Trellix ADVANCED RESEARCH CENTER

Threat Intelligence Group

Advanced Research Center

Threat Analysis Report: EMEA Oil and Gas Sector

Period: December 31, 2024 - March 31, 2025 (90 days)
Sector Focus: Oil and Gas
Region: EMEA
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.

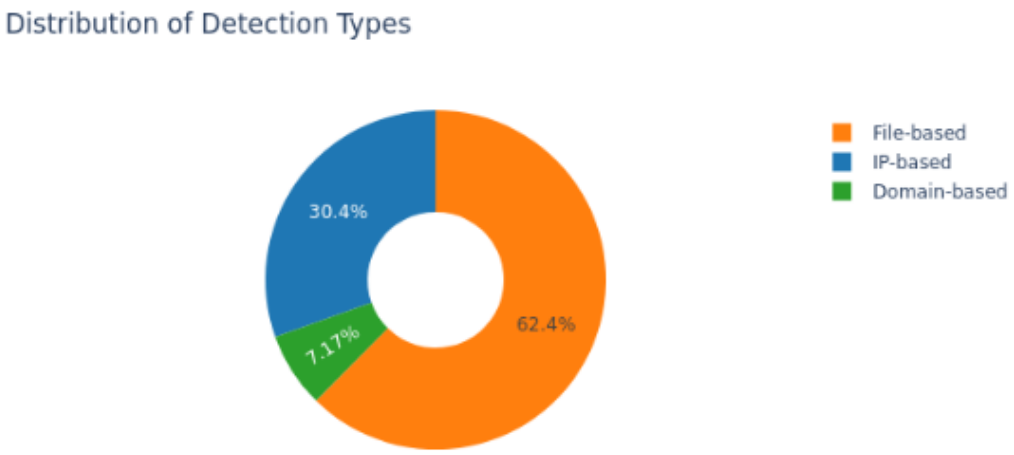
Executive Summary

This report presents a comprehensive analysis of cyber threats targeting the oil and gas sector in the EMEA region over the past 90 days. The analysis combines insights from ransomware tracking, campaign detection, underground intelligence, and threat actor profiling to provide a holistic view of the current threat landscape.

1. Key Findings

Detection Activity

- Total of 487,305 security detections observed
- Distribution of detection types:
  - File-based: 62.4% (303,976 detections)
  - IP-based: 30.5% (148,374 detections)
  - Domain-based: 7.1% (34,955 detections)



Ransomware Activity

- Minimal to no publicly disclosed ransomware incidents specifically targeting the sector
- Possible indicators:
  - Enhanced security posture in the sector
  - Non-public incident handling
  - Tactical shift by threat actors

2. Active Threat Actors

State-Sponsored Groups:

1. **Sandworm Team (Russia)**
   - Specializes in ICS/SCADA targeting
   - Tools: Industroyer2, BlackEnergy, CaddyWiper

2. **TEMP.Veles (Russia)**
   - Focus on critical infrastructure
   - Tools: TRITON framework, Mimikatz, PsExec

3. **APT33 (Iran)**
   - Targets energy and petrochemical sectors
   - Tools: Shamoon, DROPSHOT, TURNEDUP, StoneDrill

4. **Dragonfly (Russia)**
   - Focuses on energy sector supply chain
   - Tools: Havex/Oldrea, WSO Webshell, Industroyer, Mimikatz, WSO WebShell

5. **Cyber Av3ngers (Iran)**
   - Specializes in ICS targeting
   - Focus on specific PLC systems

3. Underground Activity Analysis

- **Limited direct discussions about oil & gas targets**
- **Significant technical capability development:**
  - New ransomware strains
  - ICS vulnerability exploitation tools
  - Network penetration capabilities
  - Social engineering services
- **Critical Vulnerability Discussions**
  - Windows Common Log File System Driver (CVE-2024-49138)
  - Arbitrary read/write capabilities
  - SYSTEM level privilege escalation potential
- **Access Methods Being Traded**
  - Corporate network access
  - Industrial control system vulnerabilities
  - Remote access capabilities

4. Threat Assessment Matrix

Threat Vector	Risk Level	Trend	Primary Actors
ICS/SCADA	High	↑	Sandworm, TEMP.Veles
Ransomware	Medium	→	Various Cybercrime Groups
Supply Chain	High	↑	Dragonfly, APT33
Phishing	Medium	→	Multiple Actors
Network	High	↑	All identified groups

Conclusion

The analysis of cyber threats targeting the oil and gas sector in EMEA over the past 90 days reveals a complex and evolving threat landscape characterized by sophisticated state-sponsored actors, advanced technical capabilities, and multi-vector attack approaches. While public ransomware activity has been notably low, the high volume of detections (487,305) across multiple vectors indicates persistent and active targeting of the sector.

The presence of well-resourced threat actors like Sandworm Team, TEMP.Veles, and APT33, combined with the ongoing development of attack capabilities in underground forums, suggests that the threat level will remain elevated for the foreseeable future. The sector faces particular challenges from threats targeting industrial control systems and operational technology, with potential for both espionage and destructive operations.

Organizations in the oil and gas sector must maintain heightened security vigilance and continue to evolve their defense capabilities. The combination of technical controls, operational security measures, and robust incident response planning will be crucial for protecting critical infrastructure against current and emerging threats. Regular assessment and updating of security measures, coupled with active threat intelligence monitoring, will be essential for maintaining resilient operations in this challenging threat environment.

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