ZEROFOX INTELLIGENCE

Brief

Why European Energy is Targeted by Cyber Threat Actors

B-2026-02-20a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical, DDW

February 20, 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 12:45 PM (EST) on February 19, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | Why European Energy is Targeted by Cyber Threat Actors

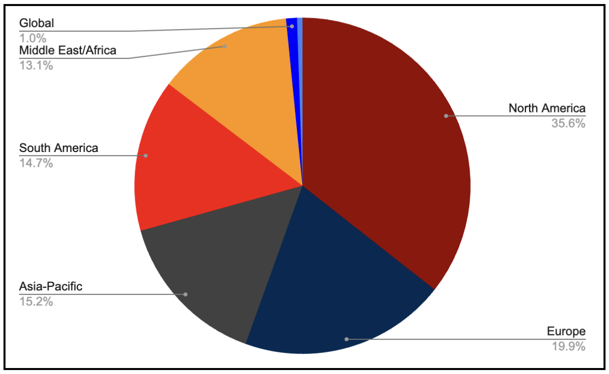
| Key Findings

- ZeroFox has observed an increase in cyberattacks targeting the European energy sector since 2024. European states have increased investment in the energy sector since Russia's war in Ukraine began, very likely attracting both geopolitically and financially motivated threat actors.
- During this transition to a modern energy grid, the wider European energy sector remains vulnerable to outside forces disrupting its energy supply.
- Efforts to avoid energy shortages since 2022 have likely contributed to the high cost of living and an uncompetitive business landscape in Europe, which together very likely risk undermining the future investments needed to safeguard European energy.
- Energy insecurity and rising costs have been a key source of political unrest in Europe since the Russia-Ukraine war began. Elevated energy prices will likely continue to generate social tensions. Russia is likely limiting supplies—thus driving up prices and contributing to the overall cost-of-living crisis—in an attempt to weaken Western resolve to back Ukraine.

Details

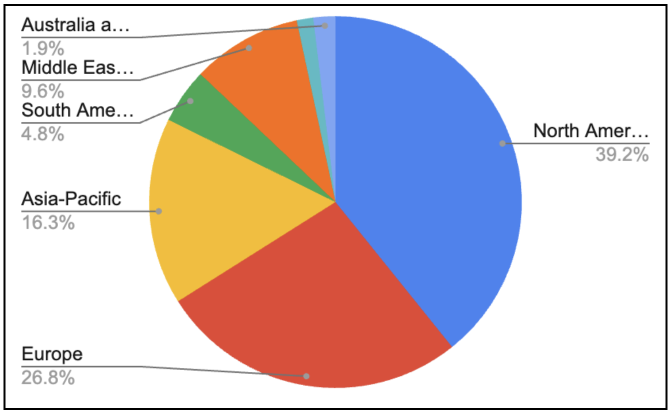
ZeroFox observed at least 38 cyberattacks targeting the European energy sector in 2024, making it the second most targeted region after North America, where 68 incidents took place. Europe accounted for nearly 20 percent of all energy-related cyber incidents in 2024.

In 2025, the European region experienced at least 56 separate incidents, with its global share increasing to nearly 27 percent, while North America experienced 82 incidents, accounting for nearly 40 percent of all energy-related cyberattacks that year.



Cyberattacks targeting the energy sector in 2024

Source: ZeroFox Intelligence



Cyberattacks targeting the energy sector in 2025

Source: ZeroFox Intelligence

As of February 17, 2026, ZeroFox Intelligence has observed at least 12 cyberattacks against the European energy sector, just below the 14 seen against North America's energy sector and double the amount seen during the same period in 2025.

Europe's Energy Challenges

The escalation in cyberattacks against the European energy sector is very likely linked to high-profile European efforts to reorient the sector since Russia's war in Ukraine began in February 2022.

- At the onset of Russia's war in Ukraine in early 2022, the European Union (EU) quickly reduced its dependence on Russian gas from about 40 percent of its supplies to around 8 percent in 2023.[1] This contributed to a large spike in EU-wide inflation, as alternative liquified natural gas (LNG) supplies are more expensive and cumbersome to transport. This energy price spike spanned the wider economy, making transport, agriculture, and energy-intensive industries (such as factories and chemical manufacturing) more expensive. This overall increase in the cost of living has very likely contributed to wider societal tensions, including protests related to inflation and immigration, as well as to election losses for incumbent governments.

The elevated energy costs remain consequential across Europe, as they are reducing consumers' purchasing power and keeping operating costs prohibitively high; as a result, many European businesses are seeking out more affordable operating environments. Europe's pursuit of alternative suppliers and sources of energy also comes with various challenges, as each alternative has its own unique vulnerabilities tied to weather, sabotage, demand, and cost.

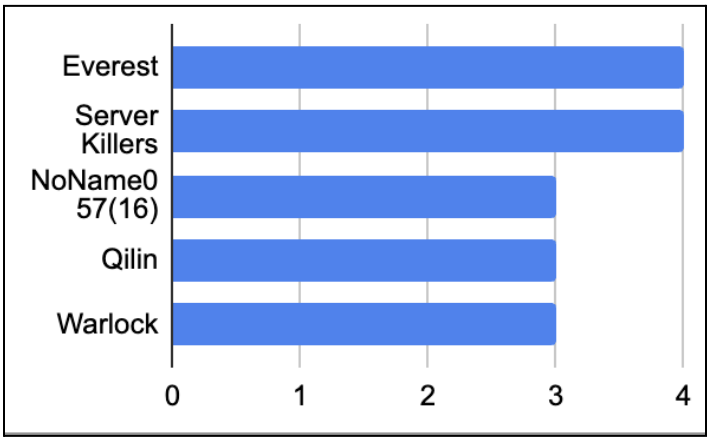
ZeroFox has observed that geopolitically motivated threat actors are continuing to target the European energy sector, likely to exacerbate societal fissures around the cost of living and the financial consequences of maintaining support for Ukraine.

- On February 16 and 17, 2026, pro-Russia threat groups "NoName057(16)" and "Server Killers" claimed responsibility for distributed denial-of-service (DDoS)

[1] hXXps://www.consilium.europa[.]eu/en/infographics/eu-gas-supply/

attacks on the websites of multiple Spain-based entities after Spanish Prime Minister Pedro Sánchez announced a financial aid package of approximately EUR 2 billion for Ukraine. Among those targeted were the Instituto IMDEA Energía, a Spanish research and development institute focused on clean and renewable energy sources.[2]

  - NoName057(16) and Server Killers were two of the top five threat actors targeting the EU energy sector in 2025.



Top five threat actors targeting the European energy sector in 2025

Source: ZeroFox Intelligence

- On February 13 and 14, 2026, pro-Russian threat actor group "Inteid" claimed on its official Telegram channel that it had conducted DDoS attacks targeting entities based in Ukraine and France, including National Nuclear Energy Generating Company Energoatom, the largest electricity producer in Ukraine.[3]

Spending

Since the 2022 energy crisis, many European countries have enacted stimulus measures amounting to as high as 2 percent of their gross domestic product (GDP) in the form of direct cash transfers, tax cuts, and incentives to purchase renewable energy such as home solar panels or heat pumps.[4] However, this is almost certainly only the beginning of a massive pan-European investment boom in the energy sector.

[2] ZeroFox Intelligence Flash Report: DDoS Attacks Target Spanish Government Websites, February 17, 2026
[3] ZeroFox Intelligence
[4] hXXps://www.weforum[.]org/agenda/2022/09/what-is-the-cost-of-europe-s-energy-crisis/

- Additionally, there are new dynamics at play—including heat waves causing concern for energy supplies, added demand from Asia, and potential strain on energy supplies—with advancements in technology necessitating the need for more electricity.
    - Artificial intelligence (AI) systems require copious amounts of electricity, especially during the testing phase. The number of data processing centers is growing in Europe, and these also require large amounts of electricity.

Discussions on a wider doctrine that addresses Europe's lack of business competitiveness are forthcoming ahead of approving the 2028–2035 EU budget,[5] which amounts to over EUR 2 trillion and is up EUR 800 billion from the 2021–2027 budget cycle.[6] Support for Ukraine is expected to come in at around EUR 100 billion, while direct EU budgetary support for the energy sector could come as high as EUR 150 billion.[7] Additionally, private sector investments in energy infrastructure as part of European plans to decarbonize and update the energy grid are almost certain to push total spending on the European energy sector to well over EUR 1 trillion.

This increased spending will very likely inspire additional cyberattacks against the European energy sector from financially motivated cyber threat actors.

- For example, on February 12, 2026, ZeroFox observed an update on the LockBit 5.0 ransomware leak site targeting Renovagy, a Spain-based company that provides IT consulting, engineering, and energy control systems, particularly for renewable energy projects.

ZeroFox assesses that further cyberattacks against start-ups focusing on energy-related projects such as small modular reactors, fusion energy, or carbon capture and storage are very likely.

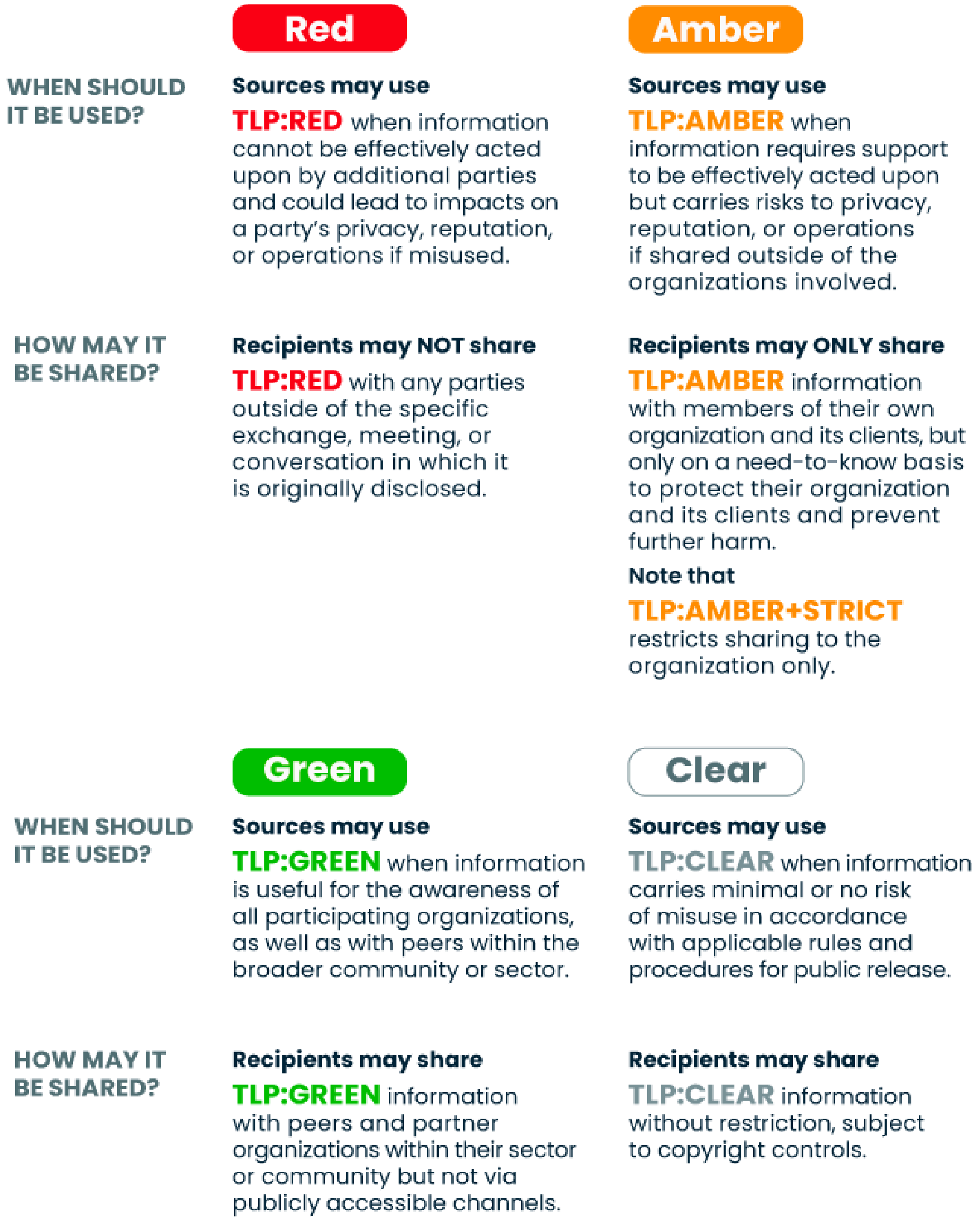
[5] hXXps://commission.europa[.]eu/topics/budget/eu-budget-2028-2034-explained_en
[6] hXXps://www.consilium.europa[.]eu/en/policies/eu-annual-budget/2025-budget/
[7] hXXps://www.contexte[.]com/eu/article/energy/five-things-the-new-eu-budget-would-mean-for-energy-and-climate_234455

More established players in the European energy market focused on managing grid congestion and electricity transmissions will likely also be targeted.

Conclusion

The European Commission estimates that EU states will need EUR 1.2 trillion to modernize the European energy grid. Additional funding will very likely be required to ensure the European energy grid can keep pace with AI-related increases in electricity demand. The energy transition will be competing against other critical EU priorities, such as growing the European defense sector, supporting Ukraine, and making investments to boost the competitiveness of European businesses against those in Asia and the United States. Together, this provides obvious targeting incentives for both financially and geopolitically motivated threat actors seeking to advance their interests by disrupting Europe's energy transition.

Appendix A: Traffic Light Protocol for Information Dissemination

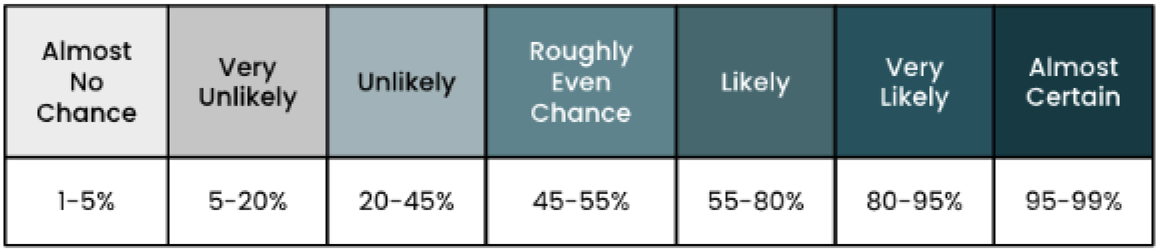


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively 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%