



EUROPEAN
TLD ISAC

Top-Level Domain Threat Landscape Analysis 2026

Executive Summary



TOP-LEVEL DOMAIN THREAT LANDSCAPE ANALYSIS 2026

ABOUT THE EUROPEAN TLD ISAC

The European Top-Level Domain Information Sharing and Analysis Centre (European TLD ISAC) is a collaborative initiative dedicated to strengthening the cybersecurity posture of country code top-level domain (ccTLD) registries across Europe. It serves as a trusted platform for sharing threat intelligence, promoting best practices and fostering cooperation among ccTLD operators, security experts and other stakeholders. For more information: <https://www.tld-isac.eu>.

CONTACT

To contact the European TLD ISAC or for media enquiries about this report, please send an e-mail to info@tld-isac.eu.

LEGAL NOTICE

The European TLD ISAC is a special Working Group within CENTR ASBL/VZW. This publication represents the views and interpretations of CENTR. CENTR has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain the CENTR and the European TLD ISAC as its source. Third-party sources are quoted as appropriate. CENTR is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither CENTR nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. CENTR maintains its intellectual property rights in relation to this publication.

Executive Summary

The *Top-Level Domain Threat Landscape Analysis (TLA) 2026* presents an updated assessment of the most relevant threats facing European country code Top-Level Domain (ccTLD) registry operators. Building on the inaugural 2024 analysis, this edition assesses a threat environment shaped by evolving cyber tactics, supply-chain dependencies, regulatory pressure (notably Directive 2022/2555 or “NIS2”), and operational complexity across the domain name system (DNS) ecosystem.

The 2026 analysis is based on an **all-hazard** threat model and incorporates threat assessments of the majority of European ccTLD registry operators. Respondents assessed 28 refined threat scenarios against their **likelihood** of occurrence combined with four distinct **impact dimensions**: financial, operational, governance/regulatory/compliance (GRC), and reputational. The result is an **objective risk score** based on survey responses, which allows security officers to prioritise the threats.

Social engineering and phishing targeting registry employees consistently emerges as the highest-ranked (combined) threat, reflecting how human-centric attack vectors can affect otherwise highly resilient technical infrastructures.

Other recurrent highly ranked threats include:

- **Compromise of the Domain Management System (DMS)**, which, while considered less likely, can have a more severe impact – particularly in operational and regulatory dimensions.
- **Persistent infiltration conducted by sophisticated threat actors**, indicating prolonged, covert operations instead of isolated events.
- **Cyber incidents at critical suppliers**, highlighting the exposure introduced by third-party and supply-chain dependencies.
- **Use of legacy systems and weak security discipline**, indicating structural risk accumulation rather than isolated failures.

The averaged risk heatmap, shown below, illustrates that most threats cluster in the *possible/unlikely* likelihood range with minor to moderate impact. Due to using averages, outliers across the four impact dimensions are not necessarily visible and demonstrate the importance of avoiding single-metric risk prioritisation. Additionally, differences in interpretation amongst ccTLD registry operators also lead to averages settling in the clusters. To address this, ccTLD registry operators receive a comparison chart containing their answers and the averages of all other answers to review and benchmark their responses.

Overall, the analysis shows that risk (for ccTLDs) is driven by **people, processes, and ecosystem dependencies**, rather than core DNS technology itself. The results of this report provide a baseline for ccTLD registries to benchmark their own risk assessments, support NIS2-aligned governance, and prioritise mitigation strategies based on worst-case impact scenarios across multiple dimensions.

While this Threat Landscape Analysis may be used as an inspiration for individual ccTLD registries, national regulatory requirements can influence how likelihood and impact are assessed.

		IMPACT				
		INSIGNIFICANT	MINOR	MODERATE	MAJOR	SEVERE/ CATASTROPHIC
LIKELIHOOD	CERTAIN	0	0	0	0	0
	LIKELY	0	0	0	0	0
	POSSIBLE	0	5	2	0	0
	UNLIKELY	0	8	6	1	0
	RARE	0	0	6	0	0

The findings highlight the importance of coordination, as several of the highest-ranked threats come from external dependencies (registrars, suppliers) rather than from the registry's core infrastructure.



EUROPEAN
TLD ISAC