Trellix ADVANCED RESEARCH CENTER

Threat Intelligence Group

Advanced Research Center

Threat Analysis Report: US Oil and Gas Sector

Period: December 31, 2024 - March 31, 2025 (90 days)
Sector Focus: Oil and Gas Industry
Region: United States
Report Date: March 31, 2025

The information presented in this report was compiled from Trellix's Insights platform as well as Trellix's Advanced Threat Landscape Analysis System (ATLAS).

Insights data is collected and vetted, from internal research as well as open-source data incidents and events by the Trellix Threat Intelligence Group (TIG).

ATLAS is a data analysis tool that seamlessly integrates Trellix's data sources (Repper, REST, RealProtect, JCM, etc.) and provides enrichment data for global emerging threats such as sector and geolocation.

The data from both platforms is correlated to provide a dedicated view for campaigns consisting of events, threat actors, IOCs, and more. The Trellix Insights and ATLAS platforms give customers unprecedented access to malicious file, domain, and IP detections from Trellix's sensors strategically placed around the globe.

Executive Summary

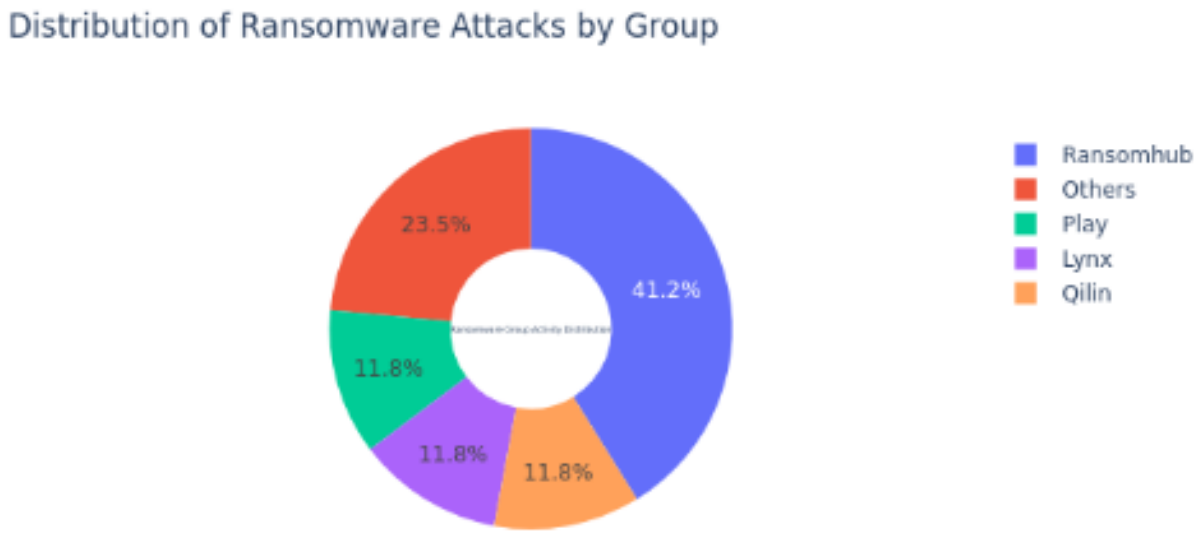
This report presents a comprehensive analysis of cyber threats targeting the US oil and gas sector over the past 90 days. The analysis reveals a complex threat landscape characterized by increasing ransomware attacks, sophisticated state-sponsored operations, and concerning underground criminal activities.

1. Threat Activity Overview

Detection Activity

- 47 unique cyber campaigns identified
- 4,517 security incidents detected
- 21 different organizations directly affected
- 17 confirmed ransomware incidents
- Multiple state-sponsored APT groups active

Attack Distribution



2. Threat Actor Landscape

State-Sponsored Actors

- **Primary Actors**: APT37, APT43, Bitter APT, FIN7

- **Origin Countries**: Russia, India, North Korea, China, Iran
- **Focus Areas**: Intelligence gathering, infrastructure compromise

- **Additional Actors:** TEMP.Veles (Xenotime), Sandworm Team, Dragonfly, APT29 (Cozy Bear), Volt Typhoon
- **Specific Targeting:** ICS/SCADA targeting, safety system manipulation, industrial control systems, supply chain attacks.

Criminal Groups

- **Major Players**:
  - Ransomhub (most active, 41.2% of ransomware attacks)
  - Play, Lynx, Qilin (each responsible for multiple attacks)
  - Hunters International and Dridex Group (active in non-ransomware operations)
- **Additional criminal groups:** Safepay, Medusa, Everest.

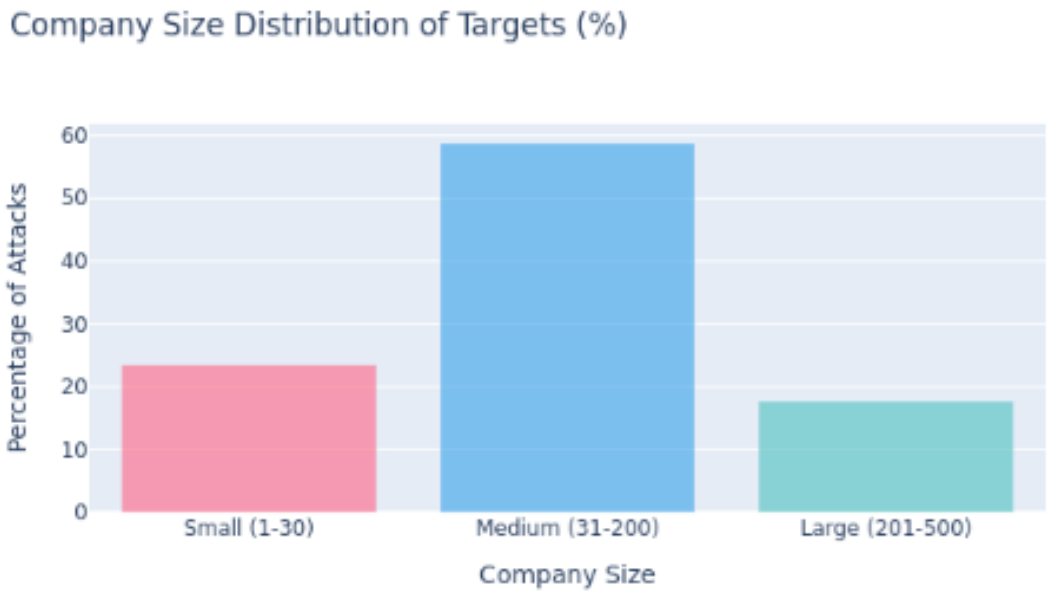
3. Attack Patterns and Methods

Technical Approaches

- Living-off-the-land techniques utilizing PowerShell and Command Prompt
- Script-based attacks (WScript, VBScript)
- Information stealers and downloaders
- Supply chain compromises.
- 87% of attacks targeting Windows systems
- PowerShell exploitation, command line abuse.

Target Demographics

- **Company Size Distribution**:
  - Small (1-30 employees): 23.5%
  - Medium (31-200 employees): 58.8%
  - Large (201-500 employees): 17.7%



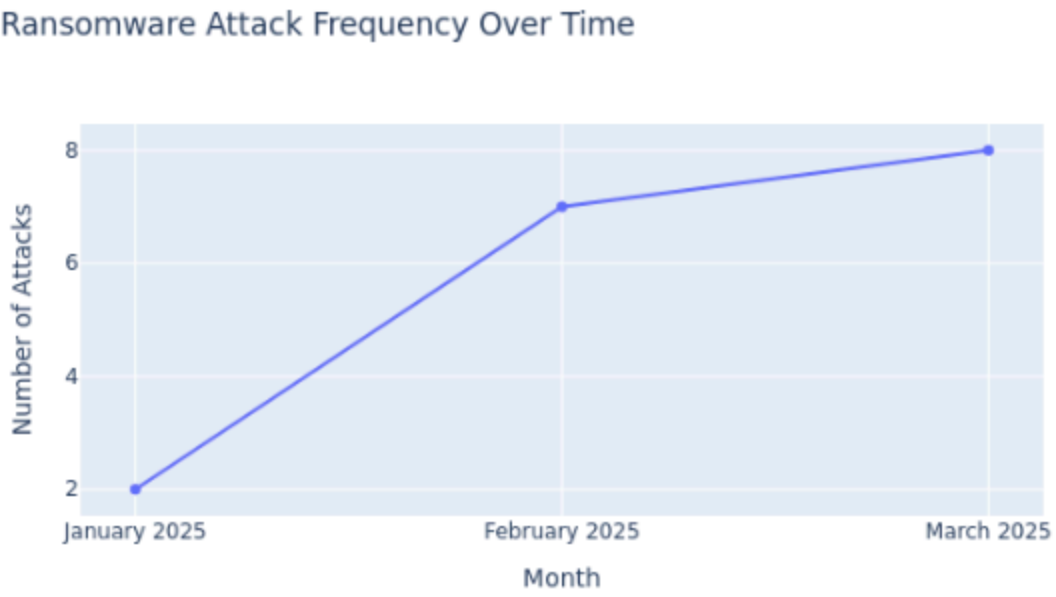
4. Temporal Analysis

Attack Frequency

- Significant escalation in Q1 2025
- March 2025: 8 ransomware attacks
- February 2025: 7 ransomware attacks
- January 2025: 2 ransomware attacks

Most Targeted States

- Texas (35.3% of attacks)
- Rhode Island (11.8%)
- Other affected states: Louisiana, Michigan, Missouri, Tennessee, Kansas, Connecticut.



5. Underground Activity Analysis

Current Threats

- Active trading of exploit kits and vulnerabilities
- Large-scale credential database trading (3.5M to 12M records)
- Windows Common Log File System Driver vulnerability (CVE-2024-49138) exploitation
- SSH DOS/MITM vulnerability exploits in circulation
- Industrial control system exploits.
- Compromised credential databases.

Infrastructure Targeting

- Increased sophistication in exploit development
- Focus on:
  - Corporate networks
  - Supply chain vulnerabilities
- Trading of specialized access tools
- Interest in industrial system exploits
- Limited direct targeting of oil and gas infrastructure

Conclusion

The US oil and gas sector faces a complex and evolving threat landscape with increasing sophistication in attack methods and a diverse range of threat actors. The sector must maintain heightened security awareness and implement robust defense measures to protect against these growing threats.

Report generated: March 31, 2025 Trellix Threat Intelligence Group (TIG)
Classification: TLP:AMBER