In Q1 2023, we analysed 130 malicious activities of interest targeting EU institutions, bodies, and agencies (EUIBAs) or their vicinity, and we released 49 Threat Alerts.

When known, the main motive of the attackers was cyberespionage - 46% of the cases. Cyberespionage attacks were, in all likelihood, carried out by threat actors highly likely originating from Russia & China.

Governement, transportation & diplomatic sectors = the 3 most targeted sectors.

We noticed active exploitation of vulnerabilities (as zero-day or n-day) in at least 15 software products likely used by EUIBAs: Microsoft Outlook & IIS, Fortinet appliances, Zoho ManageEngine, Zimbra, and VMWare ESXi.

We also observed breaches affecting at least 6 IT companies actually or possibly servicing EUIBAs.
19 threat actors had been active against EUIBAs or in their vicinity

7 likely of Russian origin, 5 of likely Chinese origin

There was sustained spearphishing activity by two Top Threat Actors – highly likely Russia-linked and China-linked. They focused on the diplomatic sectors

Finally, we observed the emergence of two little known, but dangerous threat actors named Winter Vivern & Dark Pink
We detected significant active scanning, from a known set of infrastructure associated by trusted partners with Chinese threat actors.

We also observed adversaries spoofing EUIBAs or public administrations of EU countries in attempts to lure constituents in phishing attacks.

In a likely cybercrime activity, several EUIBAs reported on attempted delivery of malware disguised as Microsoft OneNote documents.

In our constituency, the most active malware families were Agent Tesla - a major information stealer, Ave Maria - an information stealer and keylogger, SocGolish - used for initial access, and Qbot a.k.a Qakbot - a network-aware worm with backdoor capabilities.