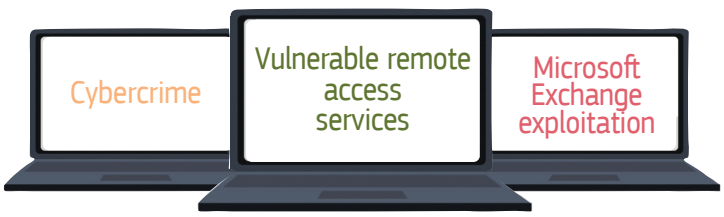
Threat Landscape Report - Q1 2021

Executive Summary

Direct threats to EUIBAs - (European Union institutions, bodies, and agencies)

During the first quarter of 2021, 7 significant incidents affected EU institutions, bodies, and agencies.



One was of a cybercrime nature, as an infection chain was initiated and would have led to a ransomware infection if it wasn't stopped in its tracks.

Two were related to the global Microsoft Exchange ProxyLogon exploitation.

Three were caused by highly-skilled threat actors who exploited unknown vulnerabilities in remote access services.

The motive behind the remaining significant incident is unclear.

CERT-EU released 20 threat alerts related to:

- Spear phishing campaigns in sectors of interest to EUIBAs
- High-profile cybercrime malware activity
- Techniques, tactics and procedures (TTPs) used in significant incidents
- Active exploitation of VPN vulnerabilities, potentially compromised software, and recent APT tools

The two most used initial access techniques against EUIBAs are currently spear phishing and the exploitation of public-facing services and applications such as remote access services.

Finally, at least 5 out of the 12 top threat actors tracked by CERT-EU have been active during 2021Q1.

Threats in Europe

Ransomware remains the top cybercrime threat in Europe with at least 112 victims in Q1, the highest score ever recorded by CERT-EU.

Several phishing campaigns spoofing public administration attempted to distribute advanced malware.

DDoS attacks targeted European ISPs.

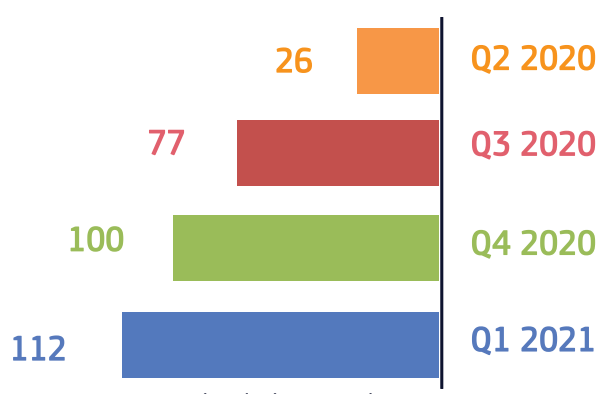
SIM swapping and SMS phishing campaigns were observed in some countries.

The exploitation of Microsoft Exchange ProxyLogon by APT and cybercrime groups is widespread in Europe.
This campaign is still ongoing.

As regards to cyberespionage, additional victims of the SolarWinds Orion supply chain attack were found in Europe.

At least six state-sponsored cyberespionage threat actors have been active in Europe, targeting governmental and private organisations.

Known RaaS victims in Europe



Source: data leak sites and open sources

Affected sectors: health, local administration, finance, managed service providers, etc.

At least 16 major Ransomware as a Service (RaaS) operations are currently active in Europe. Two of them have been disrupted by law enforcement operations.