CEO Brief

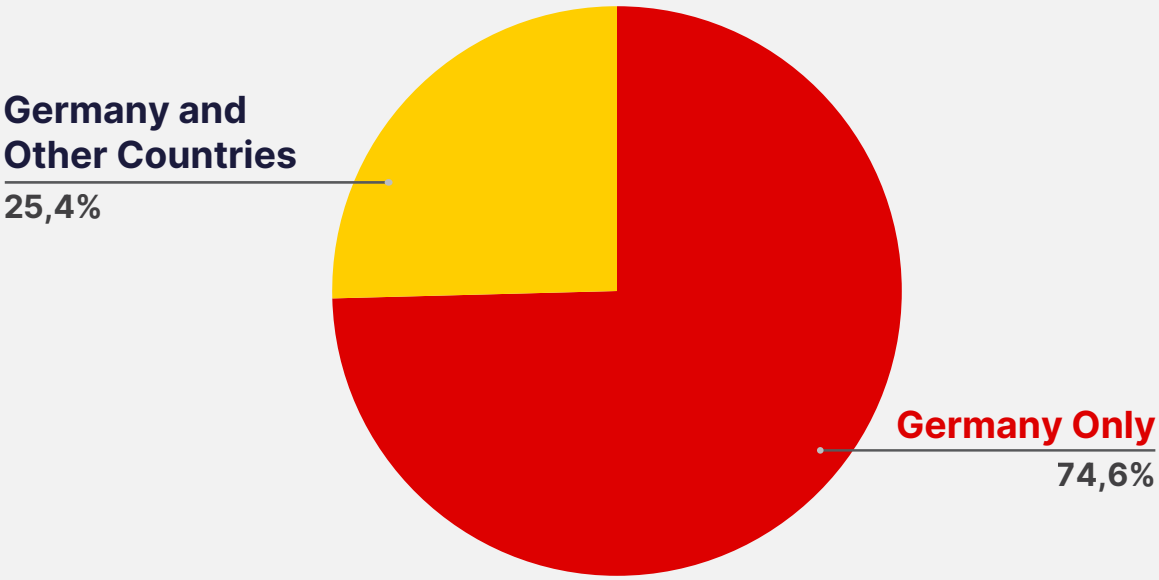
GERMANY

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

Distribution of Dark Web Threats by Country



When analyzing dark web posts specifically targeting Germany, 74.6% of posts focused exclusively on German victims, while 25.4% posts also included organizations or individuals from other countries.

This indicates that the majority of threat actor activity against Germany on underground forums and marketplaces is highly localized, reflecting region-specific targeting preferences. However, the notable portion of multi-country targeting highlights how some operations remain opportunistic or globally distributed, bundling German victims with international attack campaigns.

Distribution of Dark Web Threats by Industry

Retail Trade
Highest exposure due to payment data handling

Finance and Insurance
Valuable financial credentials target

Electronic Shopping and Mail-Order
E-commerce ecosystem vulnerability

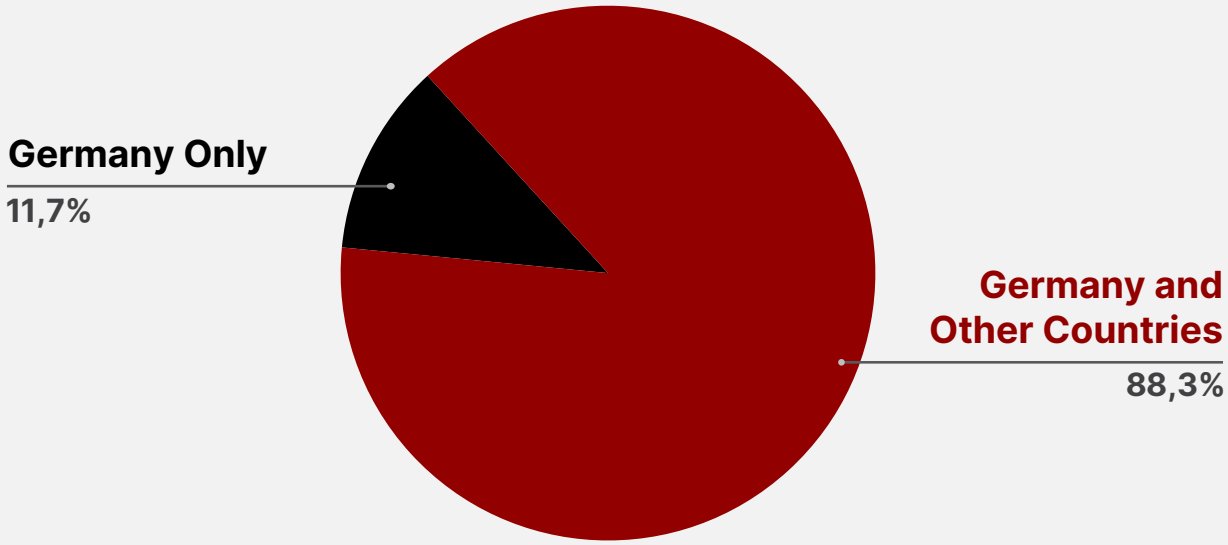
In the German dark web threat landscape, the retail trade sector emerges as the most targeted industry, accounting for 14.72% of observed threats, likely driven by the sector's extensive handling of customer payment data and its relatively fragmented cybersecurity posture.

Close behind, the finance and insurance sector (12.05%) remains a prime focus for threat actors, reflecting the persistent value of financial credentials and access to monetary systems within underground markets.

Notably, electronic shopping and mail-order houses rank third at 10.43%, underscoring how Germany's growing e-commerce ecosystem has become an increasingly attractive target for cybercriminals exploiting online transaction data and customer accounts.

This distribution highlights a clear trend: sectors directly managing sensitive financial and consumer data continue to face the greatest dark web exposure.

Distribution of Ransomware Attacks by Country

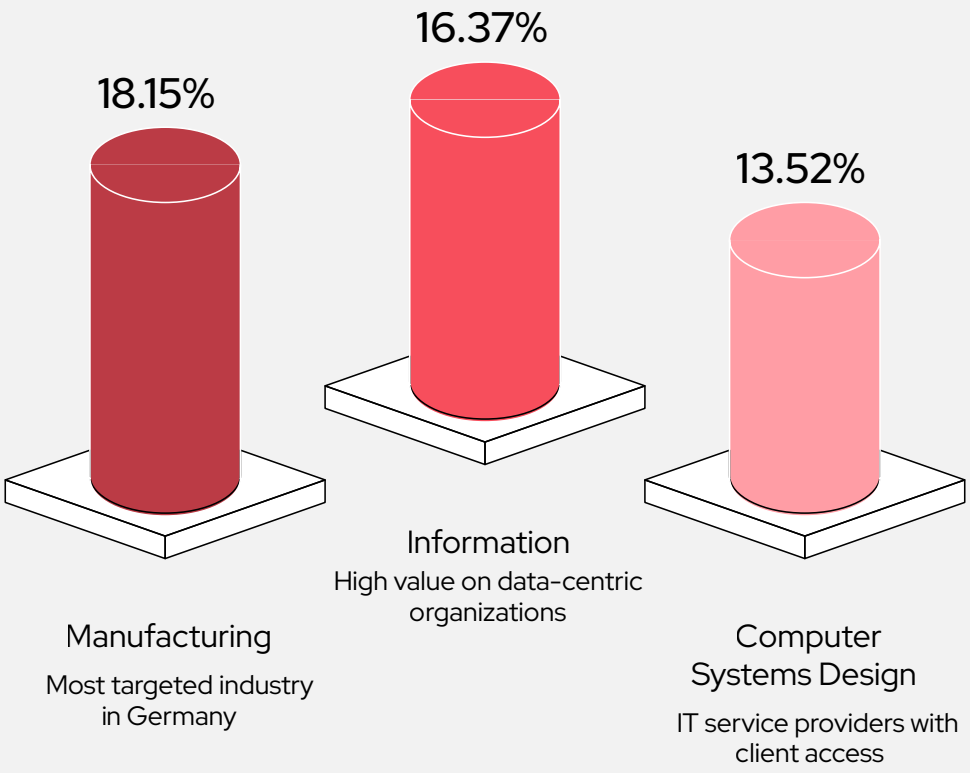


In contrast to dark web posts, the ransomware landscape shows that only 11.7% of ransomware incidents exclusively targeted German organizations, while a significant 88.3% involved Germany alongside victims from other countries.

This indicates that ransomware operations affecting Germany are predominantly part of broader, globally coordinated campaigns rather than localized attacks.

It reflects the highly opportunistic and borderless nature of modern ransomware groups, who often deploy attacks at scale across multiple regions and industries, with German organizations frequently caught within wider targeting patterns.

Distribution of Ransomware Attacks by Industry



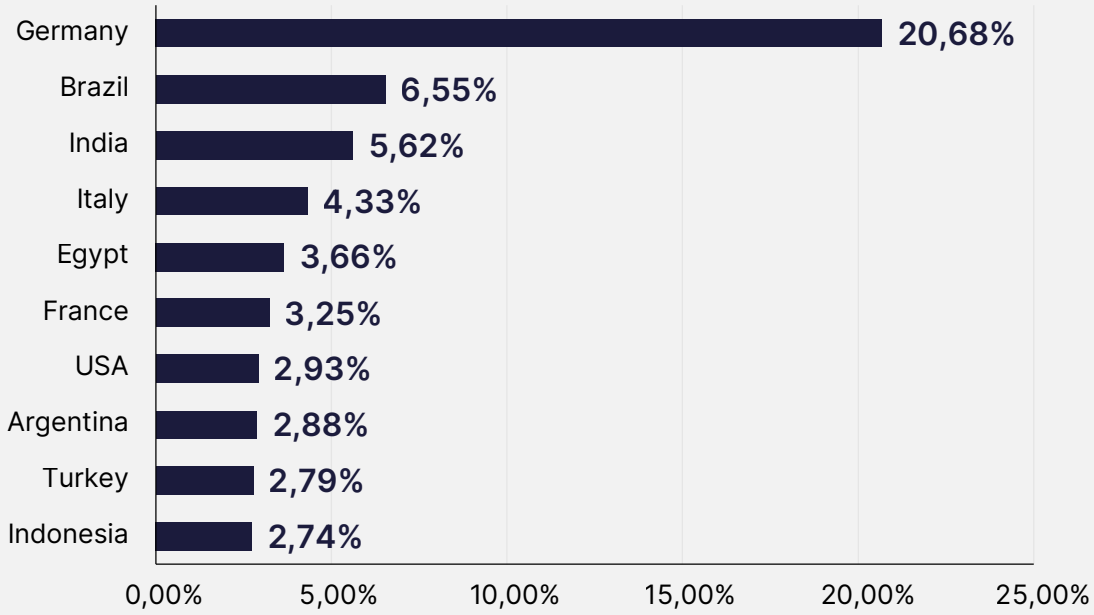
In Germany's ransomware threat landscape, the manufacturing sector stands out as the most targeted industry, accounting for 18.15% of attacks.

The information sector follows closely at 16.37%, reflecting the high value placed on data-centric organizations and their often interconnected digital infrastructure.

Computer systems design and related services rank third at 13.52%, indicating that IT service providers are frequent targets, likely due to their access to multiple client environments and critical systems.

These insights point to ransomware operators prioritizing sectors where downtime is costly and where lateral access can amplify the impact of their attacks.

Stealer Logs - Distribution of the Compromised Data by Victim Country



Stealer log data reveals that Germany accounts for 20.68% of compromised records, making it the most impacted country by a significant margin. This suggests a higher localization rate among German users and most visited domains we selected for this case.

Recommendations for CEOs:

- **Invest in Cybersecurity as a Strategic Priority:** Allocate sufficient budget and resources to bolster cybersecurity measures, recognizing that robust digital defenses are critical to protecting the company's reputation and financial assets.
- **Foster a Culture of Security**: Champion cybersecurity at the executive level to ensure it is integrated into business strategy. Encourage cross-departmental collaboration and continuous employee training to minimize risks stemming from phishing and insider threats.
- **Enhance Risk Management and Business Continuity:** Develop and regularly update comprehensive risk management and incident response plans. Prioritize investments in cybersecurity insurance and business continuity planning to mitigate potential financial impacts from cyber incidents.
- **Leverage Data-Driven Cyber Intelligence:** Utilize insights from threat intelligence reports to inform decision-making. Understanding evolving risks—such as ransomware and dark web threats—can guide strategic investments and partnerships for improved defense.
- **Strengthen Regulatory and Compliance Posture:** Stay ahead of evolving regulatory requirements and industry standards. Proactive compliance can reduce legal risks and build trust with customers, investors, and partners.
- **Collaborate with Industry Peers and Stakeholders:** Engage with cybersecurity forums, industry groups, and government initiatives to share best practices and intelligence. Such collaboration enhances overall resilience and can lead to collective responses to emerging threats.