

# Threat Action Profile: Red Dune Collective

---

## **Origin:** Mars (suspected Martian cyber-activist group)

Red Dune Collective is believed to originate from Mars-based territories, operating as a sophisticated cyber-activist organization with strong ties to Martian independence movements.

Intelligence suggests the group consists of former Mars Colonial Administration IT personnel and disgruntled mining technicians who possess intimate knowledge of interplanetary industrial systems.

Their operations demonstrate advanced understanding of both Earth and off-world infrastructure, indicating possible state-level support or coordination with Martian separatist factions.

## **Target:** Space mining companies (Earth and Lunar operations)

The collective specifically targets space mining corporations operating across Earth-Moon industrial corridors, with particular focus on asteroid belt extraction operations and Lunar helium-3 facilities.

Their victim profile includes major conglomerates involved in rare earth element extraction, water ice harvesting, and platinum group metal mining.

Recent campaigns have expanded to include supply chain attacks against Earth-based manufacturers of space mining equipment and orbital logistics companies that support off-world operations.

## **Motivation:** Economic disruption, resource theft, sabotage

Red Dune Collective's primary motivation centers on destabilizing the Earth-dominated space mining economy through coordinated cyber operations designed to redistribute wealth and resources toward Mars-based colonies.

Their activities include intellectual property theft of mining technologies, financial fraud targeting commodity trading systems, and operational sabotage of critical mining infrastructure.

The group appears motivated by ideological opposition to Earth's colonial exploitation of space resources and seeks to establish Mars as an independent economic power in the solar system.

## **Government Relations:** No official Martian government support

Intelligence assessments indicate that Red Dune Collective operates independently without endorsement or support from the official Martian Colonial Government (MCG).

The MCG has publicly condemned the group's activities and has cooperated with Earth-based law enforcement agencies in several joint investigations.

However, the collective continues to exploit legal and jurisdictional gaps between Earth and Martian territories, making prosecution difficult despite official government disapproval from both planetary administrations.

## Example Dropped Files & Hashes

File Name	Purpose	SHA256 Hash	SHA1 Hash
marsminer.exe	Initial access loader	3a1f2b6e8c9d4e5f7a2b1c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b0c1d2e3f	1a2b3c4d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b
redshift.dll	Credential stealer	7b8c9d0e1f2a3b4c5d6e7f8a9b0c1d2e3f4a5b6c7d8e9f0a1b2c3d4e5f6a7b8c	2b3c4d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b1c
commsat.ps1	C2 beacon script	5d6e7f8a9b0c1d2e3f4a5b6c7d8e9f0a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e	3c4d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b1c2d

## MITRE ATT&CK TTPs

Red Dune Collective typically gains initial access through spearphishing attachments and supply chain compromise techniques.

Once inside, they execute malicious code using PowerShell and rely on user execution of malicious files.

For persistence, they employ DLL search order hijacking and scheduled tasks. The group escalates privileges through exploitation techniques and valid account abuse.

They evade detection with embedded payloads and renaming legitimate utilities. Credential access is achieved through credential dumping and input capture methods.

Their discovery phase involves system information gathering and network service scanning. Lateral movement occurs via SMB/Windows admin shares and remote desktop protocol.

Command and control is maintained through web protocols and custom protocols. Data exfiltration happens over C2 channels and web services.

Finally, they cause impact through data destruction and resource hijacking operations.

## Infrastructure & IOCs

### Known Command & Control Servers:

- mars-mining[.]co (185.243.117.92)
- red-planet-resources[.]net (203.142.67.88)
- asteroid-ops[.]com (174.129.45.201)

### Common User Agents:

- Mozilla/5.0 (MarsOS 2.1; rv:98.0) Gecko/20100101 Firefox/98.0
- RedPlanet-Bot/1.3 (Mining Operations)

### Registry Keys Modified:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MarsUpdate
- HKCU\Software\RedDune\Config

## Defensive Recommendations

### Detection Rules:

- Monitor for processes spawning from unusual locations
- Alert on PowerShell execution with base64 encoding
- Watch for outbound connections to suspicious Mars-themed domains

### Mitigation Strategies:

- Implement application whitelisting
- Deploy EDR solutions with behavioral analysis
- Regular security awareness training focusing on space industry targeting
- Network segmentation between operational technology and IT systems

## Identity History & Group Affiliations

### Previous Names & Aliases:

Red Dune Collective has operated under several identities since its emergence in 2381:

- Mars Liberation Front (MLF) - Original identity focused on political activism
- Phobos Mining Collective - Early cybercriminal operations targeting asteroid mining
- Red Sand Warriors - Brief militant phase before transitioning to cyber operations

### Linked Groups & Relationships:

The collective maintains operational connections with several Earth and off-world threat actors:

- **Titan Shadows** (Saturn moon-based): Intelligence sharing and joint operations targeting outer system mining operations
- **Belt Runners** (Asteroid Belt): Coordination on supply chain attacks and resource theft operations
- **Europa Underground** (Jupiter moon): Shared toolsets and communication infrastructure

### Historical Evolution:

Originally formed as a legitimate mining workers' union on Mars, the group radicalized following the 2379 Olympus Mons Mining Disaster. Leadership transitioned from labor organizers to cybercriminals with the recruitment of former Mars Colonial Administration security personnel.

The group's transformation accelerated after establishing contact with Earth-based hacktivist networks, adopting sophisticated cyber capabilities while maintaining their original resource-focused targeting.

## Conclusion

Red Dune Collective represents a significant and evolving threat to space-based industrial operations throughout the solar system. Their unique combination of insider knowledge of space mining operations, sophisticated cyber capabilities, and ideological motivation makes them particularly dangerous to Earth-Moon economic interests.

The group's evolution from legitimate labor organization to advanced persistent threat demonstrates the complex security challenges facing interplanetary commerce. Their ability to operate across jurisdictional boundaries while maintaining operational security poses ongoing challenges for traditional law

enforcement approaches.

Organizations operating in the space mining sector should prioritize implementing the defensive recommendations outlined in this profile, with particular attention to supply chain security and employee vetting procedures. Continued monitoring of Mars-themed infrastructure and coordination between Earth and Martian security agencies will be essential for disrupting future operations.

As space-based economic activities continue to expand, threat actors like Red Dune Collective will likely inspire similar groups across the outer system. Proactive threat intelligence sharing and enhanced cybersecurity frameworks specific to space industry operations will be critical for maintaining security in this expanding domain.

---

**DISCLAIMER:** This threat action profile was partially generated by AI for educational and exercise purposes only. Any resemblance to real events, organizations, individuals, or threat actors is purely coincidental. This document is fictional and intended solely for training and simulation scenarios.