Hacktivism:
Hacktivism against European countries was mostly due to political motives, with low technical impact in most cases. Killnet and Noname057(16) were the most active self-claimed hacktivist groups targeting European countries. TeamOneFist was the most active self-claimed hacktivist actor targeting Russia.

Cybercrime:
The top 5 most active ransomware families in Europe were Lockbit, Blackbasta, Vice society, AlphV and Play. We recorded 132 ransomware attacks against European entities in Q4 2022.

Cyberespionage:
We observed cyberespionage activity supposedly originating from Russia, China, and North Korea. Several spearphishing campaigns used public EUlBA or other European-origin documents as lures.

Data exposure and leaks:
Data leaks in this quarter were mostly the result of criminal or hacktivist activity. In at least one case, a handling mistake led to data exposure.

Disruption and hijacking:
There were several physical incidents affecting telecommunication cables across Europe.