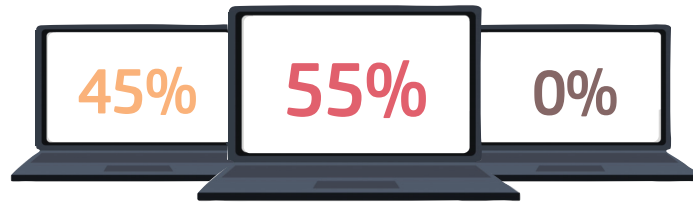


Direct Threats to EU Institutions, Bodies and Agencies

2020 Q3 : EU-I | Identified Threat Actors



EU institutions, bodies, and agencies (EU-I) are usually facing threats from 3 categories of threat actors: **cybercriminals**, **cyberespionage**, and **hactivist groups**.

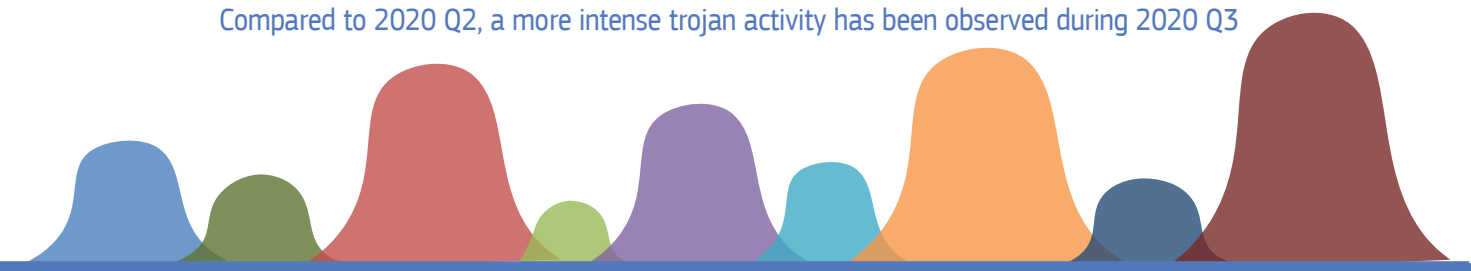
Cyberespionage : CERT-EU observed targeted intrusion attempts against **several EU-I**. In two cases, the threat actor compromised the VPN services used by the victims to allow their staff to work from home during the COVID-19 pandemic.

Cybercrime : **4 major criminal collectives** have been observed attempting to infect EU-I. **Mummy Spider** (a group known as the operator of the Emotet malware) is among them.

Hactivist groups : No hactivist activities against EU-I have been attributed to a specific threat actor.

Tactics & Techniques

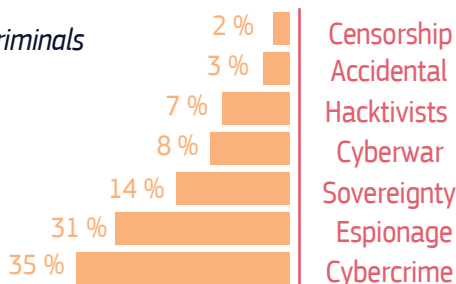
Compared to 2020 Q2, a more intense trojan activity has been observed during 2020 Q3



The **top 3** most observed tools or pieces of malware are **Emotet** (21 EU-I), **LokiBot** (6 EU-I) and **Agent Tesla** (5 EU-I). **DoS** and **defacement attacks** are slightly on the rise. **Coronavirus** outbreak has been again the most observed subject in **generic phishing attacks**. Cloud-related phishing also remains significant. There have been **targeted phishing** attempts, using a spoofed EU-I email address, to lure recipients in at least 4 EU-I. Attackers are also using **fake domains** looking like legitimate EU-I ones. The discovery of **leaked EU-I staff credentials** associated with their professional email addresses on publicly accessible repositories remains a major issue: **48 distinct EU-I** affected. A steady number of **impersonations of EU official accounts** have been detected on LinkedIn, Facebook, YouTube, Twitter, and Instagram.

Sectorial Threat Landscape: Government and Administration

In several countries, cybercriminals have impersonated public administrations in malware distribution campaigns.



Geographical Threat Landscape: Europe

Ransomware remains the most significant cybercrime threat in Europe

