Threat Landscape Report 2022 Q3 - Executive Summary

DIRECT THREATS TO EU INSTITUTIONS, BODIES, AND AGENCIES

- A threat actor breached the network of an EUIBA through a supply-chain attack, causing a significant incident.
- In early July, an Emotet spear-phishing campaign targeted at least 24 EUIBAs.

Attacks in the vicinity

We released 35 threat alerts to warn of malicious activities detected in the proximity of EUIBAs.

- In 63% of the cases, the malicious activity was of cyberespionage nature.
- The government, diplomatic and defence sectors remain the most targeted.
- 51% of the attacks leveraged spear-phishing for initial access and 20% vulnerability exploitation (zero-days or n-days).

As observed in Q2 2022, attacks in the vicinity of EUIBAs remain more opportunistic than targeted, compared to Q1.

Threat actor activity

- In Q3 2022, we have been tracking 11 Top Threat Actors (TTAs), the same number as in Q2.
- We detected activity by 3 of them, but there was no breach.
- We also observed activity by 6 other malicious groups.
- Well-known Russian groups have been active, especially Gamaredon.

Attack patterns & malware

- Credentials harvesting has been the most observed technique.
- Threat actors have continued to spoof the identity of EUIBAs in their phishing campaigns.
- The Agent Tesla information stealer has returned and we observed it in 7 EUIBAs.

THREATS IN EUROPE

Russia's war on Ukraine.

Cyberattacks related to Russia's war on Ukraine belong to 3 main categories:

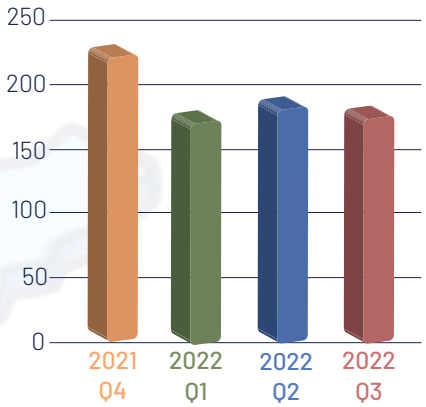
1. Targeted intrusion attempts by 4 major Russian threat actors in particular.
2. Disruptive attacks, mainly claimed by pro-Ukrainian hacktivists against Russian critical infrastructure, with unknown impact.
3. Hacktivist attacks (DDoS, defacements, data leaks) claimed by pro-Russian hacktivists, against Ukraine and EU countries. At least 7 groups have been active. They seek visibility but the technical impact of their attacks is so far low.

Cybercrime.

- Based on information from public sources and data leak sites (DLS), we have recorded 186 attacks against European entities.
- Lockbit has been the most active ransomware family in Europe with 86 reported victims. Lockbit accounted for almost 50% of the breaches in the continent.
- The private sector has remained more targeted than the public sector.
- Notable attacks targeted municipalities and critical sectors such as energy, healthcare and transportation.

Ransomware victims in EU

source: OSINT



Cyberespionage.

- 5 Russian, 2 Chinese and 2 North Korean threat actors have been active in various European countries.
- We also recorded new cases of private sector offensive actor (PSOA) operations.

Disruption and hijacking.

- A combination of uncoordinated cybercriminal and state-sponsored cyberattacks caused notable disruptions in governmental services and critical infrastructure in the Western Balkans.