# Threat Landscape Report 2022 Q4 - Executive Summary

## DIRECT THREATS TO EU INSTITUTIONS, BODIES, AND AGENCIES

### Main attacks

- A series of DDoS attacks affected websites belonging to 7 EUIBAs between late November and mid-December 2022.
- A supposedly Chinese threat actor attempted to spearphish two EUIBAs using EU official documents as a lure.
- A threat actor spoofed the identity of an EUIBA to target an EU country's ministry.

### Threat alerts

- We released 33 Threat Alerts related to malicious activities detected within, or in the vicinity of EUIBAs.
- In 36% of the cases, we had initial evidence that the malicious activity had targeted at least one EUIBA.
- Spearphishing and the direct exploitation of vulnerabilities have remained the main initial access techniques.

### Threat actor activity

- In Q4 2022, we have been tracking 11 Top Threat Actors (TTAs).
- We detected activity by 5 of them but, and to the best of our knowledge, there was no breach.

### Malware

- The Agent Tesla information stealer was the most active piece of malware with at least 6 affected EUIBAs.
- After a hiatus of 4 months, Emotet returned and affected at least 5 EUIBAs.

## THREATS IN EUROPE

**Hacktivism:**

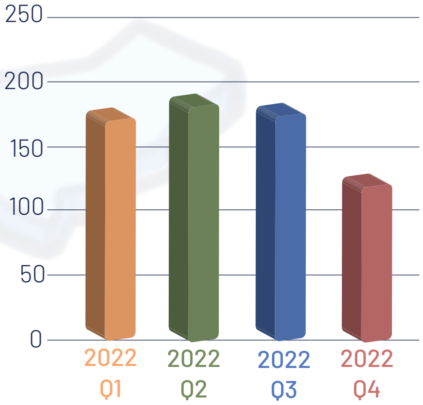
Hacktivism against European countries was mostly due to political motives, with low technical impact in most cases. Killnet and Noname057(16) were the most active self-claimed hacktivist groups targeting European countries. TeamOneFist was the most active self-claimed hacktivist actor targeting Russia.

**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. We observed a slight decrease in the number of ransomware victims in Europe in Q4 2022 compared to the rest of 2022.

Ransomware victims in EU

source: OSINT



**Cyberespionage:**

We observed cyberespionage activity supposedly originating from Russia, China, and North Korea. Several spearphishing campaigns used public EUIBA 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.