In Q3 2023, we responded to 9 significant incidents

7 of them were due to vulnerability / weakness exploitation in internet-facing software products

2 software products were particularly targeted: Citrix NetScaler & Ivanti Endpoint Manager Mobile (EPMM, formerly MobileIron Core)

These attacks were quickly detected & mitigation measures implemented

None of the significant incidents could be attributed to known threat actors or activity clusters
We analysed 126 malicious activities of interest targeting EU institutions, bodies, and agencies (EUIBAs) or their vicinity.

We released 46 Threat Alerts.

When known, the main motive of the attackers was cyberespionage.

Activities were sighted in 10 sectors of interest, with the 3 most targeted being government, diplomacy & finance.
Attackers targeted at least **33 software products** used by EUIBAs

- Vendors of these products include Adobe, Apple, Cisco, Citrix, Fortinet, Ivanti, Microsoft & VMWare
- In addition, a breach affected an **IT company** delivering services to EUIBAs
We have been tracking 13 Top Threat Actors (TTAs)

However, we did not notice any significant exposure of EUIBAs to these TTAs

33 threat actors were active against EUIBAs or in their vicinity
Vulnerability exploitation in public facing products for initial access was used at least as often as (spear)phishing.

At a much lower scale, we keep observing activity involving drive-by compromises or the use of removable media as initial access methods in the vicinity of EUIBAs.

The most observed malware strains were FormBook & Agent Tesla.