CERT-EU 10 years

TLP:WHITE

Threat Landscape Report 2022 Q1 - Executive Summary

Direct Threats to EU Institutions, Bodies and Agencies

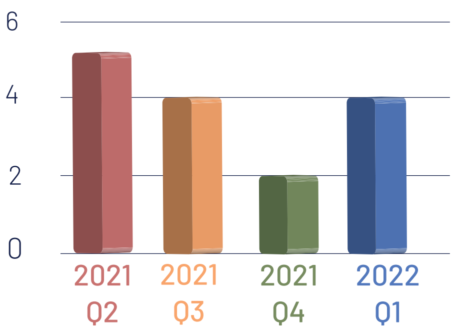
INCIDENTS

There were 4 new significant incidents affecting EUIBAs in Q1 2022.

In two cases, attackers abused valid user credentials to access online platforms.

In the remaining cases, attackers brute forced a Microsoft Exchange Web Service (EWS) instance.

Significant incidents that affected EUIBAs



Top threat actors:

CERT-EU has been tracking 11 Top Threat Actors (TTAs).
Seven of them, likely of Chinese and Russian origin, were active against EUIBAs in Q1.
The 4 others were active in the vicinity of the EU and elsewhere.

THREATS

More than a dozen EUIBAs were targeted by a threat actor in a password spraying campaign against Microsoft Exchange services.

At least 7 spear-phishing campaigns highly likely linked to state-sponsored threat actors targeted EUIBAs.

CERT-EU released 42 threat alerts in Q1 2022. Nearly three quarters of them were related to cyberespionage activities.

Also, three quarters of them were related to spear phishing attacks.

In 23% of the attacks reported in threat alerts: Diplomatic entities (embassies, delegations or representation in third countries) were especially targeted. *This figure is unprecedented.*

It is likely that the Russia's war on Ukraine has stimulated the interest of state-sponsored threat actors in collecting intelligence from governmental entities in the EU.

Moreover, EUIBAs were exposed to the activity of non-top threat actors:
4 being highly likely state-sponsored groups, 3 cybercriminals and the last 2 having unknown motives.

Techniques:

There was a significant number of brute force / passwords spraying attacks against Microsoft Exchange services.
At least 7 EUIBAs were targeted in impersonation attacks. At least 5 EUIBAs have detected cases in which attackers spoofed legitimate Microsoft Teams messages.

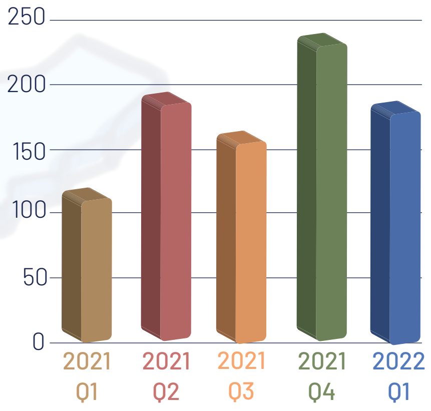
Threats in Europe

Russia's war on Ukraine. Overall, incidents related to Russia's war on Ukraine have been the majority of cybersecurity cases in Europe. One of most serious events, the disruption of the KA-SAT satellite-based internet service in some parts of Europe was due to a cyber-attack with spillover consequences.
According to open source intelligence (OSINT), the cyber attacks in Ukraine were of different nature: disruptive attacks targeting internet service providers (ISPs) and critical infrastructure, wiper attacks aiming at incapacitating key Ukrainian networks, phishing/targeted intrusions to maintain presence in Ukrainian networks and steal information, DDoS attacks (with limited effects) aiming at shifting the attention from a number of information operations on social media and other attacks.

Cyberespionage. Several threat groups were active in Europe. Most of them are likely of Russian origin. There was also a Chinese espionage activity, making use of lures related to Russia's invasion of Ukraine. Ministries of Foreign Affairs and the government sector were particularly targeted. Finally, new cases related to the use of the Pegasus spyware were reported in Europe.

Ransomware victims in EU

source: OSINT



Cybercrime. Ransomware remained the most significant cybercrime threat in the EU. There were cases of ransomware in particular in the oil supply, aviation, postal services, and telecommunications sectors, which, due to the geopolitical situation, caused concern as possible cyberwar actions. The three most active ransomware operations in Europe were Lockbit, Conti and Alphv.