In Q2 2023, we analysed 151 malicious activities of interest targeting EU institutions, bodies, and agencies (EUIBAs) or their vicinity, and we released 39 Threat Alerts.

When known, the main motive of the attackers was cyberespionage - 63% of the cases.

Cyberespionage attacks were, in all likelihood, carried out by threat actors highly likely originating from Russia & China. There was a small number of activities reportedly coming from North Korea, Iran, Turkey, and Vietnam.

Activities were sighted in 11 sectors of interest, with the three most targeted being government, diplomacy, and transport.
When attempting to exploit software vulnerabilities, malicious activities of interest targeted more than 30 software products used by EUIBAs.

This included Microsoft Azure, Microsoft Teams, MOVEit Transfer, Atlassian Confluence, Fortinet, Kubernetes, and VMware.

We didn’t observe any breach affecting IT companies actually or possibly delivering IT services to EUIBAs.
25 threat actors were active against EUIBAs or in their vicinity

11 likely of Russian origin, 7 of likely Chinese origin

There was sustained spearphishing activity by two Top Threat Actors – highly likely Russia-linked and China-linked; one of them used EU lures on several occasions

Several EUIBAs of the financial sector were targeted with DDoS attacks in a pro-Russia hacktivist campaign
As regards **initial access**, the observed techniques detected against EUIBAs or their vicinity were spearphishing (52%), exploitation of public-facing applications (19%), drive-by compromise (7%), and infection via removable media (5%).

We also observed adversaries spoofing EUIBAs or companies working with EUIBAs in attempts to lure victims in phishing attacks.

In our constituency, the **most active malware families** were SocGolish, used for initial access, Formbook, and Agent Tesla information stealers.