Anomali Energy Threat Defense

Energy Sector Specific Malware Intelligence

As a security team at an energy company, it's crucial to stay vigilant and well-informed about the latest threats targeting your sector . Malware targeting companies like yours is often explicitly created to target industrial control systems (ICS) systems for espionage, disruption, or sabotage. This type of malware is often associated with nation-state threat actors As such, it is vital that you have the most up-to-date sources of energy sector-specific malware threat intelligence to always maintain a competitive edge in defending against such attacks.

Anomali's Energy Threat Defense Intelligence Channel is hereto help.

This Intelligence Channel provides a real-time, global, curated feed of thousands of weekly observables related to Malware and Ransomware families that target Energy, ONG (Oil and Natural Gas), Utilities, Critical Infrastructure, ICS, OT/IT, and SCADA globally.Finally, with the large density of Oil and Gas exploration located in the Gulf countries in the Middle East, this feed also highlights the threats specifically targeting that region.

The use of samples collected and sandboxed globally to provide greater accuracy and context is a significant advantage. This ensures that the intelligence is reliable and relevant, making it easier for your security team to manage intelligence related to your specific intelligence requirements.

This Intelligence Channel, powered by PolySwarm, sources and grades malware intelligence through an incentive-based marketplace. Anomali's Threat Research team curates top-notch intelligence from expert malware researchers and anti-virus engines, offering customers affordable, up-to-date, and high-quality insights.

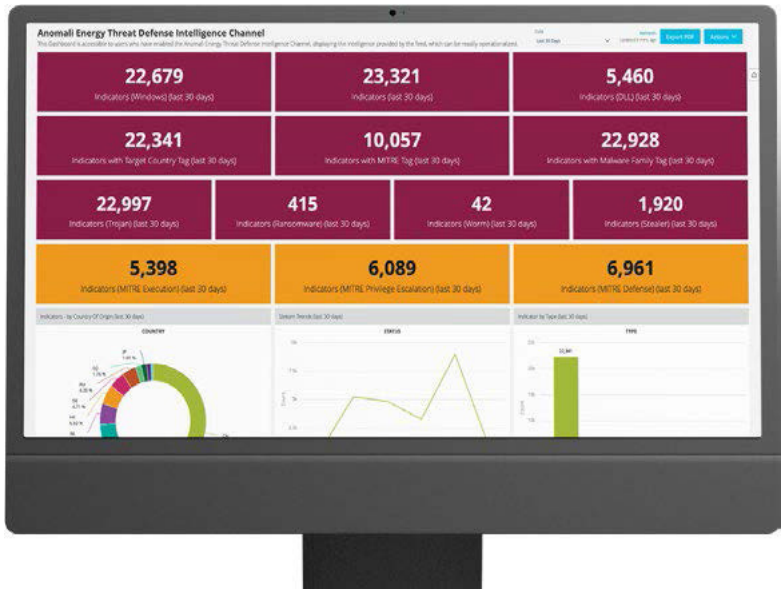
This partnership between PolySwarm and Anomali provides your security team with access to world-class, constantly up-todate malware intelligence at an affordable cost. The use of global samples, extended tagging, and sector-specific insights ensures that the intelligence is reliable, relevant, and actionable.

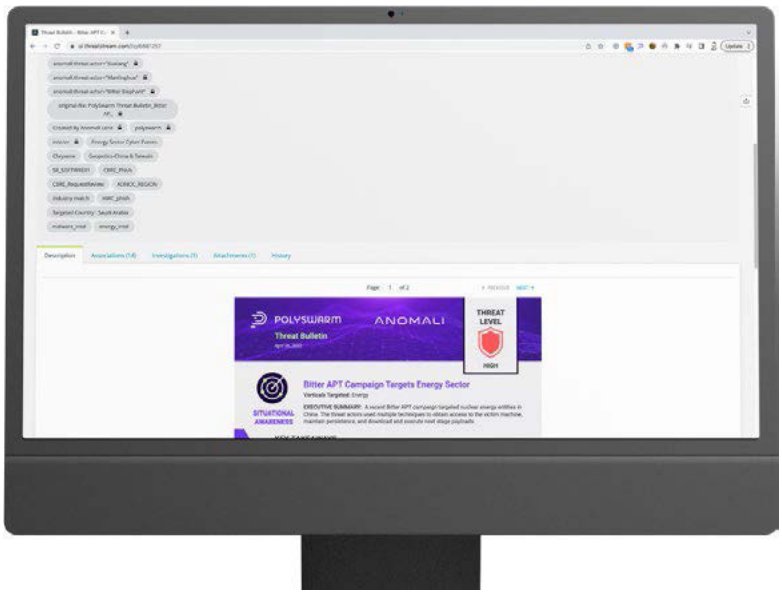
BENEFITS

- Increased visibility and early warning of targeted threats towards Energy Sector
- Reduced exposure to potential breaches
- Increased productivity and reduced burnout of Threat Intelligence and SOC Teams
- Increased SIEM/SOAR R.O.I.
- Streamline CTI team workflows
- Value pricing extends the capabilities of CTI and SOC Teams

KEY CHANNEL BENEFITS

- Global energy malware coverage is 100% sandboxed
- Detailed C2 information
- Unified Malware naming
- Integrated Risk Scoring directly in Threatstream
- Mitre TTP support
- Malware from Threat Actors known to target the Energy Sector
- Detailed ThreatStream Dashboard to quickly operationalise indicators
- Enriched Observables with further information
- Malware identified as having been written in languages commonly associated with attacks on the energy sector in the Middle East.





PREMIUM MALWARE THREAT REPORTS

- Energy Malware Premium Threat Reports
- Provides Associated Mitre TTP's
- Threat Level indicators (e.g. Low, High)
- Type of Report (e.g. Situational Awareness, Campaign)
- Gain valuable insights and actionable context
- Uncover specific industry and geography related issues
- Published 2-3x per week

Key Use Cases

CTI/SOC Automation

Extensive tagging and scoring provide an easy way to collect and disseminate intelligence downstream

Threat Hunting

Intelligence on malware from over 30+ malware and ransomware families targeting the Energy Sector

Telemetry enrichment

Comprehensive tagging and C2 information

Incident Response

Mitre TTP details, with associated IOCs for automated dissemination

Vulnerability management prioritization

CVE information and numeric threat scoring

ANOMALI