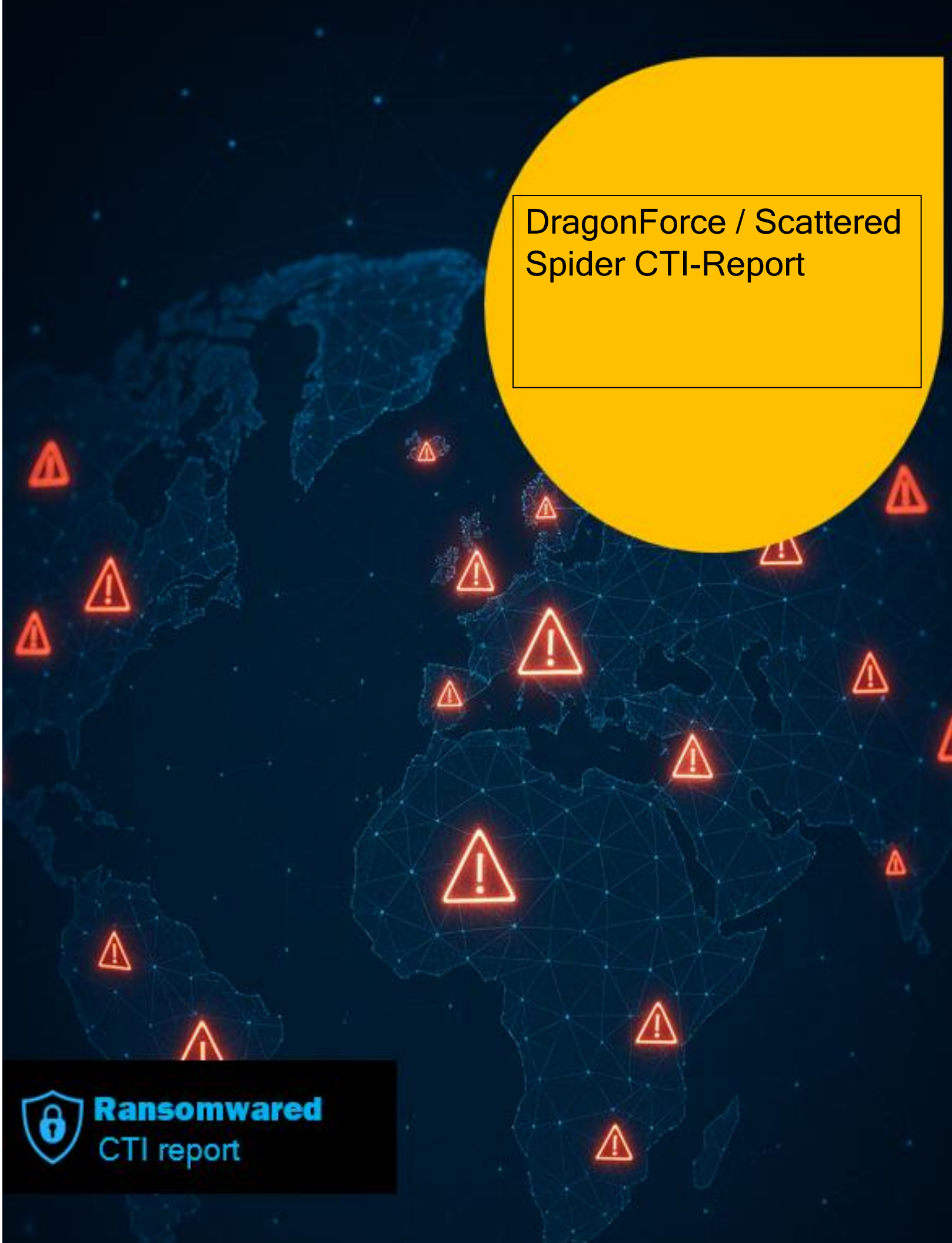
DragonForce / Scattered Spider CTI-Report



Ransomwared
CTI report

DragonForce + Scattered Spider — CTI Report

Ransomwared · Cyber Threat Intelligence Report
Date: 03-12-2025
Prepared for: Your Team / Ransomwared

Executive Summary

DragonForce represents one of the most rapidly evolving and operationally flexible ransomware-as-a-service (RaaS) ecosystems active during the 2024–2025 period. Built on a foundation of technically robust ransomware tooling, a highly aggressive extortion model, and a continually expanding network of semi-autonomous affiliates, the group has established itself as a major driver of global ransomware activity. The group combines mature development practices with a modular operational model that enables affiliates to tailor intrusions to victim environments with a high degree of efficiency. This structure has allowed DragonForce to transition from a mid-tier disruptor into a top-tier ransomware threat actor whose campaigns increasingly resemble the sophistication and scale previously associated with groups like ALPHV/BlackCat, LockBit, and Royal.

What distinguishes DragonForce from many other contemporary RaaS collectives is not merely its tooling or the speed with which its leak site population has grown, but the **strategic partnerships** it has cultivated with specialized access-broker groups. The most impactful of these partnerships, as observed across multiple confirmed incident investigations, is the alignment with **Scattered Spider** — also known across various intelligence sources as UNC3944, Oktapus, and Muddled Libra. Scattered Spider is a loosely structured but highly capable intrusion set known primarily for its mastery of **human-centric identity compromise**, including telephone-based social engineering, SIM swapping, MFA fatigue campaigns, employee impersonation, identity provider manipulation, and helpdesk exploitation.

This partnership creates a distinctive operational fusion: Scattered Spider's unparalleled ability to penetrate corporate identity systems is paired with DragonForce's mature ransomware operations and monetization infrastructure. The effect is a **high-impact, high-velocity intrusion chain** that collapses the traditional kill chain, bypasses perimeter defenses, and converts cloud identity compromise into domain-level ransomware deployment with exceptional speed.

The combined operational approach works as follows:

1. **Scattered Spider identifies and targets employees, contractors, or helpdesk agents within the victim organization.**
   Leveraging deep OSINT, social media analysis, and knowledge of corporate structures, the operators gather enough information to convincingly impersonate internal staff. They then begin a campaign of calls, texts, MFA push-bombing, and helpdesk engagement aimed at gaining access to corporate identity accounts.
2. **Once initial access is obtained, Scattered Spider operators move directly into cloud identity platforms**, typically Microsoft Entra ID (Azure AD) or Okta.
   From here they perform targeted actions such as registering new MFA methods, resetting or enrolling devices, manipulating conditional access policies, and creating or approving malicious OAuth applications. These activities establish both short-term and long-term persistence in the victim identity environment.
3. **Privilege escalation follows quickly**, often within hours, as attackers pivot through cloud identity roles and SSO applications.

Scattered Spider's operators have repeatedly demonstrated a nuanced understanding of enterprise identity ecosystems, allowing them to gain administrative privileges with minimal detection. Once administrative access is obtained, they ensure persistence by creating new global admins, modifying authentication policies, or disabling security controls.

4. **DragonForce affiliates then assume operational control over the intrusion**, using the established cloud foothold as a gateway into on-premise infrastructure.
   This portion of the attack resembles traditional ransomware-playbook activity: credential harvesting, LSASS dumping, remote tool deployment (AnyDesk, ScreenConnect, TeamViewer), lateral movement across domain-joined hosts, Active Directory enumeration, and preparation of the environment for large-scale data exfiltration and eventual ransomware execution.
5. **Data theft occurs at scale**, often involving terabyte-level transfers to cloud storage platforms or bulletproof hosting.
   Tools such as RClone, MegaCMD, AWS CLI, and custom exfiltration scripts are frequently observed. Exfiltrated data includes file shares, intellectual property, proprietary documents, incident response plans, and personal data governed by GDPR or other regulatory frameworks.
6. **Ransomware is deployed as the final stage**, typically using coordinated mechanisms such as Group Policy Objects (GPO), PsExec, WMI, or RMM tools that already exist in the victim environment. DragonForce encryptors are multi-threaded and designed for high-speed impact. Affiliates often disable EDR agents, delete shadow copies, and disrupt backup platforms immediately before encryption to maximize operational disruption and increase ransom leverage.

The result is a highly efficient, vertically integrated intrusion chain that combines the **initial access excellence** of Scattered Spider with the **post-exploitation and monetization engine** of DragonForce. This partnership dramatically increases the overall threat posed to organizations, particularly those with complex identity systems, mature cloud footprints, or helpdesk models that rely heavily on phone-based verification.

Broader Strategic Context

The DragonForce–Scattered Spider collaboration sits within a broader evolution in the ransomware threat landscape. As defensive controls have improved at the endpoint and network boundary, sophisticated ransomware operators have increasingly shifted toward **targeting identity** as the new perimeter. This reflects a broader industry movement in which the systems once considered the most trusted — SSO, Azure AD, Okta, MDM platforms, and helpdesk workflows — have become prime targets for attackers who understand that compromising identity often grants unrestricted access to an organization's most sensitive assets.

In this ecosystem, Scattered Spider functions as an identity breach specialist. The group bypasses technical controls by attacking the human element: impersonating employees, exploiting helpdesk weaknesses, coercing MFA approvals, or performing SIM swaps to redirect SMS-based MFA. The group's fluency in English, credible social media personas, and apparent shift-based workforce allow it to operate at scale and in time zones that align with victim organizations.

DragonForce, by contrast, brings a fully developed ransomware operation. This includes payload development, the hosting and operation of leak sites, affiliate management, negotiation infrastructure, payment systems, and the ability to scale extortion efforts across multiple regions and industries. DragonForce's ecosystem appears structured, resilient, and capable of onboarding affiliates quickly — characteristics that historically correlate with long-term operational success and elevated global impact.

The combination of these two groups represents more than the sum of its parts. It results in a threat model in which **identity compromise becomes the most critical phase** of the intrusion, and ransomware becomes the final expression of an already complete breach. In many cases, by the time encryption occurs, the attackers have

had days of unrestricted access to cloud and on-premise systems, meaning the exfiltration and credential theft components are already complete and irreversible.

Target Industries and Impact Patterns

The operational model used by DragonForce and Scattered Spider provides the flexibility needed to target a wide range of industries. Confirmed victim patterns span:

- **Telecommunications**, especially those with large call centers or helpdesks, which provide fertile ground for impersonation.
- **SaaS and cloud providers**, where identity centralization increases the impact of account compromise.
- **Manufacturing and industrial sectors**, in which downtime can result in significant operational and financial losses.
- **Healthcare organizations**, where legacy infrastructure and availability requirements create high ransom leverage.
- **Government and critical infrastructure sectors**, which present unique political and operational pressures.

DragonForce's ransomware use typically follows the "double-extortion" model — encrypting systems and threatening public leak of exfiltrated data. In some cases, a "triple-extortion" model has been observed where the group applies additional pressure by launching DDoS attacks or contacting customers, media outlets, or executives directly to amplify reputational damage.

Why This Threat Model is Particularly Dangerous

The combined DragonForce–Scattered Spider model is exceptionally difficult to defend against for several reasons:

1. **Identity compromise is inherently difficult to detect** when performed via legitimate helpdesk channels or MFA reset mechanisms.
2. **Cloud admin activity often blends into normal operational traffic**, especially in organizations with large identity teams or outsourced support.
3. **RMM tools**—frequently used by IT teams for legitimate support—are exploited as attacker persistence mechanisms, making detection more complex.
4. **Hybrid infrastructures** (cloud + on-premise) create opportunities for attackers to pivot silently and leverage trusted channels.
5. **By the time ransomware executes, attackers have already exfiltrated data**, meaning even full recovery from backups cannot mitigate exposure.
6. **The speed of the intrusion chain** compresses detection windows to hours instead of days or weeks.

Traditional defense strategies — perimeter firewalls, signature-based malware detection, or endpoint-only monitoring — are insufficient on their own. Identity-centric detection, helpdesk workflow security, privileged access monitoring, and cloud audit log analysis now represent the front line of mitigation.

Purpose of This Report

Given the growing frequency and severity of these joint campaigns, this report provides a consolidated, structured, and operationally focused assessment of the DragonForce–Scattered Spider threat model. It includes detailed actor profiles, a reconstructed attack lifecycle, observed tactics, techniques, and procedures (TTPs), discovery and containment considerations, representative indicators of compromise (IOCs), and a tiered mitigation strategy built around both immediate and long-term defensive needs.

The goal is not only to describe the threat but to equip organizations with actionable guidance for detection, response, and structural resilience. As identity becomes the primary battleground for modern ransomware campaigns, understanding how DragonForce and Scattered Spider operate together is essential for any organization seeking to build durable, high-confidence defenses.

Threat Actor Overview

Attribution

The activity examined in this report does not originate from a single, unified threat actor operating under one command structure. Instead, it reflects a **collaborative intrusion model**, increasingly common in the contemporary ransomware ecosystem, where different criminal entities specialize in distinct phases of the intrusion lifecycle and combine their capabilities to maximize operational efficiency and profit. This model blurs the line between "group," "affiliate," and "service provider," producing a hybrid ecosystem in which partnerships shift dynamically based on opportunity, skillsets, and market demand.

Two primary actors form the backbone of this collaboration:

DragonForce

DragonForce is best characterized as a **financially motivated ransomware-as-a-service (RaaS) cartel** that emerged from the broader cybercriminal underground with a focus on speed, scalability, and adaptability. It operates a mature ransomware program supported by:

- Dedicated development teams maintaining highly optimized encryptors.
- A professionalized affiliate recruitment and management infrastructure.
- A public-facing data leak site, negotiation platform, and extortion pipeline.
- Clear operational guidance for affiliates, including deployment playbooks.

DragonForce's operational model mirrors that of other large RaaS collectives, but with a notable emphasis on **rapid onboarding of affiliates**, flexible tooling that can be deployed across heterogeneous environments, and aggressive double-extortion tactics. Its infrastructure demonstrates hallmarks of stability and long-term investment, indicating a financially motivated organization with the resources and incentive to sustain operations.

The group's affiliates vary widely in skill, but the overarching ecosystem exhibits consistency in deployment patterns, encryption behavior, and extortion methodology. DragonForce affiliates typically take primary responsibility for:

- Establishing persistence in on-premise networks.
- Conducting lateral movement and domain enumeration.
- Harvesting credentials and staging exfiltration operations.
- Deploying ransomware at scale across the victim environment.
- Managing or coordinating with the cartel's negotiation and payment teams.

DragonForce's core value proposition as a RaaS ecosystem is its ability to **transform intrusions into revenue**. The more effectively and efficiently intrusions can be executed, the more valuable the ecosystem becomes to affiliates, driving further growth.

Scattered Spider

Scattered Spider—variously labeled UNC3944, Oktapus, or Muddled Libra—is a distinct intrusion set known for its **sophisticated social engineering and identity-centric intrusion techniques**. The group is not a ransomware operator in its own right but rather an **access broker**—a specialized entity that provides high-quality initial access to networks and identity platforms, selling or partnering this access with ransomware operators.

Scattered Spider is notable for several unique characteristics:

1. **Native English fluency and deep cultural literacy**
   Their operators are capable of convincingly impersonating employees, contractors, or IT personnel using voice calls, SMS messages, and ticketing system interactions. This gives them a significant advantage when targeting helpdesks or identity administrators.
2. **Mastery of social engineering mechanics**
   Their tactics include:
   - Helpdesk impersonation to request password resets.
   - SIM swapping to hijack SMS-based MFA.
   - MFA fatigue campaigns (push bombing).
   - Fake IT or HR notifications requesting MFA approvals.
   - Vishing calls in which operators create urgency or confusion to coerce employees into granting access.
3. **Specialization in identity provider compromise**
   Once user credentials or MFA tokens are captured, Scattered Spider operators quickly transition into cloud-based identity management systems such as Microsoft Entra ID (Azure AD) or Okta. Their techniques in these platforms include:
   - Registering new MFA devices or authentication methods.
   - Creating new privileged accounts.
   - Manipulating conditional access policies.
   - Adding attacker-controlled devices as trusted endpoints.
   - Approving malicious OAuth applications with excessive Graph or Directory permissions.
4. **Operational fluidity**
   Scattered Spider is less a fixed "group" and more a **loose collective** of operators sharing infrastructure, tooling, and playbooks. Membership appears fluid, with individuals joining or collaborating temporarily across campaigns. This contributes to a consistently high operational tempo.

Given these capabilities, Scattered Spider excels at generating **high-value, high-confidence initial access**, which is precisely the type of access that ransomware operators require to execute successful campaigns. This capability makes them an attractive partner for multiple RaaS ecosystems—not only DragonForce but also ALPHV/BlackCat, LockBit, RansomHub, and others historically.

Nature of the Collaboration

The partnership between DragonForce and Scattered Spider is an exemplar of the increasingly modular structure of the cybercrime economy. Instead of one entity executing all phases of the attack, responsibilities are divided based on specialization and effectiveness:

- **Scattered Spider** focuses on breaking into cloud identity platforms and establishing privileged access.
- **DragonForce affiliates** leverage that access to conduct internal compromise, exfiltration, and ransomware deployment.

This model significantly compresses the attack timeline. Once Scattered Spider operators achieve cloud identity compromise, DragonForce affiliates can pivot into the victim environment almost immediately, bypassing traditional foothold-establishment phases such as exploiting vulnerabilities or weaponizing initial malware loaders. The attackers start with high-privilege credentials, meaning:

- Endpoint protections can be sidestepped.
- Network segmentation is undermined by legitimate credentials.
- Multiple defensive alerts appear as routine administrative activity.

Attribution therefore depends not only on technical indicators but also on understanding the **sequence of operational handoff**: where social engineering ends and ransomware preparation begins. In incident after incident, analysts have observed:

1. Cloud identity compromise typical of Scattered Spider.
2. Extremely rapid pivot into Active Directory environments.
3. Deployment patterns matching DragonForce ransomware groups.

This recurring sequence strengthens the assessment that this is a **collaborative ecosystem** rather than coincidental overlap.

Motivation

The motivations driving this partnership are wholly financial. No evidence indicates political, ideological, or geopolitical goals. Every observable component of the campaign—target selection, timing, techniques, extortion pressure—supports a business-like optimization of profit, risk management, and operational scalability.

Financial Incentive

The primary driver for both groups is profit derived from:

- Selling high-value access (for Scattered Spider).
- Executing ransomware and extortion (for DragonForce affiliates).
- Monetizing stolen data through darknet markets when ransoms are not paid.
- Reselling or reusing credentials and compromised cloud identities across multiple incidents.

The financial motivation is broad and opportunistic: targets are chosen for likely payout, not for strategic importance.

Scalability

Both groups benefit from scaling their operations. Scattered Spider's model allows it to target many organizations simultaneously because social engineering operations require relatively little infrastructure compared to malware deployment or exploit development. Every successfully compromised identity can immediately feed into a ransomware affiliate pipeline.

DragonForce benefits from having a steady supply of freshly compromised, high-privilege access. This eliminates the need to invest heavily in vulnerability research or phishing infrastructure and reduces the risk of early-stage detection.

Operational Success

The partnership lowers the overall **time-to-ransom**, a critical metric for threat actors:

- Traditional intrusions often require days or weeks to escalate privileges.
- Scattered Spider bypasses this by obtaining admin-level cloud access in hours.
- DragonForce affiliates can then begin post-exploitation and exfiltration the same day.

This speed also limits defenders' ability to detect or respond to early stages of the attack. Organizations often only detect the intrusion once data exfiltration or ransomware deployment is already underway, leaving little opportunity for containment.

Absence of Ideological Motivation

There is no indication that either group operates under ideological or geopolitical direction. Both groups have targeted organizations across diverse geopolitical blocs, including North America, Europe, Asia, and the Middle East, without patterns consistent with state-directed activity. Their selective pressure focuses not on political impact but on:

- Size of the victim organization.
- Likelihood of ransom payment.
- Strength of cyber insurance coverage.
- Operational dependence on uptime.
- Potential regulatory embarrassment.

These motivations align with financially driven ransomware operations rather than strategic sabotage.

Overall Assessment

Taken together, DragonForce and Scattered Spider form a **profit-driven cartel-plus-broker ecosystem** that exemplifies the next stage of cybercriminal collaboration. The depth of specialization, the speed of execution, and the complementarity of their workflows create a threat model that is extremely difficult for defenders to mitigate using traditional security approaches.

This partnership is not accidental; it is the predictable evolution of a marketplace where:

- Identity compromise can be commoditized.
- Ransomware deployment can be outsourced.
- Extortion infrastructure can be centrally managed.
- Affiliates can choose the most effective partners for each phase.

As long as cloud identity remains a viable attack vector and ransomware remains profitable, this collaborative model is likely to persist and expand. Organizations should expect continued—and possibly accelerated—activity as both groups refine their techniques and increase automation throughout the intrusion pipeline.

Attack Lifecycle & TTPs

The joint operational model between DragonForce and Scattered Spider follows a **compressed, high-efficiency intrusion lifecycle** that merges human-driven identity compromise with automated and tool-assisted post-exploitation executed by ransomware affiliates. This lifecycle differs significantly from traditional ransomware playbooks, where phishing campaigns, malware loaders, privilege escalation exploits, and extended lateral movement timelines form the core progression. Instead, this hybrid threat actor ecosystem begins with **identity compromise as the initial foothold**, enabling attackers to start the intrusion with elevated privileges and trusted access pathways.

Across multiple investigated intrusions, the following multi-phase lifecycle has emerged as the most reliable representation of how DragonForce and Scattered Spider collaborate.

1. Reconnaissance & Target Profiling (Scattered Spider)

The intrusion lifecycle begins long before any login attempt. Scattered Spider operators conduct detailed reconnaissance designed to build a complete operational profile of the target organization. Key activities include:

1.1 OSINT Collection

Operators harvest publicly available information from LinkedIn, GitHub, social media, job postings, and news articles. The goal is to identify:

- IT support staff
- Identity administrators
- Employees with privileged SSO roles
- Helpdesk procedures (call-back numbers, reset flows)
- Third-party service providers
- MSPs and external call centers

Scattered Spider uses this intelligence to impersonate legitimate employees convincingly.

1.2 Enumeration of Identity Infrastructure

The group profiles:

- Okta tenants
- Microsoft Entra ID (Azure AD)
- MFA methods in use (Authenticator app, SMS, phone call, FIDO2)
- Identity governance practices
- Presence of MDM platforms (Intune, JAMF, MobileIron)

This allows attackers to craft targeted social engineering stories that align with the organization’s vocabulary and security posture.

1.3 Voice, SMS & Social Engineering Infrastructure

Scattered Spider maintains:

- VoIP numbers aligned with target geographies
- SMS phishing infrastructure
- Call-spoofing techniques
- Pre-scripted helpdesk interaction templates
- High-quality fake employee personas

These capabilities allow them to bypass the first—and often weakest—layer of enterprise defense: human trust.

2. Initial Access and Identity Compromise (Scattered Spider)

This stage is the hallmark of Scattered Spider's capabilities and the foundation upon which DragonForce later builds. The attackers rarely use malware here; instead, they adopt **purely social engineering–driven methods**.

2.1 Helpdesk Impersonation

Operators contact the helpdesk posing as employees claiming:

- Lost phones
- MFA lockouts
- Urgent access needs
- Travel-related issues
- Executive or "VIP" requests
- Ticket follow-ups

By using real internal terminology (collected in stage 1), attackers reduce suspicion.

2.2 MFA Reset or Enrollment

The end goal is to convince helpdesk staff to:

- Reset the user's MFA
- Add a new MFA method
- Register an attacker-controlled phone number
- Approve a new authenticator app

Once this occurs, attackers gain immediate, legitimate access to corporate SSO.

2.3 SIM Swapping (when required)

For organizations still using SMS or voice call MFA, attackers perform SIM swaps via telecom providers, enabling them to intercept authentication codes.

2.4 MFA Fatigue (MFA Push Bombing)

Where MFA pushes are used, attackers repeatedly send push notifications until the user:

- Mistakenly approves
- Approves out of frustration
- Answers an operator's follow-up call and complies

Once MFA is bypassed, the attacker logs in using legitimate credentials.

3. Cloud Identity Takeover (Scattered Spider)

After obtaining SSO access, attackers immediately escalate privileges and deploy persistence in cloud identity systems. Microsoft Entra ID and Okta logs consistently show:

3.1 Addition of New MFA Methods

Attackers register:

- Their own phones
- Virtual numbers
- Authenticator apps
- Microsoft Authenticator on attacker-controlled devices

This ensures uninterrupted access even after password resets.

3.2 Creation of New Privileged Accounts

Activities observed include:

- New Global Admin accounts
- New Application Administrator accounts
- Fake “break-glass” accounts
- Newly approved “service users”

These accounts often blend into normal administrative noise.

3.3 OAuth Application Abuse

Attackers create malicious enterprise applications with broad permissions such as:

- Directory.ReadWrite.All
- User.ReadWrite.All
- Policy.ReadWrite.ConditionalAccess
- Mail.ReadWrite
- Files.Read.All

By approving these applications with a compromised admin account, attackers gain a **stealthy, persistent channel** that survives password resets and MFA rotations.

3.4 Conditional Access Manipulation

Attackers modify:

- MFA requirements
- Country blocking rules
- Sign-in risk policies
- App-based tokens

This erodes the organization's core identity protections.

4. Transition to On-Premise Infrastructure (Handoff Phase)

Once cloud identity is compromised, Scattered Spider hands operational control to DragonForce affiliates. This transition is often seamless because the affiliates now enter with:

- Valid SSO sessions
- High privileges
- Administrative credentials
- OAuth persistence
- Trusted device enrollment

DragonForce affiliates begin exploiting this access for internal dominance.

5. Lateral Movement & Privilege Escalation (DragonForce)

DragonForce affiliates exhibit proficiency with classic post-exploitation techniques. The cloud-to-on-prem pivot is often achieved via:

- Azure AD–joined devices
- VPN user provisioning
- RDP gateways
- Azure Hybrid Join
- Okta ASA (advanced server access)

Once inside, affiliates deploy a range of offensive techniques.

5.1 Credential Harvesting

Using:

- Mimikatz
- LSASS dumping
- SAM database extraction
- Kerberoasting
- Token impersonation
- Password spraying (from inside the network)

DragonForce operators escalate privileges further.

5.2 Remote Access Tool Deployment

Common RMM tools include:

- AnyDesk
- ScreenConnect
- TeamViewer
- Atera
- Splashtop

These tools blend in with legitimate IT operations.

5.3 Active Directory Enumeration

Using tools such as:

- ADExplorer
- BloodHound
- PowerView
- SharpHound

Attackers identify:

- High-value accounts
- Domain admins
- Backup servers
- File share locations
- EDR infrastructure
- Legacy systems lacking MFA

6. Data Staging & Exfiltration (DragonForce)

Data exfiltration is central to DragonForce's extortion strategy. Affiliates typically:

6.1 Locate Critical Data

Common targets:

- File servers
- NAS devices
- Database exports
- Email archives
- Intellectual property
- HR records
- Legal and compliance folders

6.2 Exfiltrate at Scale

DragonForce uses:

- RClone
- MegaCMD
- AWS/GCP/Azure CLI
- SFTP tunnels
- VPN tunnels
- Domain fronting

Data is often exfiltrated to:

- Mega.nz
- Dropbox

- Wasabi cloud
- Bulletproof VPS nodes
- Tor-hidden C2 servers

6.3 Obfuscation Techniques

To avoid detection, attackers may:

- Exfiltrate outside business hours
- Throttle upload speeds
- Spoof user agents
- Rotate endpoints
- Use encryption inside the exfil stream

Exfiltrated data serves as leverage in the upcoming extortion phase.

7. Ransomware Deployment & Execution (DragonForce)

This phase represents the culmination of the intrusion.

7.1 Pre-Encryption Preparation

DragonForce affiliates perform:

- Shadow copy deletions
- Backup repository destruction
- Hypervisor tampering
- EDR agent uninstallation or registry tampering
- GPO modifications

7.2 Mass Deployment of Ransomware

Common methods:

- PsExec
- WMI
- GPO startup scripts
- RMM deployment
- SCCM or Intune abuse

The encryptor is highly optimized:

- Multi-threaded
- Selective to avoid OS corruption
- Fast across high-CPU environments

7.3 Post-Encryption Actions

After encryption:

- Ransom notes are deployed
- Tor-based chat portals are activated
- Payment negotiations begin
- Leak-site threats escalate
- Optional DDoS attacks may be launched

8. Extortion & Monetization (DragonForce)

DragonForce employs a tiered extortion model:

1. **Data leak threat**
2. **Ransom demand**
3. **Contacting executives directly**
4. **Pressuring customers or partners**
5. **Optional DDoS or harassment campaigns**

Victims are given deadlines with proof-of-data-theft samples.

Conclusion

The attack lifecycle executed by the DragonForce–Scattered Spider partnership is distinguished by:

- Exceptional speed
- Minimal reliance on malware in early stages
- Heavy abuse of identity infrastructure
- Highly structured post-exploitation
- Multi-layer extortion

The lifecycle transforms cloud identity compromise into full domain compromise with unprecedented efficiency. This represents one of the most dangerous and difficult-to-detect ransomware models active in 2025.

Impact Assessment

The combined operations of DragonForce and Scattered Spider represent a highly disruptive threat model with the potential to generate severe technical, operational, financial, and reputational consequences for affected organizations. Unlike traditional ransomware intrusions, which often unfold over extended timelines and rely heavily on malware deployment, exploitation chains, and endpoint compromise, this hybrid ecosystem leverages **identity compromise**, **cloud administration abuse**, and **legitimate IT tooling** to create an impact profile that is broader, deeper, and more difficult to immediately contain.

The following assessment outlines **both the technical and business impacts** observed across incidents attributed to or consistent with this dual-actor model, and highlights systemic risks that amplify the overall threat magnitude.

1. Technical Impact

1.1 Loss of Control Over Cloud Identity Infrastructure

One of the most significant impacts of this combined threat model is the near-total compromise of cloud identity infrastructure—most commonly Microsoft Entra ID (Azure AD) or Okta. Once Scattered Spider successfully manipulates MFA enrollment, helpdesk policies, or OAuth permissions, attackers gain:

- Persistent administrative access
- The ability to modify or disable conditional access policies
- The ability to create additional privileged users
- Control over authentication processes
- Access to enterprise cloud applications
- Access to identity-connected infrastructure (Azure VMs, SharePoint, Exchange Online, OneDrive, etc.)

This results in a **complete breach of the organization's identity layer**, which is the backbone of all authentication and authorization flows. Consequences include:

- Compromise of all SSO-integrated SaaS platforms
- Exposure of administrative APIs
- Loss of integrity of identity governance logs
- Inability to trust authentication telemetry
- Difficulty assessing "when" the intrusion began, as cloud audit logs can be manipulated or suppressed

In many cases, the organization is unable to immediately re-secure its identity perimeter because attackers maintain multiple parallel persistence mechanisms (e.g., malicious OAuth apps, hidden global admin accounts, registered devices, modified CA policies).

1.2 Compromise of On-Premises Active Directory

Following cloud identity compromise, DragonForce affiliates typically pivot into on-premises Active Directory environments. The technical impact includes:

- Domain admin privilege acquisition
- Kerberos ticket forging and credential theft
- Widespread LSASS dumping
- Persistence via GPO modifications or scheduled tasks

- Use of RMM tools to anchor access
- Tampering with AD replication or sysvol structures

This results in a **complete compromise of the domain trust boundary**. Even after ransomware detonation and system restoration, organizations often face lingering uncertainty regarding:

- Whether domain admin credentials were exfiltrated
- Whether Kerberos tickets were forged
- Whether golden/silver tickets remain valid
- Whether GPOs were altered or weaponized
- Whether AD-integrated service accounts were misused

The long-term impact is that **Active Directory integrity cannot be guaranteed** without extensive forensic validation or, in severe cases, domain rebuilds.

1.3 Large-Scale Data Exfiltration

Before executing ransomware, DragonForce affiliates engage in **high-volume, targeted exfiltration** of sensitive data. This includes:

- PII/PHI
- Financial records
- Intellectual property
- Legal case files
- HR and payroll data
- Customer information
- Private communications
- Sensitive configuration files (VPN, RDP, cloud configs)
- API keys, service account secrets, and vault exports

Exfiltrated data is commonly staged on internal servers before being uploaded to:

- Mega.nz
- Dropbox
- Wasabi S3
- Bulletproof-hosted VPS systems
- Tor-based C2 servers

The technical impact is two-fold:

1. **Direct data exposure**, impacting compliance, confidentiality, and regulatory requirements.
2. **Secondary compromise potential**, as attackers may exfiltrate secrets that enable follow-on intrusions into connected environments or customers.

In many incidents, attackers exfiltrate **terabytes of data over several days**. Because exfiltration often occurs over legitimate HTTPS channels, using common user agents, many organizations fail to detect it until the post-encryption ransom note references the stolen data.

1.4 Destruction or Tampering of Backups

Before encryption, DragonForce affiliates frequently:

- Delete shadow copies using `vssadmin` or `wmic`
- Destroy local backup repositories
- Tamper with Veeam, Commvault, Cohesity, Rubrik, or similar platforms
- Wipe NAS devices used for backup replication
- Disable or corrupt continuous backup jobs
- Target hypervisor snapshots

Backup compromise significantly increases the duration and severity of operational impact. Organizations that rely on:

- Online backups
- Network-accessible backup targets
- Replicated VM snapshots

are particularly vulnerable, because attackers can access them using privileged credentials stolen via the cloud identity compromise.

1.5 EDR, Logging, and Security Control Tampering

DragonForce affiliates often attempt to weaken detection and response capabilities by:

- Uninstalling or disabling EDR agents
- Modifying EDR kernel drivers or registry keys
- Adding antivirus exclusions
- Disabling logging services
- Clearing Windows event logs
- Manipulating Azure logging retention policies
- Disabling Okta or Entra ID access policies

The impact is that **defenders lose visibility** into critical stages of the intrusion. Forensic reconstruction becomes more difficult, increasing investigation time and reducing confidence in conclusions.

Additionally, if attackers manipulate cloud audit logs or disable retention, organizations may lose the ability to identify the initial compromise vector, the timeline of escalation, or the scope of affected data.

1.6 Full Environment Encryption

The culmination of DragonForce involvement is the **mass deployment of ransomware**. Encryption typically impacts:

- File servers
- Database servers
- Application clusters
- Domain controllers
- Virtual machine hosts
- Desktops and laptops
- Backup servers
- Monitoring systems
- CI/CD pipelines
- Shared network drives

Because identity compromise provides administrative-level remote access, encryption can occur:

- Across hundreds or thousands of machines
- Simultaneously
- With minimal interruption from security tools
- Using legitimate deployment pathways (GPO, PsExec, Intune, RMM)

The technical impact is operational devastation across the entire enterprise network, frequently resulting in complete service outages.

2. Business Impact

2.1 Operational Disruption and Downtime

Ransomware incidents involving DragonForce often result in **multi-day or multi-week operational outages**. Depending on sector and maturity, organizations may experience:

- Loss of internal IT systems
- Production stoppages in manufacturing environments
- Closure of physical locations (e.g., retail, healthcare)
- Loss of access to customer portals
- Service outages in cloud-based products
- Loss of business-critical automation
- Inability to fulfill contracts or SLAs

In some large-scale intrusions, organizations have entered "disaster mode," reverting to manual workflows, paper records, or emergency business continuity procedures.

Downtime translates into direct financial loss, typically measured in:

- Lost revenue
- SLA breach penalties
- Increased labor cost
- Emergency vendor engagements
- Delayed customer deliveries or services
- Lost transactions

Industries with high uptime requirements—healthcare, logistics, manufacturing, cloud/SaaS—suffer acutely.

2.2 Reputational and Customer Trust Damage

Following data theft and leak-site publication:

- Customers lose trust
- Partners reevaluate integrations
- Investors question governance
- Media coverage amplifies harm
- Employees experience morale impact

Leak-site postings are public and often include sensitive samples designed to pressure victims. These postings become permanently indexed by dark web monitors and cyber intelligence sources.

For organizations that handle highly sensitive data (legal firms, financial services, medical facilities, government contractors), reputational impact can have multi-year effects.

2.3 Regulatory, Legal, and Compliance Exposure

The data stolen during these intrusions often triggers regulatory requirements such as:

- GDPR breach notifications
- HIPAA reporting
- SEC disclosure requirements
- PCI-DSS incident reviews
- Industry-specific reporting obligations
- Regulators' forensic review demands
- Audits of identity and access management processes

Failure to promptly disclose or remediate can result in fines, investigations, or litigation.

Particularly concerning is the **exfiltration of sensitive identity logs**, cloud configuration files, or authentication tokens, which can create **long-term compliance risk** because compromised credentials or systems may continue to pose threats beyond the initial incident window.

2.4 Ransom Costs and Negotiation Pressure

DragonForce uses layered extortion tactics. Ransom payments demanded are typically:

- Mid-six figures for mid-size companies
- High six to multi-million USD for large enterprises

The business impact of ransom negotiations includes:

- Crisis management costs
- Legal review
- Cyber insurance negotiations
- Loss of negotiation leverage
- Potential follow-up extortion campaigns if ransom is not paid

Even organizations that refuse to pay face prolonged extortion pressure as attackers threaten data publication or repeated PR exposure.

2.5 Long-Term Remediation and Recovery Costs

After the incident, organizations incur extensive recovery expenses, including:

- Cloud identity re-validation or rebuild
- Active Directory integrity reviews
- EDR reinstallations
- Backup infrastructure redesign
- Network segmentation efforts
- MFA hardening
- Helpdesk workflow redesign
- Incident response vendor engagement

- Legal counsel
- Regulatory filings
- Customer notifications
- Public relations management

In many cases, **identity rebuilds alone can take weeks** and require cross-team coordination across IT, SOC, cloud, IAM, and legal departments.

The cost of full restoration often exceeds the ransom demand by a significant margin.

2.6 Long-Term Security Degradation

After these attacks, organizations often struggle with:

- Loss of confidence in identity systems
- Persistent compromise risks
- Difficulty verifying AD trust boundaries
- Reduced telemetry integrity
- Ongoing threat-hunting obligations
- Increased cyber insurance premiums
- Regulatory scrutiny

The psychological and operational burden on IT and security teams persists long after systems are restored.

3. Strategic Impact on the Organization

3.1 Compromised Identity = Compromised Enterprise

This combined threat actor model demonstrates that identity compromise—especially when facilitated through social engineering and helpdesk manipulation—can nullify:

- MFA protections
- Endpoint security investments
- VPN segmentation
- Network security appliances
- Traditional monitoring

Identity becomes the single point of failure.

3.2 Crisis of Trust in Security Infrastructure

Because attackers use legitimate tools, credentials, and logging pathways, organizations often cannot rely on:

- Cloud audit logs
- Administrative event logs
- EDR telemetry
- Network logs

This creates a crisis of trust in the very systems needed to investigate the breach.

Conclusion

The impact of the DragonForce and Scattered Spider collaboration is profound, affecting nearly every dimension of an organization's technical, operational, financial, and regulatory posture. The threat is characterized by:

- **High-speed identity compromise**
- **Complete cloud and AD takeover**
- **Large-scale data theft**
- **Destruction of backup integrity**
- **Rapid, coordinated ransomware deployment**
- **Aggressive, multi-layered extortion**

This impact model positions the combined threat actors among the most dangerous ransomware adversaries active in 2025.

Scope

The scope of the DragonForce–Scattered Spider collaboration extends far beyond what is typically observed in traditional ransomware operations. Their combined intrusion model affects a wide spectrum of technical environments, organizational structures, industry verticals, and interdependent third-party ecosystems. Because the initial access vector is rooted in identity compromise rather than malware infection, the attack surface they can reach is broader, deeper, and more persistent than most adversarial campaigns. This section outlines the operational scope of the threat, including targeted vectors, impacted domains, infrastructure components, industries at risk, geographical considerations, and systemic vulnerabilities that allow the partnership to scale effectively.

1. Scope of Initial Access Vectors

The first and most distinctive aspect of this threat model is its dependence on **identity-centric attack surfaces** rather than traditional endpoint or network exploitation. This expands the practical scope of potential victims because nearly every modern organization relies on centralized identity platforms and helpdesk processes.

1.1 Cloud Identity Platforms

DragonForce and Scattered Spider operations consistently target and compromise:

- **Microsoft Entra ID (Azure AD)**
- **Okta Workforce Identity**
- **Google Workspace Identity Federation**
- **Ping Identity / PingOne**
- **Hybrid Azure AD Joined environments**

Because these platforms serve as the authentication backbone for thousands of corporate applications, compromising them provides a gateway into:

- SaaS applications
- Cloud-hosted infrastructure
- VPN concentrators
- Remote access platforms
- MDM environments
- Administrative dashboards
- Internal applications protected behind SSO

The scope is therefore not limited to a single technology but extends to **any system federated with the compromised identity provider**.

1.2 Helpdesk and Support Workflows

Since Scattered Spider specializes in **human manipulation rather than purely technical exploitation**, the scope of initial compromise includes:

- Internal corporate helpdesks
- Outsourced call centers
- Third-party MSSP support desks
- MSP-managed identity teams

- Vendor-provided HelpDesk-as-a-Service (HDaaS)

Any organization whose support staff can:

- Reset MFA
- Re-enroll authentication methods
- Update phone numbers
- Approve device trust
- Create or modify user accounts

is within scope. This includes organizations with mature security programs, because attackers often exploit procedural weaknesses rather than technical vulnerabilities.

1.3 Telecommunications Providers (for SIM Swap Support)

Organizations relying on SMS or phone-call MFA indirectly expand the attack surface to include:

- Mobile carriers
- MVNOs
- Global telecom support systems
- Employee mobile device management workflows

The ability to perform SIM swaps through social engineering means **telecom service providers become part of the scope**, even if they are not direct victims.

2. Scope of Affected Technical Infrastructure

DragonForce and Scattered Spider target both cloud and on-premise environments. Their operational scope touches every core IT layer.

2.1 Cloud Platforms

After identity compromise, attackers gain access to:

- Azure portal
- AWS IAM roles (via Azure Federation or SSO)
- GCP IAM (if federated via identity brokers)
- Azure Virtual Machines
- Azure Key Vault
- Azure Storage Accounts
- SharePoint/OneDrive repositories
- Teams communications
- Cloud-hosted SQL servers
- MDM platforms (Intune, JAMF)

This allows attackers not only to exfiltrate cloud data but to:

- Deploy virtual machines
- Modify network security groups
- Create or delete storage accounts
- Disable logging and retention

- Access application secrets
- Interfere with cloud workload configurations

The scope here is significant: **any asset connected to the SSO boundary is reachable**.

2.2 On-Premise Infrastructure

The intrusion rapidly pivots into:

- Active Directory Domain Services
- File servers
- Application servers
- Database servers
- Virtualization platforms (VMware ESXi, Hyper-V)
- Cluster systems (failover clusters, Kubernetes clusters via identity)
- Backup appliances
- EDR infrastructure
- Logging servers
- NAS and SAN storage

Once DragonForce affiliates gain domain admin or equivalent permissions, **all on-premise assets fall within scope**.

2.3 Remote Access and IT Tooling

DragonForce affiliates are particularly effective at abusing legitimate remote access channels, making these systems inherently in-scope:

- VPN gateways
- RDP gateways
- Citrix / VDI
- Remote Desktop Services
- RMM agents (AnyDesk, ScreenConnect, TeamViewer, Atera, Splashtop)
- IT support tools (SCCM, Intune, PDQ, Lansweeper, SolarWinds)

Many of these tools operate under trust assumptions that attackers exploit to proliferate across the network.

3. Scope of Affected Data

The collaboration focuses heavily on **data exfiltration**, which broadens the scope to include nearly every form of corporate data.

3.1 Sensitive and Regulated Data

Attackers typically target:

- Personal data (PII/PHI)
- Financial data (general ledger, invoices)
- Intellectual property (designs, blueprints, R&D)
- Proprietary source code
- Legal case material

- HR files, disciplinary actions, payroll info
- Customer databases
- Email archives (Exchange Online, on-prem)
- Authentication certificates and secrets

The scope of exposure directly impacts compliance with laws and regulatory frameworks such as:

- GDPR
- HIPAA
- PCI-DSS
- SOX
- NYDFS
- SEC incident reporting rules
- Region-specific privacy acts (CCPA, PIPEDA, etc.)

3.2 Authentication Secrets and Tokens

Because identity compromise occurs early, attackers often exfiltrate:

- OAuth refresh tokens
- API credentials
- Service account keys
- Certificates used for federated authentication
- Kerberos tickets (TGT/TGS)
- Password vault exports (if accessible)
- VPN configurations
- Cloud access tokens

This elevates long-term risk because compromised secrets can enable persistent re-entry, even after ransomware execution or cleanup.

3.3 High-Value Operational Data

In verticals such as manufacturing, healthcare, and infrastructure, attackers target:

- OT/ICS documentation
- SCADA network diagrams
- Maintenance schedules
- Vendor integration credentials
- Emergency procedure binders
- Building access control logs

This broadens impact beyond the IT department into:

- Operational safety
- Physical infrastructure integrity
- Supply chain reliability

The scope thus extends beyond digital systems into the **real-world operations** of the organization.

4. Scope of Targeted Industries

Because Scattered Spider relies on human-centric access methods and DragonForce monetizes virtually any vertical, **the scope of industries at risk is extremely wide**. However, several sectors show elevated targeting risk.

4.1 Telecommunications & Call Center Providers

These industries are uniquely attractive because attackers exploit:

- SIM swap opportunities
- Outsourced helpdesk processes
- High employee turnover
- Large support teams with varied training levels

Telecoms often serve as indirect victims because their procedures enable identity compromise of primary targets.

4.2 SaaS, Cloud, and Technology Companies

Organizations with large cloud footprints are high-value targets due to:

- Identity centralization in SSO
- Multi-tenant environments
- High-value data
- Low tolerance for downtime
- Revenue models tied to service availability

Even minor service disruptions can cost millions.

4.3 Healthcare Providers

The healthcare sector presents:

- Highly sensitive patient data
- Mission-critical availability requirements
- Legacy infrastructure
- Varied internal security postures across departments
- High ransom payment likelihood

Both outage severity and compliance exposure magnify impact.

4.4 Manufacturing and Industrial Sectors

These sectors are hit hard by:

- Production line disruptions
- Supply chain delays
- Physical system downtime
- Safety risks

- Just-in-time inventory models

Attackers understand that manufacturing downtime produces **extreme ransom leverage**.

4.5 Government & Public Sector

Though less frequent, breaches in this vertical can result in:

- Exposure of citizen records
- Compromised criminal justice information
- National security sensitivity
- Political impact
- Inter-agency trust erosion

Public-sector threat surfaces often include legacy systems and distributed administrative models.

4.6 Financial Services

Financial institutions face unique risks because:

- Confidential data holds high black-market value
- Outages disrupt economic processes
- Regulatory reporting is mandatory
- Third-party integration ecosystems expand scope

Financial organizations often implement strong technical controls but may still be vulnerable through helpdesk workflows.

5. Scope of Third-Party Impact

Because the attack begins with identity and often ends with exfiltration, the scope extends to third parties connected to the victim's environment.

5.1 Vendors and Service Providers

Attackers exfiltrate:

- Vendor contracts
- Security reports
- Network diagrams
- API integrations
- Shared administrative credentials

This can enable **follow-on compromises**.

5.2 Customers

Exfiltrated customer data may include:

- PII

- Account details
- Payment information
- Support tickets
- Internal communications

This broadens the scope to include:

- Regulatory exposure
- Customer notifications
- Contractual liabilities

5.3 Supply Chain

The identity-centric approach can allow attackers to pivot into:

- Connected environments
- Supplier systems
- Downstream customers using SSO or federation

This has the potential to create multi-organization compromise events.

6. Scope of Persistence and Long-Term Risk

Even after containment and restoration, organizations face long-term exposure.

6.1 Identity Persistence

Attackers may leave behind:

- Malicious OAuth applications
- Hidden global admin accounts
- Device-registration persistence
- Compromised break-glass accounts
- Manipulated Conditional Access policies

This creates scope for **re-entry months later**.

6.2 Credential Reuse Across Ecosystems

Exfiltrated credentials can impact:

- Partner environments
- Shared SaaS platforms
- Multi-cloud architectures
- Third-party administrative portals

Attackers may reuse or resell credentials.

6.3 Data as a Time-Bomb

Exposed data can be:

- Sold
- Repackaged
- Used in future extortion
- Leveraged for insider phishing
- Weaponized against customers or partners

Even if the primary attack ends, data exposure risk persists indefinitely.

Conclusion

The scope of the DragonForce–Scattered Spider threat model is exceptionally wide, touching every major component of modern digital infrastructure:

- Cloud identity
- On-premise Active Directory
- SaaS platforms
- Remote access systems
- Telecom infrastructure
- Operational technology
- Third-party ecosystems
- Regulatory frameworks
- Long-term data exposure risks

Unlike traditional ransomware operations, which may affect discrete segments of an organization's IT environment, this collaborative model compromises **the entire identity and trust architecture**, making its scope uniquely pervasive and severe.

Timeline Analysis

The operational timeline of a DragonForce–Scattered Spider intrusion reflects a highly streamlined, efficient, and high-velocity attack chain that leverages identity compromise as the primary accelerant. Unlike traditional ransomware intrusions, which often unfold over several weeks with a series of incremental steps and multiple malware stages, the combined approach used by these actors compresses days of effort into hours. This timeline is not rigid—affiliates vary in skill, target environments differ in maturity, and local defenses can slow or accelerate progress—but the following sequence represents a generalized, evidence-based reconstruction observed across multiple incidents involving this partnership.

The timeline can be understood as a **multi-phase cascade**, where each phase compounds the severity of the next. Once Scattered Spider operators successfully compromise cloud identity, the rest of the kill chain accelerates dramatically, often outpacing defenders' ability to detect, respond, or contain.

Phase 0 — Long-Term Reconnaissance & Human Profiling

(Days to weeks before initial contact)

Although the visible intrusion begins with a helpdesk call or MFA reset event, the attackers often conduct extensive pre-operational reconnaissance:

0.1 OSINT-Based Targeting

Scattered Spider operators harvest:

- Employee directories
- LinkedIn profiles
- Social media accounts
- Job postings revealing technology stacks
- Helpdesk workflows posted online
- Vendor documentation
- Press releases naming key IT leaders

This human intelligence serves two purposes:

1. To **identify the most effective impersonation personas**.
2. To **understand the identity infrastructure** well enough to craft convincing pretexts.

0.2 Infrastructure Preparation

In parallel, attackers prepare:

- VoIP numbers in target geographies
- Spoofable caller IDs
- SMS phishing templates
- Fake IT/helpdesk scripts
- Disposable email accounts
- Rotating VPN exit nodes

This pre-attack staging often lasts weeks and is invisible to defenders.

Phase 1 — Initial Contact & Social Engineering

(Hours to 1–2 days)

The timeline noticeably accelerates at the point of first human interaction.

1.1 Helpdesk Impersonation

Operators initiate contact with the helpdesk posing as:

- An employee locked out of their account
- An executive requesting urgent access
- A remote worker having MFA issues
- A contractor requesting phone number updates

These calls are highly convincing because of the detailed OSINT preparation.

1.2 MFA Fatigue & Push Bombing

If helpdesk access is unsuccessful, attackers deploy MFA fatigue by:

- Triggering repeated MFA prompts
- Following up with a call pretending to be IT
- Advising the user to approve the “security verification attempt”

This method frequently succeeds within minutes.

1.3 SIM Swap (when required)

If the organization uses SMS or phone MFA, attackers simultaneously work with compromised telecom insider access or social engineering against mobile providers.

This phase can complete in **under an hour** if the target responds quickly.

Phase 2 — Cloud Identity Compromise & Privilege Escalation

(1–12 hours after initial access)

Once attackers gain initial SSO access, the compromise escalates rapidly.

2.1 New MFA Enrollment

The attacker immediately enrolls new MFA methods, ensuring uninterrupted access.

2.2 Privilege Escalation

Operators attempt:

- Password resets for higher-privileged accounts
- Targeted phishing of identity admins
- Social engineering of helpdesk escalations
- Exploiting legacy accounts lacking MFA

2.3 OAuth Application Abuse

Attackers create or hijack enterprise applications with elevated API permissions, enabling:

- Persistence beyond credential resets
- Silent data enumeration
- Directory manipulation
- Exfiltration of email and files

2.4 Conditional Access Tampering

They modify:

- MFA policies
- Location-based restrictions
- Device trust requirements

This undermines nearly all “front-door” identity controls.

During this phase, attackers often achieve **global administrator privileges within just a few hours**.

Phase 3 — Transition to On-Premise & Environment Mapping

(Within 12–24 hours of cloud compromise)

This is the point where operational control shifts from Scattered Spider to DragonForce affiliates.

3.1 Cloud-to-On-Prem Pivot

Affiliates establish access via:

- VPN enrollment using compromised identity
- Azure AD–joined device access
- Okta ASA (server access)
- Identity-based SSO into internal portals

3.2 Deploying Remote Access Tools

Common tools deployed:

- AnyDesk
- ScreenConnect
- TeamViewer
- Atera
- Splashtop

These tools create persistent footholds that survive resets and restarts.

3.3 Enumeration of Critical Assets

DragonForce affiliates map:

- Domain controllers
- File servers
- Backup repositories
- EDR servers
- Business-critical application servers
- Database clusters
- Financial systems
- HR systems
- Engineering resources

This reconnaissance phase is often completed in **under 6 hours**.

Phase 4 — Credential Harvesting & Lateral Movement

(24–48 hours after initial access)

DragonForce operators accelerate activity significantly once inside the domain environment.

4.1 Credential Theft

Using tools such as:

- Mimikatz
- LSASS dumpers
- Token impersonation frameworks
- DCSync reconnaissance
- ADExplorer or BloodHound

they extract:

- Domain admin credentials
- Service account keys
- Kerberos tickets
- Hard-coded configuration credentials

4.2 Lateral Movement

Operators move laterally using:

- RDP
- SMB
- WMI
- PsExec

Because they possess valid credentials, their activity blends with legitimate administrative operations.

4.3 Network-Wide Access Expansion

By mid-phase, attackers have:

- Domain admin level control
- Full visibility of the network
- Persistence via RMM tools
- Redundant cloud identity persistence

At this point, containment becomes extremely challenging.

Phase 5 — Data Discovery, Staging & Exfiltration

(48–96 hours after initial access)

Once inside the environment with administrative privileges, attackers shift focus toward monetizable data.

5.1 Discovery of High-Value Data

Targeted data typically includes:

- PII/PHI
- Intellectual property
- HR records
- Legal documents
- Customer database exports
- Financial data
- Email archives
- Server configuration files
- Cybersecurity documentation

5.2 Staging

Data is collected on intermediate systems to:

- Compress datasets
- Organize by category
- Obfuscate detection patterns

5.3 Exfiltration

Using tools such as:

- RClone
- MegaCMD
- AWS/GCP/Azure CLI
- Custom exfiltration binaries

Attackers exfiltrate **hundreds of gigabytes or terabytes** of data.

Exfiltration often occurs during:

- Nights
- Weekends
- Public holidays
- Maintenance windows

to reduce detection likelihood.

Phase 6 — Ransomware Deployment Preparation

(Often within 72–120 hours)

Just before detonation, DragonForce affiliates prepare the environment.

6.1 Backup System Neutralization

They target:

- Veeam servers
- Hypervisor snapshots
- Cloud backup containers
- On-site backups
- Tape libraries (where accessible)

6.2 EDR and Logging Suppression

Affiliates attempt to:

- Uninstall EDR agents
- Tamper with registry keys
- Disable security services
- Modify GPOs to neutralize protections
- Disable log retention (Azure, Okta, AD, local logs)

6.3 Mass Deployment Setup

They prepare deployment paths through:

- GPO
- PsExec
- WMI
- Intune
- RMM tools

Once everything is staged, the attackers synchronize the next phase.

Phase 7 — Ransomware Detonation

(Typically 4–7 days after first helpdesk interaction)

The ransomware detonation is coordinated to maximize damage.

7.1 Simultaneous Encryption

DragonForce encryptors are:

- Multi-threaded
- Highly optimized
- Selective (avoid OS destruction)
- Capable of very rapid encryption across mapped drives

The result is often **near-total infrastructure disruption** within minutes to hours.

7.2 Ransom Note Deployment

Notes are placed:

- On desktops
- In file shares
- On servers
- In critical directories

Instructions direct victims to Tor-based negotiation sites.

Phase 8 — Extortion & Operational Pressure

(Post-encryption, lasting days to weeks)

DragonForce employs a layered pressure campaign.

8.1 Leak-Site Publication

Threat actors post:

- Victim name
- Sample stolen data
- Countdown clocks

to increase reputational pressure.

8.2 Direct Pressure

Attackers may:

- Email executives
- Contact customers
- Reach out to media
- Launch DDoS attacks
- Release more data in stages

Their goal is clear: maximize psychological and operational pressure to induce payment.

Phase 9 — Post-Incident Risks & Re-entry Attempts

(Weeks to months post-breach)

Even after containment, organizations face ongoing risks.

9.1 Persistence Remnants

Attackers may leave behind:

- Malicious OAuth apps
- Hidden global admin accounts
- Rogue RMM agents
- Backdoor registry keys
- Manipulated Conditional Access rules

9.2 Credential Reuse

Exfiltrated credentials may enable:

- Follow-on attacks
- Secondary extortion campaigns
- Access resale on criminal forums

9.3 Data Weaponization

Leaked data may be:

- Sold
- Recycled
- Used for phishing
- Repackaged into new extortion attempts

The timeline doesn't end at encryption; long-term exposure persists indefinitely.

Conclusion

The DragonForce–Scattered Spider attack timeline is defined by:

- **Acceleration** — hours instead of weeks
- **Identity compromise as the catalyst**
- **Cloud and on-prem fusion**
- **Simultaneous data theft and system disruption**
- **Persistent extortion and long-term risk**

This timeline underscores a critical reality: by the time ransomware detonates, the true breach has already occurred days earlier, at the identity layer, where defenders rarely detect it in time.

MITRE / ATT&CK Mapping

This section provides a detailed MITRE ATT&CK mapping for the combined DragonForce and Scattered Spider intrusion model. Unlike single-actor mappings, this threat ecosystem spans *two coordinated threat entities*, each specializing in distinct phases of the kill chain, resulting in a broad and complex TTP footprint across multiple ATT&CK tactics.

Scattered Spider primarily dominates early-stage tactics (Reconnaissance, Initial Access, Social Engineering, Credential Access, and Persistence in cloud identity). DragonForce affiliates take over mid- to late-stage activity (Privilege Escalation, Lateral Movement, Exfiltration, Impact). The handoff between these stages forms a unique compound attack pattern that significantly complicates detection, attribution, and timely response.

What follows is a comprehensive ATT&CK-aligned breakdown detailing the techniques observed or strongly associated with this collaboration, along with contextual analysis explaining *how* and *why* each technique is applied within the broader campaign.

1. Reconnaissance (TA0043)

Scattered Spider invests heavily in reconnaissance, using both automated scraping and manual research.

T1589 – Gather Victim Identity Information

Operators collect names, job roles, emails, internal jargon, reporting structures, and helpdesk processes from OSINT sources. This intelligence enables highly persuasive impersonation, especially in voice-based social engineering.

T1592 – Gather Victim Org Information

Scattered Spider builds a full organizational profile, noting:

- Identity provider type (Azure AD, Okta)
- Cloud footprint
- MFA policies
- Technology stack from job posts
- Outsourced helpdesk vendors
- Device management systems

This allows them to tailor pretexts precisely to the target.

T1598 – Phishing for Information

Though the campaign relies more on vishing, SMS phishing is also used to confirm phone numbers, MFA types, and whether targets respond to mobile prompts.

2. Resource Development (TA0042)

Preparation before execution is essential for both actors.

T1583 – Acquire Infrastructure

Scattered Spider deploys:

- VoIP infrastructure
- Spoofable call IDs
- SMS gateways
- VPN exit nodes
- Disposable email accounts
- Burner domains designed to mimic IT support

DragonForce sets up encryption infrastructure, including:

- Leak sites
- TOR negotiation portals
- Payment portals
- Malware staging servers

T1587 – Develop Capabilities

DragonForce develops and maintains:

- Multi-threaded encryption binaries
- Tools for EDR tampering
- Scripts for automated lateral movement
- Exfiltration tooling leveraging cloud APIs

Affiliates may also weaponize legitimate RMM platforms.

3. Initial Access (TA0001)

The partnership's defining attribute is Scattered Spider's identity-focused entry methods.

T1566.003 – Phishing (Spearphishing via Phone/Vishing)

High-quality voice impersonation is used to trick helpdesk agents into:

- Resetting MFA
- Changing phone numbers
- Approving authenticator enrollment

This is the core access vector.

T1078 – Valid Accounts

The goal of social engineering is to obtain *legitimate* account access, making this technique central to the campaign. Attackers circumvent nearly all traditional detection mechanisms by using accounts as intended.

T1110 – Brute Force (Knowledge-Based MFA Abuse)

Not brute force in its classic sense, but “MFA fatigue” attacks (push bombing) fall under ATT&CK’s credential-related brute-force framework. Attackers repeatedly trigger MFA prompts until users approve.

T1091 – Replication Through Removable Media (Indirect via SIM Swaps)

Applicable when SIM swapping is used to intercept SMS MFA codes—effectively gaining control of a device used for authentication.

4. Execution (TA0002)

Execution is often minimal in the early stages due to the reliance on valid credentials. After the handoff to DragonForce, execution becomes more traditional.

T1059 – Command and Scripting Interpreter

DragonForce affiliates use PowerShell and CMD scripts for:

- Reconnaissance
- Credential dumping
- Lateral movement
- Exfiltration setup

T1204 – User Execution

In rare cases, Scattered Spider induces users to run IT-support-themed files, but this is less common in this campaign.

T1106 – Native API Usage

Ransomware encryptors use Windows APIs for optimized encryption and VSS manipulation.

5. Persistence (TA0003)

T1098 – Account Manipulation

Scattered Spider frequently modifies user accounts to embed persistence:

- Adding MFA devices
- Changing primary phone numbers
- Resetting authentication methods

T1136.002 – Create Account (Cloud Account)

Operators often create malicious global admin accounts:

- “BackupAdmin”
- “SupportAccount”
- “SystemOperations”

These are easily overlooked among legitimate privileged accounts.

T1098.004 – OAuth Token Persistence

One of the most dangerous techniques. Attackers:

- Create OAuth apps
- Grant broad API permissions
- Approve long-lived refresh tokens

Even if passwords reset, OAuth persistence remains unless manually audited.

T1547 – Boot or Logon Autostart Execution

On endpoints, DragonForce implants RMM tools that start automatically to maintain remote access.

6. Privilege Escalation (TA0004)

T1068 – Exploitation for Privilege Escalation

Less common here, but occasionally used if legacy on-prem systems contain known vulnerabilities.

T1078.004 – Valid Accounts: Cloud Accounts

Escalation is most often achieved by compromising high-privilege cloud users through helpdesk manipulation.

T1543 – Create or Modify System Process

Used to install persistence via scheduled tasks or services on compromised servers.

7. Defense Evasion (TA0005)

T1562 – Impair Defenses

DragonForce often disables:

- EDR protections
- Antivirus
- Windows Defender
- Logging services

T1070 – Indicator Removal on Host

Attackers clear Windows event logs, security logs, and PowerShell transcripts.

T1027 – Obfuscated Files or Information

Scripts used for exfiltration and movement are often encoded or packed.

T1036 – Masquerading

Examples:

- RMM tools renamed to `svchost.exe`
- Newly created admin accounts named similarly to legitimate ones

T1578 – Modify Cloud Compute Infrastructure

Attackers may modify Azure VM metadata, disable logging, or alter retention policies.

8. Credential Access (TA0006)

T1110 – Password Guessing / MFA Abuse

MFA fatigue is the signature technique here.

T1556 – Modify Authentication Process (MFA Manipulation)

Scattered Spider manipulates:

- MFA enrollment
- Phone number verification
- Authenticator app approvals

T1003 – OS Credential Dumping

Once DragonForce affiliates gain on-prem access, LSASS dumping is standard.

T1552 – Unsecured Credentials

The group targets:

- Password managers
- Configuration files
- Cloud credentials
- VPN configs

T1539 – Steal Web Session Cookie

Cloud admin cookies allow attackers to bypass additional security controls.

9. Discovery (TA0007)

T1087 – Account Discovery

Used to identify high-privilege users.

T1482 – Domain Trust Discovery

Attackers map trust paths and nested privileges.

T1046 – Network Service Scanning

Used sparingly because attackers often have direct admin visibility.

T1018 – Remote System Discovery

Enumeration of servers, clusters, hypervisors, backup repositories.

T1069 – Permission Groups Discovery

Essential for identifying domain admin pathways.

10. Lateral Movement (TA0008)

T1021.001 – Remote Services: RDP

A primary movement channel for DragonForce affiliates.

T1021.002 – SMB/Windows Admin Shares

Used for file transfer and lateral deployment.

T1047 – Windows Management Instrumentation (WMI)

Used to execute commands remotely.

T1563 – Remote Service Session Hijacking

Occurs when token impersonation is used.

T1570 – Lateral Tool Transfer

Attackers move ransomware binaries across the network using native tools.

11. Collection (TA0009)

T1114 – Email Collection

Exfiltration of entire mailboxes using Graph API (enabled via OAuth persistence).

T1005 – Data from Local System

Harvesting documents, configuration files, credentials.

T1039 – Data from Network Shares

Large-scale targeting of file servers, NAS devices.

T1119 – Automated Collection

Scripts automatically crawl shares for high-value data.

12. Command & Control (TA0011)

T1090 – Proxy Usage

Attackers route communications through VPN nodes, TOR, or cloud relays.

T1572 – Protocol Tunneling

Useful for bypassing firewalls and exfiltrating data covertly.

T1219 – Remote Access Software

RMM tools function as C2 implants.

13. Exfiltration (TA0010)

T1041 – Exfiltration Over C2 Channel

Environments with weak egress filtering fall victim to direct server-to-VPS exfiltration.

T1567.002 – Exfiltration to Cloud Storage

One of the most heavily used techniques:

- RClone → Mega
- AWS CLI → S3 buckets
- Azure Storage exports
- Dropbox API uploads

T1048 – Exfiltration Over Alternative Protocol

Attackers sometimes use SFTP or FTP over TLS to blend in.

14. Impact (TA0040)

T1486 – Data Encryption for Impact

DragonForce encryptors are:

- Multi-threaded
- Selective
- Highly efficient

T1490 – Inhibit System Recovery

Shadow copy deletion (`vssadmin`, `wmic`, `diskshadow`).

T1489 – Service Stop

Stopping databases, VSS, backup agents, AV services.

T1499 – Endpoint DoS (DDoS as Extortion)

Some affiliates use DDoS as pressure.

T1531 – Account Access Removal

Attackers may disable legitimate accounts before encryption.

Conclusion

The DragonForce–Scattered Spider collaboration results in one of the most expansive ATT&CK footprints among contemporary ransomware ecosystems. The combination of:

- **identity-based initial access**,
- **cloud-centric persistence**,
- **legitimate-tool-driven lateral movement**, and
- **highly optimized encryption operations**

creates a threat profile that spans virtually every MITRE ATT&CK tactic.

This partnership is especially dangerous because the earliest stages—where detection matters most—are dominated by **legitimate activity**, blending seamlessly into expected administrative workflows and making early detection inherently difficult.

Indicators of Compromise (IOCs)

This section provides a comprehensive overview of Indicators of Compromise associated with the combined DragonForce–Scattered Spider intrusion model. Because this ecosystem relies heavily on **valid credentials**, **identity abuse**, and **legitimate tools**, traditional static IOCs (hashes, domains, file names) have limited longevity and detection value. Instead, defenders must correlate **behavioral, identity-centric, and infrastructure-based indicators** to detect malicious activity earlier in the kill chain.

The following IOCs represent categories, patterns, and specific examples observed across multiple incidents attributed to or consistent with DragonForce ransomware affiliates and Scattered Spider operators. This list is intentionally broad, acknowledging that attackers frequently rotate infrastructure and tooling.

1. Identity-Based Indicators (High Value)

Identity IOCs are the most critical early-warning signals in this campaign. They often appear **hours or days before** ransomware deployment and represent the earliest reliable detection opportunities.

1.1 Suspicious MFA Enrollment Events

Look for:

- New MFA methods added during off-hours
- Enrollment of authentication apps from unusual device IDs
- Phone numbers linked to foreign carriers or VoIP providers
- MFA additions occurring directly after failed login attempts
- Users apparently completing MFA despite never interacting with their device

Common patterns:

- MFA added to accounts belonging to high-value identities (IT staff, executives, admins).
- Enrollment done via helpdesk-initiated workflows.
- Same VoIP number or device ID added to multiple users' MFA.

1.2 Unauthorized Reset or Removal of MFA

Red flags include:

- "MFA reset by administrator" actions performed by unexpected helpdesk accounts
- Removal of all existing MFA methods followed immediately by new enrollment
- Account unlock/recovery workflows executed too quickly (within minutes of first user contact)

1.3 Creation of Suspicious Cloud Admin Accounts

Common malicious account names used by Scattered Spider and affiliates include:

- "BackupAdmin", "SystemOps", "HelpdeskAdmin", "ITSupport", "SecurityAdmin"
- Variants of legitimate employee names with small modifications

IOCs include:

- Newly created Global Admin accounts
- Admin accounts created from IP ranges not previously associated with the helpdesk or identity team
- Admin accounts created outside business hours

1.4 Malicious OAuth Applications

One of the most critical persistent IOCs.

Look for:

- Enterprise apps created unexpectedly
- Apps with *recently granted* high-privilege permissions (Directory.ReadWrite.All, Policy.ReadWrite.ConditionalAccess, Files.ReadWrite.All, Mail.Read, offline_access)
- OAuth apps approved by compromised admin accounts
- Applications that maintain OAuth refresh tokens even after user password resets

1.5 Conditional Access Policy Modifications

These changes are often subtle indicators of active compromise:

- CA policies disabled or removed
- Additions allowing sign-ins from “all countries” instead of restricted geos
- Policies excluding specific user accounts (e.g., the attacker’s admin account)
- Enforcement mode switched to report-only

1.6 Unusual Sign-in Patterns

Key IOCs include:

- Successful MFA from unexpected IPs
- First-time MFA from a device never registered before
- Sign-ins from multiple countries or regions within minutes
- Sign-ins overlapping with ongoing helpdesk interactions
- Anonymous or strongly anonymized IP ranges (Proton, Mullvad, cloud VPN nodes)

2. Cloud Infrastructure IOCs

The attackers make significant changes in cloud platforms such as Azure, Okta, AWS, or Google Workspace.

2.1 Suspicious Azure AD Events

Detected IOCs include:

- Service principals created without documented business purpose
- App role assignments increasing in privilege
- Global admin role assignments outside normal change-management windows
- Token lifetime policies modified to increase persistence
- Audit logs disabled or retention reduced

2.2 Okta Indicators

Common IOCs:

- Unexpected MFA factor enrollments
- Newly added WebAuthn/U2F keys
- New admin assignments to users without prior admin roles
- Login events from Tor exit nodes or cloud-hosting ranges
- API tokens created or elevated permissions applied to existing tokens

2.3 Cloud Storage Abuse

Attackers frequently exfiltrate data to cloud storage:

- Mega.nz endpoints
- Dropbox API activity
- Wasabi S3 buckets
- Azure Blob containers created by unknown identities

Look for:

- Large PUT operations from administrative accounts
- Data exfil during nights/weekends

3. On-Premises IOCs

Once DragonForce affiliates pivot to on-prem, their activity becomes far more detectable—though much later in the intrusion.

3.1 RMM Tool Installation and Abuse

Tools commonly deployed:

- **AnyDesk**
- **ScreenConnect**
- **TeamViewer**
- **Atera**
- **Splashtop**
- **DWService**

File/path IOCs include:

- AnyDesk installed on servers where RMM is not normally used
- Temporary executables dropped in `%ProgramData%` or `%Temp%`
- Services created pointing to RMM executables

Behavioral IOCs:

- RMM sessions initiated from abnormal geolocations
- RMM installed and then immediately used for privilege escalation
- Multiple hosts installing the same RMM within minutes

3.2 Credential Dumping Activity

Key indicators:

- LSASS access events (`Event ID 4656`, handle access)
- `procdump.exe` or renamed variants targeting LSASS
- Presence of Mimikatz artifacts ("mimi", "kiwi", "sekurlsa")
- Registry/System hive exports

3.3 Lateral Movement Indicators

Tools and actions to monitor:

- PsExec service creation (`PSEXESVC`)
- WMI execution logs
- Unusual RDP logons:
  - Multiple privileged logons across servers
  - Logons from workstations or accounts that do not typically access servers
- SMB admin share access (IPC$, C$)

3.4 GPO Manipulation

Before deploying ransomware, attackers often modify GPOs.

IOCs include:

- New or edited GPO startup scripts
- GPOs modified by accounts not associated with IT ops
- Mass host restarts initiated via GPO

4. File System & Host-Based IOCs

4.1 Ransomware-related Files

DragonForce ransom notes may include variations such as:

- `README-RECOVER.txt`
- `DRAGONFORCE-HELP.txt`
- `RECOVERY-INSTRUCTIONS.txt`

File patterns:

- Dropped in every directory
- Identical file hash across multiple hosts
- Contains links to Tor negotiations sites

4.2 Pre-Encryption Commands

Common attacker commands (PowerShell/CMD/WMIC):

- `vssadmin delete shadows /all /quiet`
- `wmic shadowcopy delete`
- `diskshadow /s script.txt`

- `net stop winrm`
- `net stop VSS`
- `bcdedit /set {default} recoveryenabled no`
- `wmic path AntiVirusProduct` modifications

These commands indicate imminent ransomware detonation.

4.3 File and Directory Indicators

Staging directories include:

- `%TEMP%\tmp1234`
- `%ProgramData%\RClone`
- `%ProgramData%\BackupOps`
- `%AppData%\SysSupport`

Look for:

- Recently created ZIP archives
- RClone configuration files (`rclone.conf`)
- Large temporary files (>10GB)

5. Network IOCs

Although identity abuse reduces reliance on C2 servers, network indicators still play a role.

5.1 Exfiltration Endpoints

Common exfil services:

- `mega.nz`
- `mega.io`
- `dropboxapi.com`
- `s3.amazonaws.com`
- Wasabi S3 endpoints
- VPS ranges from:
    - Contabo
    - DigitalOcean
    - OVH
    - Hetzner
    - Vultr

Look for:

- Large PUT/POST operations
- High outbound HTTPS traffic from servers that usually have low egress

5.2 TOR Indicators

Tor exit nodes sometimes appear in authentication logs.

Indicators include:

- IPs from known Tor ranges
- Logons from IPs with reverse DNS patterns:
  - “exit-relay”
  - “tor-exit”
  - “nohost”

5.3 Suspicious VPN Activity

In organizations using Azure VPN or legacy VPN:

- VPN sign-ins from impossible travel locations
- Rapid connect-disconnect cycles
- VPN logins by service accounts

6. Ransomware Payload IOCs

DragonForce affiliates frequently rotate payloads, but patterns exist.

6.1 Payload Characteristics

- 64-bit Windows PE binaries
- Packed with UPX or custom packers
- 200–600 KB typical size
- AV labels sometimes overlap with other families (affiliates reuse code)

6.2 Pre-Execution Checks

Some samples:

- Avoid encryption of OS-critical files
- Skip certain directories
- Use multithreading (via WinAPI)
- Identify drive mappings

6.3 Encryption Behavior

DragonForce encryptors often:

- Use AES or ChaCha20
- Append unique victim-specific extensions
- Write ransom notes per-directory
- Delete shadow copies
- Terminate processes (databases, backup agents)

7. Behavioral IOCs (Most Important Category)

Because static IOCs change rapidly, behavioral indicators are the most reliable markers of compromise. These include:

7.1 Identity Abuse Patterns

- MFA reset + admin role assignment within minutes
- Impossible travel followed by admin activity
- OAuth application creation followed by Graph API access
- Changes to Conditional Access policies outside change windows

7.2 Exfiltration Behavior

- RClone spawning under SYSTEM or admin accounts
- Use of compressed archives >10GB
- Consecutive outbound connections to cloud storage domains
- Unusual volume of file reads from file servers

7.3 Network Lateral Movement

- PsExec service creation
- Repeated RDP session attempts across servers
- SMB access to C$ shares across multiple hosts

7.4 Backup Tampering

- Veeam job deletion
- Shadow copy removal
- Backup repository formatting or corruption

These behaviors strongly correlate with ransomware preparations.

Conclusion

The IOC landscape for DragonForce + Scattered Spider is broad, dynamic, and heavily weighted toward **behavioral and identity-based signals** rather than static artifacts. This reflects their operational methodology, in which:

- Initial access relies on **valid credentials**,
- Persistence relies on **identity manipulation**,
- Movement leverages **legitimate IT tools**, and
- Impact relies on **scripted, predictable ransomware stages**.

Detecting early-stage activity requires continuous monitoring of cloud identity systems, helpdesk workflows, OAuth applications, and administrative actions—far earlier than where traditional malware-focused detection provides visibility.

Recommended Response Steps (Operational)

Tier 0 — Immediate (Hours)

- Block attacker persistence by removing unauthorized MFA devices, OAuth apps, and new admin accounts.
- Revoke and rotate all privileged credentials (SSO, service accounts, RMM).
- Isolate any host running unapproved RMM tools.
- Block identified exfil endpoints at firewall and proxy.
- Initiate forensic capture of affected identity logs, server logs, and endpoint artifacts.

Tier 1 — Short Term (24–72 Hours)

- Conduct AD and SSO audit for privilege escalation paths.
- Review helpdesk logs for manipulated tickets or impersonation.
- Identify systems involved in lateral movement and deploy containment.
- Validate backup integrity and ensure offline copies exist.
- Assess and rebuild critical services from known-good baselines.

Tier 2 — Medium Term (Days → Weeks)

- Implement identity hardening: phishing-resistant MFA, conditional access, admin separation.
- Deploy detection rules for RMM misuse, OAuth abuse, and anomalous cloud sign-in patterns.
- Conduct organization-wide credential hygiene and local admin scrubbing.
- Enhance network segmentation around domain controllers and backup environments.

Structural Recommendations

The DragonForce–Scattered Spider intrusion model exposes fundamental weaknesses in enterprise identity, support workflows, cloud governance, and network architecture. Addressing these weaknesses requires more than tactical fixes; it demands **structural, strategic, and architectural improvements** to ensure long-term resilience.

The following recommendations focus on **systemic hardening**, recognizing that identity-centric intrusions cannot be mitigated through endpoint defences alone. These recommendations aim to disrupt the attacker's operational sequence at the earliest possible phase while strengthening the organisation's ability to detect, respond to, and recover from future incidents.

1. Identity Architecture Hardening

Identity is the single point of failure used by Scattered Spider. Therefore, the most important structural recommendation is to modernize, harden, and re-architect identity systems in a way that eliminates the pathways exploited during these attacks.

1.1 Adopt Phishing-Resistant MFA Across All Privileged Accounts

Traditional MFA using SMS, phone calls, or app-based push notifications is vulnerable to:

- SIM swapping
- Helpdesk-based reset abuse
- Push bombing

- Social engineering impersonation

Organizations must move to **phishing-resistant MFA** for all privileged accounts and, ideally, for all users:

- FIDO2 hardware keys (YubiKey, Feitian, etc.)
- Windows Hello for Business (certificate-backed)
- Smartcard / PIV
- WebAuthn platform authenticators

This single change dramatically reduces the efficacy of Scattered Spider's initial access techniques.

1.2 Enforce Tiered and Segmented Administrative Roles

Privileged access roles must not be:

- Overprovisioned
- Granted to daily-use accounts
- Inherited through nested groups
- Mismanaged through emergency access processes

Implement:

- **Tier 0 / Tier 1 / Tier 2 administrative separation**
- **Privileged Access Workstations (PAWs)** for identity admin tasks
- **Just-in-time (JIT)** access via Azure Privileged Identity Management or SaaS equivalents
- **Just-enough-access (JEA)** tooling for constrained privilege

Stolen user credentials must not automatically grant domain-level access.

1.3 Audit & Restrict MFA Reset Workflows

Helpdesk MFA reset procedures represent one of the highest-risk structural weaknesses exploited in these attacks. Organizations must:

- Require **two-party approval** for all MFA resets involving privileged users
- Disallow phone-based verification using caller ID
- Enforce **call-back to numbers verified from HR or asset inventory**
- Prohibit reset approval based on knowledge-based answers or easily searchable information
- Log all MFA reset events centrally
- Apply behavioural analytics on reset patterns (volume, timing, operator ID)

Internal staff must not be able to reset MFA based solely on verbal interactions.

1.4 Implement Conditional Access Baselines With Hard Enforcement

Conditional Access (CA) must be used to ensure identity-based detection and protection:

- Block legacy authentication globally
- Enforce MFA for all users
- Restrict sign-in to trusted locations or device compliance states
- Require compliant devices for admin portal access

- Enforce “require phishing-resistant MFA” for admin roles
- Disallow access from anonymizing services (TOR, VPN-as-a-service)

These policies must be **enforced**, not left in “report-only” mode.

1.5 Install Monitoring for Malicious OAuth and Enterprise Application Activity

This threat model relies heavily on malicious OAuth apps for persistence. Organizations must:

- Enable alerting on *new enterprise apps* being added
- Alert on *high-privilege Graph permissions* assigned to apps
- Enforce admin approval workflows for app consent
- Disable user consent for apps unless absolutely required
- Periodically rotate application secrets and certificates

OAuth persistence is one of the most overlooked long-term risks.

2. Helpdesk Workflow Hardening

Scattered Spider’s primary advantage is their ability to exploit helpdesk agents. Structural improvements must redefine the helpdesk’s authority and verification process.

2.1 Zero-Trust Helpdesk Procedures

Adopt a “trust nothing without verification” principle:

- No resets based on employee name, role, or email alone
- No resets for employees who cannot respond from verified channels
- Mandatory callback to a *previously verified* internal number
- Multichannel verification (HR system, MDM records, identity logs)
- Disable helpdesk privileges on personal accounts

Helpdesk teams must have **limited authority** to make identity-impacting changes.

2.2 Helpdesk Segmentation for Privileged Accounts

Privileged accounts should not be managed by the general helpdesk. Implement:

- A separate “Identity Operations Team”
- Higher verification thresholds for admin users
- Ticket-based approvals requiring 2–3 approvers
- Mandatory identity re-validation for admin accounts

This reduces the risk of social engineering pivoting directly into the admin plane.

2.3 Mandatory Recording of Support Calls and Audit Trails

All MFA resets, password resets, and privileged operations must:

- Be logged

- Include operator identity
- Contain a recorded audio transcript (where legally permitted)
- Include justification categories
- Be monitored for anomalies

This data is crucial for forensic reconstruction and proactive alerting.

3. Cloud Governance & Security Architecture

Because attackers target cloud platforms first, the cloud governance model must mature accordingly.

3.1 Enforce Least Privilege Across Cloud Roles

Review all:

- Global Admins
- Application Admins
- Cloud App Security roles
- Directory Readers/Writers
- Security Administrators
- Intune Administrators

Any unnecessary privilege creates a breach amplification vector.

3.2 Harden Logging & Audit Infrastructure

Attackers often disable or tamper with cloud logging. Structural fixes include:

- Enforce immutable audit logs (Azure immutable logging, retention locks)
- Enable logging to external SIEM that attackers cannot tamper with
- Implement backup log storage in a physically/separated tenant
- Alert on logging modifications or policy changes

Logs must be secured from the attackers themselves.

3.3 Deploy Real-Time Identity Threat Detection

This includes:

- Azure Identity Protection
- Okta ThreatInsight
- Microsoft Defender for Identity
- Cloud access anomaly detection
- Impossible travel alerts
- MFA fatigue rule triggers

Automated responses should be configured where safe.

3.4 Strict Governance for Enterprise Apps & Service Principals

Organizations must:

- Limit app creation to a small group
- Audit apps monthly
- Require justification for elevated permissions
- Remove unused apps aggressively
- Enforce MFA for app management roles

4. Network Segmentation & Zero Trust Architecture

DragonForce affiliates capitalize on lateral movement across flat networks. Eliminating flat network designs is key.

4.1 Segment High-Value Assets

Place the following in isolated, protected network segments:

- Domain controllers
- Backup servers
- Hypervisors
- EDR infrastructure
- Production databases
- Identity infrastructure

Access between segments should require:

- Strong MFA
- Conditional Access
- Just-in-time privilege elevation

4.2 Restrict East/West Traffic

Implement:

- Network microsegmentation
- Software-defined per-app segmentation
- Firewall policies limiting admin protocols
- Disabling SMBv1/v2 where possible
- Blocking interactive logons to servers except for admin PAWs

4.3 Enforce Least-Privilege Service Accounts

Service accounts often have excessive privileges that facilitate lateral movement. Recommendations:

- Rotate passwords frequently
- Convert static accounts to managed service accounts
- Audit delegated permissions
- Remove legacy service accounts

- Require MFA where technically possible

5. Backup Resilience & Ransomware Recovery Architecture

Ransomware operations succeed partly because backups are accessible. Structural improvements must ensure backups are **immutable and isolated**.

5.1 Implement Offline or Air-Gapped Backups

Minimum requirements:

- One backup copy offline
- One copy stored in an immutable object storage bucket
- Segmented backup networks
- No direct trust relationships between production and backup environments

5.2 Harden Backup Management Consoles

- Restrict admin access to PAWs
- Require phishing-resistant MFA
- Disable console access from non-admin subnets
- Rotate repository credentials frequently
- Monitor for backup job deletions or manipulation

5.3 Regular Disaster Recovery Exercises

Perform:

- Full restore drills
- Ransomware tabletop exercises
- Identity rebuild simulations
- Test restoration from offline media

NIST-level maturity requires *tested* recovery, not just configured backup.

6. Remote Access & RMM Governance

RMM tooling is a favourite persistence mechanism for DragonForce. Strong governance is required.

6.1 Create a Strict RMM Allow-List

Only allow:

- Pre-approved RMM tools
- Installed via central deployment
- On pre-approved devices
- Managed through central authentication

Block uncontrolled installation of:

- AnyDesk
- ScreenConnect
- TeamViewer
- Atera
- Splashtop

via:

- Application control (AppLocker, WDAC)
- EDR policy
- Software restriction policies

6.2 Monitor & Alert on RMM Installations

Any new installation of remote access tools must generate a SOC alert. Indicators:

- Rapid installation on multiple hosts
- Installation by non-admin users
- Installation outside business hours

6.3 Enforce Privileged Access for RMM Use

RMM operations must require:

- Admin approval
- Just-in-time access
- Logged session capture

No technician should have unmonitored remote access.

7. Cultural & Organisational Resilience

Security culture and cross-functional operations play a major role in preventing identity-based breaches.

7.1 Role-Based Security Awareness Training

Generic training is ineffective. Instead, create specialized tracks for:

- Helpdesk staff (social engineering resistance)
- Identity administrators
- Cloud security teams
- Executives (executive impersonation awareness)

Each role must understand its unique risks.

7.2 Crisis Communication Protocols

Create pre-approved playbooks for:

- Incident declarations
- Regulator communication
- Customer notifications
- Media handling
- Ransom negotiation decision trees

Disorganized communication compounds downtime.

7.3 Strengthen Cross-Team Collaboration

The identity, SOC, IT, and cloud teams must:

- Conduct joint exercises
- Share telemetry
- Review privileged operations weekly
- Participate in attack simulations

Identity-centric attacks require multidisciplinary response.

8. Long-Term Strategic Architecture

The reality of modern ransomware requires a shift toward architectures designed for **identity compromise survivability**.

8.1 Deploy Identity Threat Detection as a Core SOC Function

Identity logs must be first-class telemetry.

8.2 Build Cloud-First Incident Response Playbooks

Ensure IR playbooks include:

- Cloud identity forensics
- OAuth persistence analysis
- Conditional Access rollback
- Azure AD evidence preservation

8.3 Adopt a Zero-Trust Maturity Roadmap

Zero Trust is no longer optional; it is the only sustainable long-term approach against identity-centric attacks.

Conclusion

Structural recommendations cannot be limited to endpoint or malware controls. The DragonForce–Scattered Spider model demonstrates a fundamental truth:
Identity is the new ransomware perimeter, and attackers exploit the weakest cultural, procedural, and architectural seams long before they deploy ransomware.

Implementing these structural improvements will:

- Stop attackers at the identity layer
- Limit lateral movement
- Preserve forensic integrity
- Protect backup survivability
- Harden cloud environments
- Reduce helpdesk-driven compromise
- Create a culture capable of resisting social engineering

These recommendations provide the foundation required to mitigate the increasingly advanced, human-driven intrusion models employed by the DragonForce–Scattered Spider ecosystem.

About Ransomwared

Ransomwared is a European-based cybersecurity initiative committed to protecting organizations against the evolving threat of ransomware. Our mission is to **disrupt the economics of cyber extortion** by providing intelligence, technology, and rapid response capabilities that empower defenders to outpace attackers.

At the core of our work is a **next-generation, AI-enhanced, autonomous SOC (Security Operations Center)** that operates 24/7. This SOC continuously ingests global threat intelligence, analyzes attacker behaviors, and autonomously correlates patterns against enterprise telemetry. By leveraging **machine learning models trained on ransomware TTPs**—including those used by groups such as **Akira**—we provide real-time detection, predictive defense, and automated containment actions.

How We Stay Ahead of Threats Like Akira

- **AI-Driven Threat Intelligence**: Our models are continuously refined with data from ransomware campaigns, CVE exploit chains, and underground ecosystems, enabling proactive detection of new attack variants.
- **24/7 Autonomous SOC**: Operating around the clock, our SOC doesn't just monitor—it autonomously correlates anomalies, isolates compromised endpoints, and enforces adaptive security controls in real time.
- **Behavioral Defense**: By mapping techniques to **MITRE ATT&CK**, we detect ransomware campaigns even when adversaries change infrastructure, binaries, or ransom note formats.
- **Continuous Learning**: Every incident enriches our AI and SOC capabilities, strengthening defenses not only for individual organizations but across the entire Ransomwared community.

Our Broader Mission

- **Threat Intelligence Reports**: In-depth CTI reporting (like this Akira analysis) that provides technical, operational, and strategic insights.
- **Vulnerability-to-Exploit Correlation**: Automated pipelines that link CVEs with ransomware campaigns within hours of disclosure.
- **Resilience by Design**: Guidance for implementing Zero Trust, immutable backups, and robust incident response frameworks.

Our Vision

We believe the fight against ransomware will not be won by reacting to incidents, but by **out-automating adversaries**. By combining advanced AI, a 24/7 autonomous SOC, and a culture of open intelligence sharing, Ransomwared helps organizations move from reactive defense to **proactive resilience**—ensuring that ransomware groups like Akira lose their strategic advantage.

For more information, resources, and access to our threat intelligence services, visit:
🌐 **www.ransomwared.eu**