ZEROFOX INTELLIGENCE

Flash

Spanish Energy Company Breached

F-2026-01-12a

Classification: TLP:CLEAR

Criticality:LOW

Intelligence Requirements: Data Breach, Threat Actor, Energy Sector

January 12, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EST) on January 12, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Spanish Energy Company Breached

| Key Findings

- On January 4, 2026, actor “spain” announced on the dark web forum BreachForums that they had breached Endesa, a Spanish energy company. On January 5, 2026, actor “glock” posted the same advertisement on the dark web forum DarkForums. ZeroFox assesses it is almost certain these personas are being operated by the same threat actor.

- According to spain/glock, the sales post was approved by both forums’ moderation teams, and the data was verified, likely lending significant credibility to the post.

- Endesa confirmed in a statement that a threat actor gained unauthorized and illegitimate access to its systems and extracted sensitive personally identifiable information (PII).

- It is almost certain that the advertisements on the dark web forums will attract significant attention from potential buyers, especially considering that Endesa has confirmed the breach.

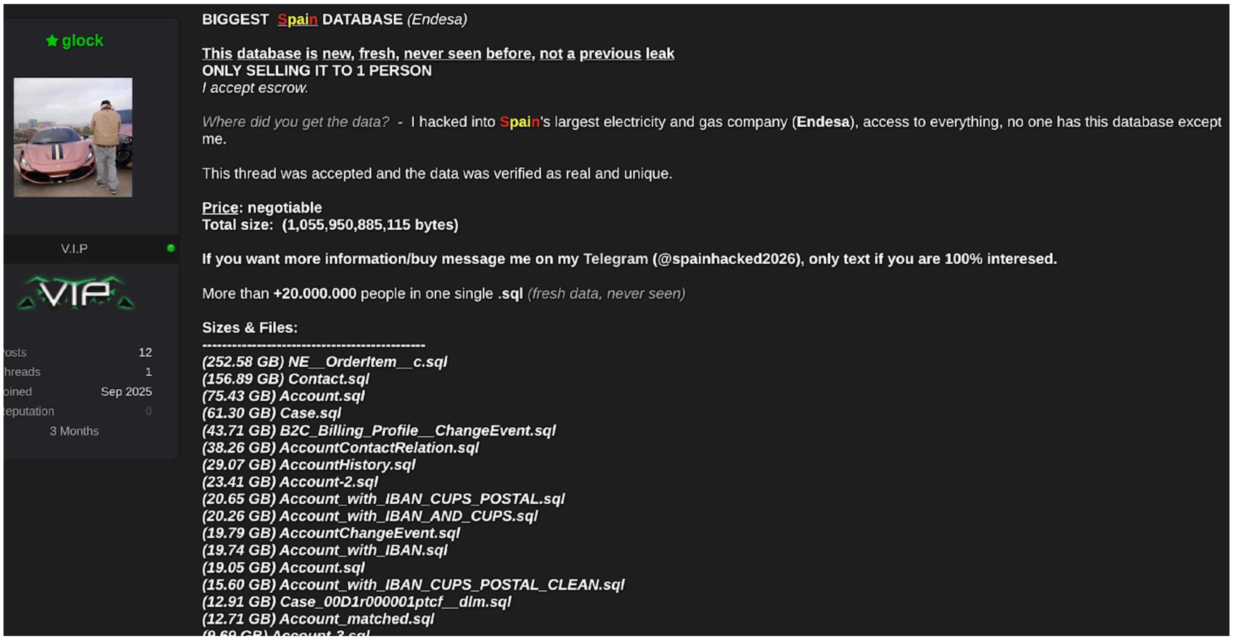
Details

On January 4, 2026, newly registered and unvetted actor spain announced on the dark web forum BreachForums that they had breached Endesa, a Spanish energy company. The actor claimed to have full access to all data stored by the company; they also claimed that this was a new breach and that they are the sole actor in possession of the data. Endesa subsequently confirmed that it had been breached.[1]

- On January 5, 2026, newly observed and unvetted actor “glock” posted the same advertisement on the dark web forum DarkForums. Both actors have the same profile picture and are almost certainly the same individual. Spain/glock was very likely attempting to enhance circulation of the advertisement to attract more potential buyers.
- Spain joined BreachForums in January 2026, and glock joined DarkForums in September 2025; neither persona has accumulated a positive reputation on the respective forums.
- Endesa is reportedly one of Spain’s largest gas and electricity companies and documented a nine-month revenue of approximately EUR 16 billion from January to September 2025.[2]

[1] hXXps://www.telemadrid[.]es/noticias/economia/Hackeo-a-Endesa-Energia-compromete-datos-sensibles-de-millones-de-clientes-0-2852114765--20260112104854.html

[2] hXXps://www.endesa[.]com/en/press/press-room/news/economic-information/september-2025-results



★ glock

V.I.P

osts 12
hreads 1
oined Sep 2025
eputation 0
3 Months

BIGGEST Spain DATABASE *(Endesa)*

This database is new, fresh, never seen before, not a previous leak
ONLY SELLING IT TO 1 PERSON
I accept escrow.

Where did you get the data? - I hacked into Spain's largest electricity and gas company (**Endesa**), access to everything, no one has this database except me.

This thread was accepted and the data was verified as real and unique.

Price: negotiable
Total size: (1,055,950,885,115 bytes)

If you want more information/buy message me on my Telegram (@spainhacked2026), only text if you are 100% interesed.

More than **+20.000.000** people in one single **.sql** *(fresh data, never seen)*

Sizes & Files:

(252.58 GB) NE__OrderItem__c.sql
(156.89 GB) Contact.sql
(75.43 GB) Account.sql
(61.30 GB) Case.sql
(43.71 GB) B2C_Billing_Profile__ChangeEvent.sql
(38.26 GB) AccountContactRelation.sql
(29.07 GB) AccountHistory.sql
(23.41 GB) Account-2.sql
(20.65 GB) Account_with_IBAN_CUPS_POSTAL.sql
(20.26 GB) Account_with_IBAN_AND_CUPS.sql
(19.79 GB) AccountChangeEvent.sql
(19.74 GB) Account_with_IBAN.sql
(19.05 GB) Account.sql
(15.60 GB) Account_with_IBAN_CUPS_POSTAL_CLEAN.sql
(12.91 GB) Case_00D1r000001ptcf__dlm.sql
(12.71 GB) Account_matched.sql
(9.69 GB) Account-3.sql

glock's post on DarkForums

Source: ZeroFox Intelligence

According to spain/glock, the sales post was approved by both forums' moderation teams, and the data was verified, likely lending significant credibility to the post. The full dataset reportedly contains information pertaining to more than 20 million Spanish residents and exceeds 1 TB in size. The price is reportedly negotiable, and the actor stated that they will only sell to one person via escrow.

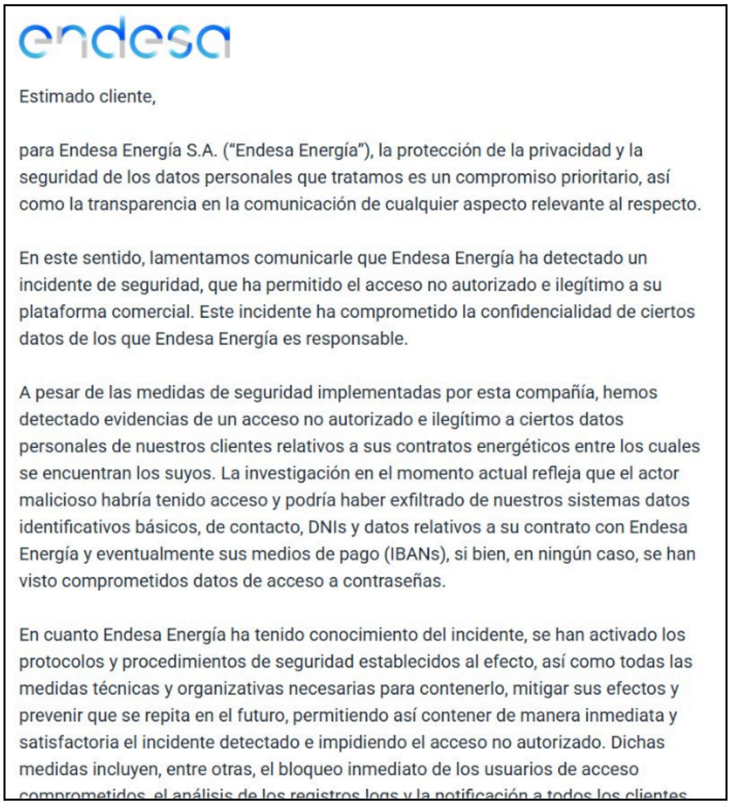
- The dataset allegedly contains highly sensitive PII related to both customers and internal company business information.
- Among the most sensitive data are potential Foreigner Identity Numbers (NIEs), national ID numbers, names, emails addresses, International Bank Account Numbers (IBANs), phone numbers, and other personal details.

Endesa confirmed in a statement that a threat actor gained unauthorized and illegitimate access to its systems and extracted sensitive PII; however, online passwords were reportedly not extracted.[3] Endesa also warned customers that, although it had not

[3] hXXps://www.europapress[.]es/portaltic/ciberseguridad/noticia-hackeo-endesa-energia-compromete-datos-sensibles-clientes-incluidos-dni-medios-pago-20260112100753.html

detected any mishandling of the compromised data, it could be used for identity fraud and social engineering campaigns.

- In February 2024, the Spanish Data Protection Agency (AEPD) fined Endesa EUR 6.1 million for General Data Protection Regulation (GDPR) violations following a security breach in 2024 that likely exposed customer data.[4]



endesa

Estimado cliente,

para Endesa Energía S.A. ("Endesa Energía"), la protección de la privacidad y la seguridad de los datos personales que tratamos es un compromiso prioritario, así como la transparencia en la comunicación de cualquier aspecto relevante al respecto.

En este sentido, lamentamos comunicarle que Endesa Energía ha detectado un incidente de seguridad, que ha permitido el acceso no autorizado e ilegítimo a su plataforma comercial. Este incidente ha comprometido la confidencialidad de ciertos datos de los que Endesa Energía es responsable.

A pesar de las medidas de seguridad implementadas por esta compañía, hemos detectado evidencias de un acceso no autorizado e ilegítimo a ciertos datos personales de nuestros clientes relativos a sus contratos energéticos entre los cuales se encuentran los suyos. La investigación en el momento actual refleja que el actor malicioso habría tenido acceso y podría haber exfiltrado de nuestros sistemas datos identificativos básicos, de contacto, DNIs y datos relativos a su contrato con Endesa Energía y eventualmente sus medios de pago (IBANs), si bien, en ningún caso, se han visto comprometidos datos de acceso a contraseñas.

En cuanto Endesa Energía ha tenido conocimiento del incidente, se han activado los protocolos y procedimientos de seguridad establecidos al efecto, así como todas las medidas técnicas y organizativas necesarias para contenerlo, mitigar sus efectos y prevenir que se repita en el futuro, permitiendo así contener de manera inmediata y satisfactoria el incidente detectado e impidiendo el acceso no autorizado. Dichas medidas incluyen, entre otras, el bloqueo inmediato de los usuarios de acceso comprometidos, el análisis de los registros logs y la notificación a todos los clientes

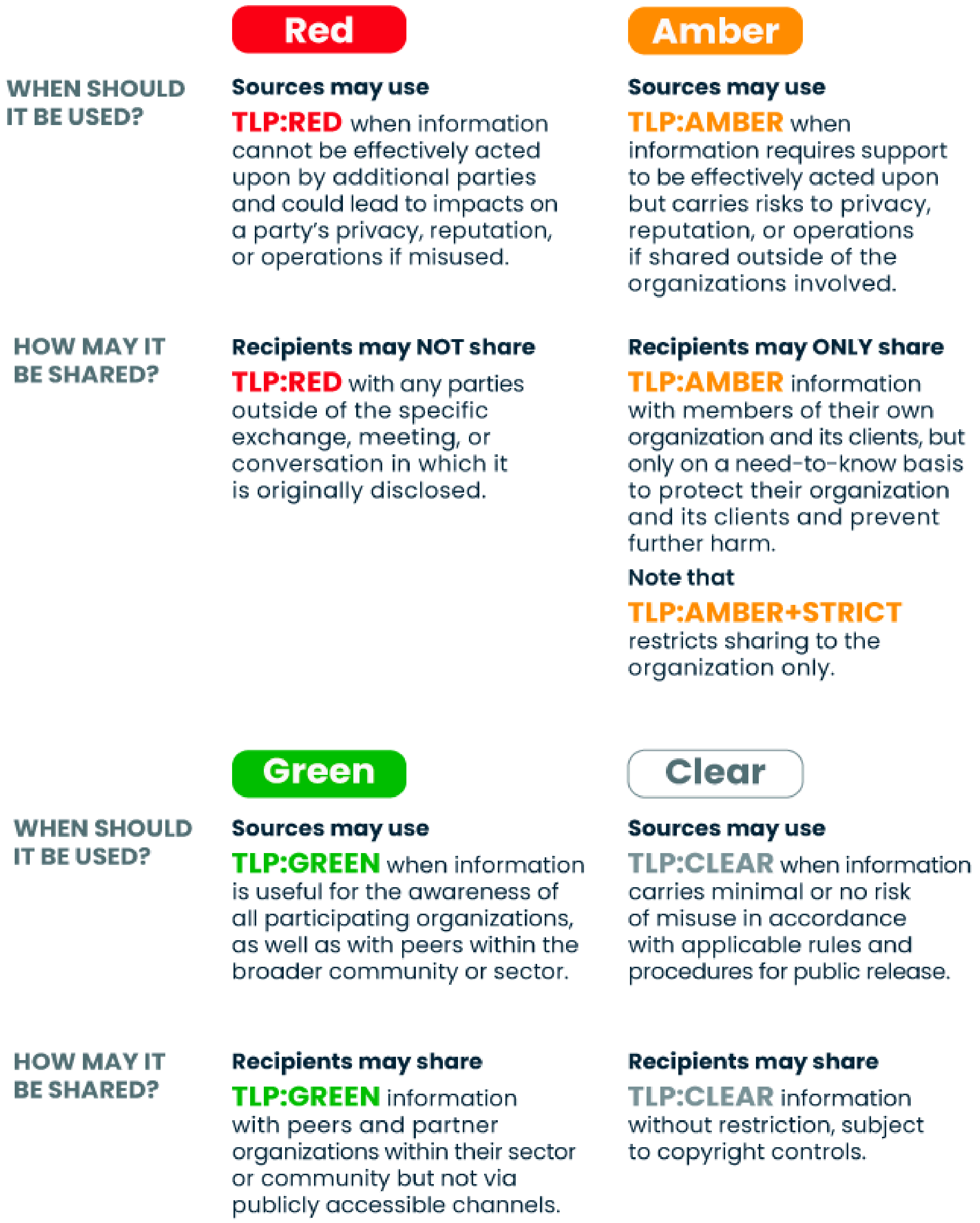
Endesa's Acknowledgement of Breach to Customers

Source: hXXps://x[.]com/H4ckmanac/status/2010634136176959799/photo/1

It is almost certain that the advertisements on the dark web forums will attract significant attention from potential buyers, especially considering that Endesa has confirmed the breach. Threat actors will very likely seek to use the data for social engineering—such as phishing or smishing (SMS phishing)—and identity fraud campaigns for financial gain.

[4] hXXps://www.dataguidance[.]com/news/spain-aepd-fines-endesa-energ%C3%ADa-61m-data-protection

Appendix A: Traffic Light Protocol for Information Dissemination

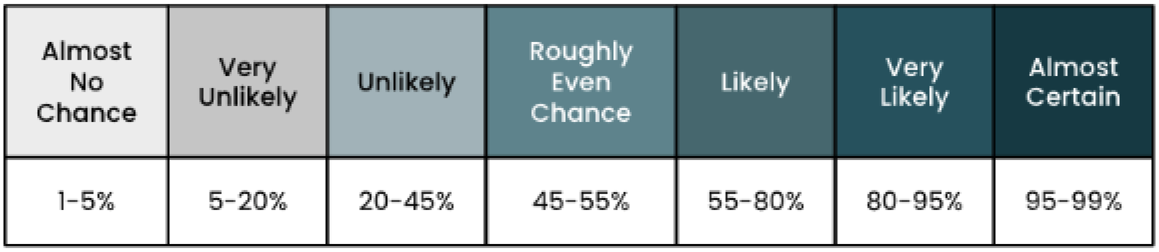


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%