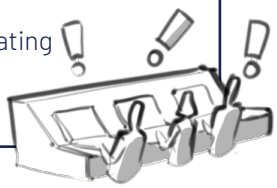
Threat Landscape Report 2022 Q2 - Executive Summary

Direct Threats to EU Institutions, Bodies and Agencies

DIRECT THREATS

No significant breach has been recorded in EUIBAs during Q2 2022.

However, a number of noteworthy direct attacks were observed. These include:
A case of high-profile impersonations on WhatsApp, Signal and Telegram, one Emotet campaign impersonating an EUIBA and targeting several EU countries, and cases where the Raspberry Robin worm was installed via infected USB devices.



Attacks in the vicinity:

We released 39 threat alerts to warn of malicious activities detected within or in the vicinity of EUIBAs.

- In 67% of the cases the malicious activity was of cyberespionage nature.
- In a quarter of the cases, at least one EUIBA had been targeted. The governmental sector was the most targeted (41% of the cases).
- Vulnerability exploitation was the primary method used by attackers (38% of the cases).
- Flaws in technologies such as Android, VMware, MS Exchange, MS Office, AWS and Confluence were actively abused.

Overall, attacks in the vicinity of EUIBAs were more opportunistic than targeted, compared to Q1 2022.

Threat actor activity:

In Q2 2022, we have been tracking 11 Top Threat Actors (TTAs).
- 6 of them were sighted (active) but, and to the best of our knowledge, there had been no breach. Well known groups that are highly likely Russia-sponsored continue to be active.
- 2 relatively new groups, allegedly of Chinese origin, have been seen for the first time in the vicinity of EUIBAs.

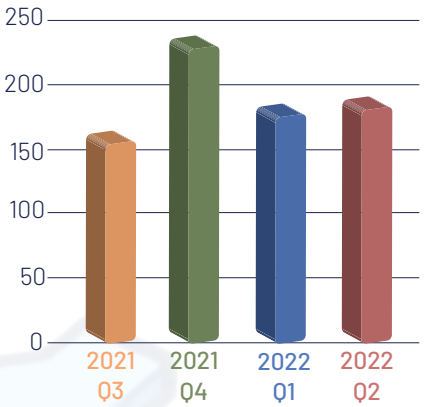
THREATS IN EUROPE

Russia's war on Ukraine.
3 main categories of cyber attacks related to Russia's war on Ukraine were observed:
1. Targeted intrusions, mainly against Ukraine, which are reportedly attributed to a number of Russian threat actors including APT28, Gamaredon, and Sandworm.
2. Disruptive attacks, often including wiper, against critical infrastructure (energy, internet access, ...)
3. Hacktivist attacks (DDoS, defacements, data leaks), affecting European countries, Ukraine, or Russia, and usually having a low impact.

Cyberespionage.
Prominent Russian threat actors Gamaredon, Turla, APT29, and Calisto have been active in various European countries.
We have also been made aware of cyberespionage campaigns conducted by Chinese groups such as Mustang Panda, APT10, Gallium, and Aquatic Panda.
New cases of infection with malware sold by private sector offensive actors (PSOAs) have been reported in Europe.

Ransomware victims in EU

source: OSINT



Cybercrime.
Ransomware victims have been identified in at least 20 different European countries. The 6 most targeted sectors are legal & professional services, manufacturing, retail, construction & engineering, healthcare, and technology.
Beside ransomware, Emotet was one of the most active piece of malware in Europe.

THREATS IN THE WORLD

China reportedly continues to conduct cyberespionage campaigns against targets in Asia, the Middle East, North America and Europe.

The majority of cyber activity coming out of or targeting Russia was linked to Russia's war on Ukraine. Israel, the US, India and the Middle East remain the targets of allegedly Iranian threat actors.

North Korean threat actors expanded their activity from targeting cryptocurrency exchanges to the exploitation of decentralised finance (DeFi) protocols.