



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Energy Sector Situational Awareness Update

European Network of Transmission System Operators for Gas (ENTSOG)

Workshop on Data Exchange and Cybersecurity

Recent Trends

Focus on gas sector

Reporting period: January-December 2025



In 2025, Gas represented the **third most targeted energy subsector**, following Electricity and Oil



Much of the observed activity consists of **unconfirmed Distributed Denial of Service (DDoS) attacks** primarily claimed by **hactivist groups** and often linked with **key geopolitical events**.



The **gas sector** is also targeted by **ransomware operators** and other **opportunistic threat actors** claiming **data extortion and data breach** attacks.

Relevant Incidents

Focus on gas sector

Reporting period: July-September 2026

Energy company dataset allegedly breached by CI0p extortion group

Geography	 Netherlands
Date	14/08/2026
Threat actor	CI0p
Threat type	Data breach

- 14 August: the extortion group CI0p listed the company on its data leak site, along with approximately 50 other organisations in the same campaign
- The group claimed to have exfiltrated approximately 90 gigabytes of data, including technical drawings, facility images, scans of test report and project plans
- The company stated it was aware of a potential cyber incident and was investigating the breach but did not confirm CI0p's claims
- Security researchers linked the wider campaign to the exploitation of the EUVD-2026-37831 (CVE-2026-12569) vulnerability in PTC's Windchill engineering software

Threat actor "MrL33tH4x0rmm" offers alleged energy company database on DarkForums

Geography	 France
Date	14/07/2026
Threat actor	MrL33tH4x0rmm
Threat type	Data breach

- 14 July: threat actor MrL33tH4x0rmm advertised the alleged sale of a 20 million-record database purportedly belonging to a French energy company on DarkForums
- According to the post, the database contains customer information including names, telephone numbers, service point identifiers, supplier information, postal addresses, pricing plans, subscription power requests and other utility-related records
- The seller shared a sample dataset but the authenticity of the data and the actor's claims has not been independently verified

Relevant Incidents

Focus on gas sector

Reporting period: July-September 2026

Spanish electricity and gas supplier allegedly suffers data breach

Geography	 Spain
Date	26/08/2026
Threat actor	LokiLeads
Threat type	Data breach

- 26 August: DarkForums user “LokiLeads” advertised for sale an alleged customer database from a leading Spanish electricity and gas supplier
- Based on the listing’s description, the data included customer identity, contact details, address, tariff, supply point and energy consumption information
- The data was offered for sale via a Telegram contact and the listing reportedly included 50 sample lines to support the claim’s legitimacy
- As of the time of writing, the company has not publicly addressed the actor’s breach claim

Spanish Supply Point Information System (SIPS) listed on PwnForums

Geography	 Spain
Date	06/09/2026
Threat actor	spain
Threat type	Data breach

- 06 September: PwnForums user “spain” advertised a dataset allegedly sourced from Spain’s Supply Point Information System (SIPS), a regulated registry of electricity and gas supply points
- The data allegedly included more than 40 million lines, including Universal Supply Point Code (CUPS) supply-point identifiers, supply addresses, customer and account-holder details, contact information, meter and metering equipment data and energy consumption figures
- 15 September: DarkForums user “benabdelozzh” advertised what is assessed to be the same dataset
- As of the time of writing, SIPS has not publicly addressed either actor’s breach claims

Thank you for your attention



+30 28 14 40 9711



info@enisa.europa.eu



enisa.europa.eu

ENISA

European Union Agency
for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium