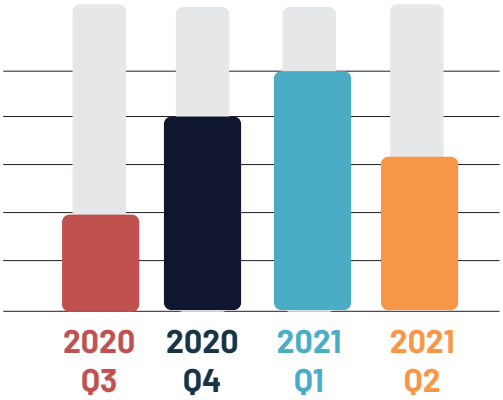
Direct Threats to EU Institutions, Bodies, and Agencies

2021 Q2: EUIBAs | Significant incidents

5 significant incidents affected EU institutions, bodies, and agencies:

- Two exploited the Microsoft Exchange ProxyLogon vulnerabilities. One has been attributed to a Chinese threat actor.



Since the beginning of 2021, CERT-EU has already recorded 12 significant incidents (compared to 13 during the whole of 2020).

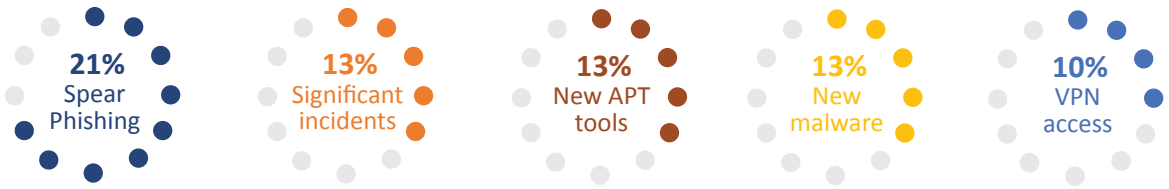
Significant threats - CERT-EU released 22 threat alerts (compared to 20 during 2021 Q1) :

- At least 8 phishing campaigns in Europe have targeted sectors of interest for EUIBAs, such as government and diplomacy.
- In 4 operations, attackers breached VPN remote accesses systems.
- On 5 occasions, CERT-EU has alerted on new tools or malware used by advanced threat actors.

CERT-EU is currently tracking **13** top threat actors due to their interest in targeting EUIBAs, their high level of expertise and resources.

EUIBAs have been exposed to the activity of 7 of them during 2021 Q2. This is unprecedented and indicates a very high level of threat.

Top 5 threat alert types released by CERT-EU



Tactics & Techniques

Threat actors are preparing their attacks by acquiring infrastructure (servers, domains), obtaining capabilities (digital certificates, vulnerabilities) or compromising assets (email accounts, web services).

The most observed initial access vectors remain spear phishing and the compromise of public-facing applications.

Supply chain attacks are comparatively less frequent but much more devastating.

Threats in Europe

Top 3 Ransomware-as-a-Service operations:

Ransomware: 65% increase compared to 2021 Q1

Victims listed on DLS (data leak sites): **112** in 2021 Q1 - vs - **185** in 2021 Q2

State-sponsored: At least 4 distinct Russian threat actors have been observed.
They have engaged in large-scale cyber intrusion and influence operations.
Russia is also conducting cyber-enabled hybrid and disinformation campaings in Europe, and computer-generated deepfake persona to deceive EU politicians.

Hacktivism: "Hack-and-delete" and "Hack-and-leak"

Influence operations: Chinese threat actors are running influence operations in the European cyber space, using techniques such hack-and-leak, influence-for-hire networks or deepfakes.