Threat Landscape Report 2021 Q4 - Executive Summary

Direct Threats to EU Institutions, Bodies, and Agencies

INCIDENTS

2 significant incidents affected EUIBAs.

One involved phishing emails sent from a compromised EUIBA email address.

The other one was highly likely due to a Chinese threat actor who exploited ProxyShell on an exposed MS Exchange server.

Overall, in 2021, CERT-EU has recorded 17 significant incidents, compared to 13 in 2020.

THREATS

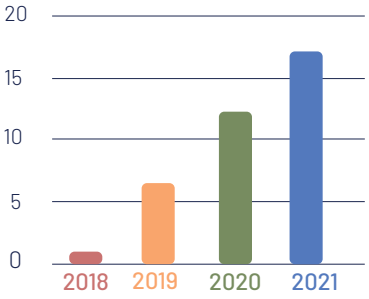
CERT-EU alerted EUIBAs on 28 cyberespionage campaigns, 12 cybercrime activities and 1 information operation.

A number of EUIBAs were found exposed to Log4Shell – however, no successful exploitation has been observed so far.

In 20 malicious activities, the threat actors were targeting one or more sectors of interest for EUIBAs (government & administration, diplomacy, defence, or aerospace).

In 12 cases the threat actor was highly likely Russian, in 6 cases highly likely Chinese, in 3 cases allegedly Iranian, and in 2 cases purportedly North Korean.

Significant incidents that affected EUIBAs since 2018



Top threat actors:

CERT-EU has been tracking 13 top threat actors.
One of them, highly likely of Chinese origin, represents currently a critical threat.
Four threat actors represent a high threat, three a medium threat, and five a moderate threat.

Techniques:

The dominant attempted initial access method has been spear-phishing, followed by exploitation of exposed and vulnerable applications.

Threats in Europe

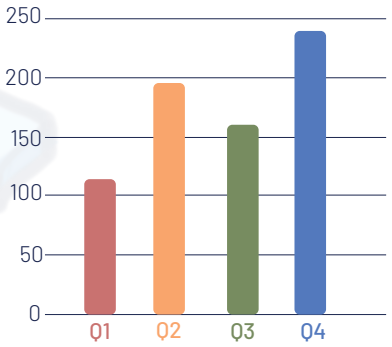
Ransomware continues to be the most prolific type of cybercrime activity both in Europe and worldwide. However, the number of ransomware attacks targeting government entities (e.g. municipalities, educational institutions, hospitals) has diminished in Q4 2021. At least 230 victims have been claimed in Europe (source = OSINT and data leak sites).
Lockbit, Conti, Spook, Grief and Hive have been the top 5 most active RaaS in Europe.

APT29, a highly likely Russian threat actor, and Ke3chang, a highly likely Chinese cyberespionage threat actor have been particularly active with some of their targets located in Europe.

A number of nation-state threat actors have attempted Log4Shell exploitation.

Information operation activities originating in China and Russia have been observed in Europe.

RaaS victims in EU 2021



Threats in the World

China continues to conduct cyberespionage against dissidents and Chinese nationals both domestically and abroad. The APT27 threat actor is targeting multiple critical sectors worldwide. Constant inauthentic social media activity supports political interests of China.

Russia is enforcing internet controls by fining Google, Meta, and Twitter for providing prohibited content, including calls to protests. APT29 is very active, seeking to conduct supply chain attacks and spear-phishing against non-profits and foreign policy entities.

In **Iran**, cyber threat actors are looking for US voter information and also access to SCADA systems. Iranian petrol stations stopped working due to a cyber attack.

North Korea continues to lure technical experts on social media with fake job offers in order to compromise their employers. An increasing number of formerly known North Korean cyberespionage actors are now also conducting financially motivated attacks.