on Troy Hunt (Have I Been Pwned) – Mailchimp-sso domain.

2025 (Feb–Apr): Campaigns targeting Klaviyo, HubSpot, Pure Storage; Spectre RAT deployed.

2025 (Ongoing): Adoption of DragonForce ransomware, hypervisor-level attacks on VMware ESXi.

2024: Transition from ALPHV to RansomHub RaaS after law enforcement disruption.

2023 (Sep): MGM Resorts & Caesars Entertainment breaches; $100M+ losses.

2022 (Aug): Early Okta/SSO phishing & SIM swapping campaigns.

ANALYST NOTES (Defensive Takeaways)

- Monitor for short-lived phishing domains (Okta/SSO lookalikes).
- Harden MFA defenses against fatigue/vishing/SIM swapping.
- Review VMware ESXi security posture for ransomware resilience.
- Restrict RMM tool usage (AnyDesk, TeamViewer, Tailscale) and log for anomalies.