CERT-EU

TLP:WHITE

Direct Threats to EU Institutions, Bodies and Agencies

2020 Q2 : EU-I | Threat Actors

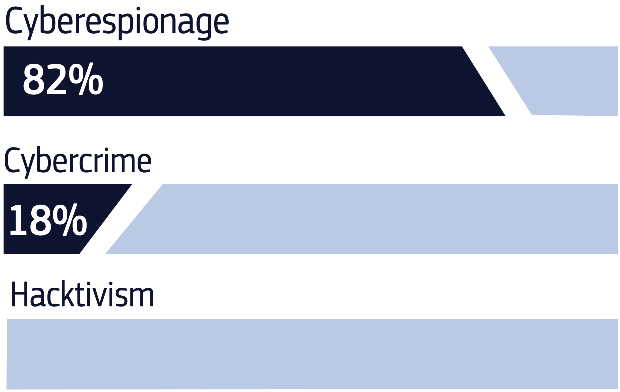
EU institutions, bodies and agencies (EU-I) face threats from 3 categories :

Cybercrime - 4 major criminal collectives have been observed attempting to infect EU-I: TA505 (aka Indrik Spider), TA542 (aka Mummy Spider) who is the operator the Emotet malware, Crypto-Core, and for the first time within EU-I: FIN7.

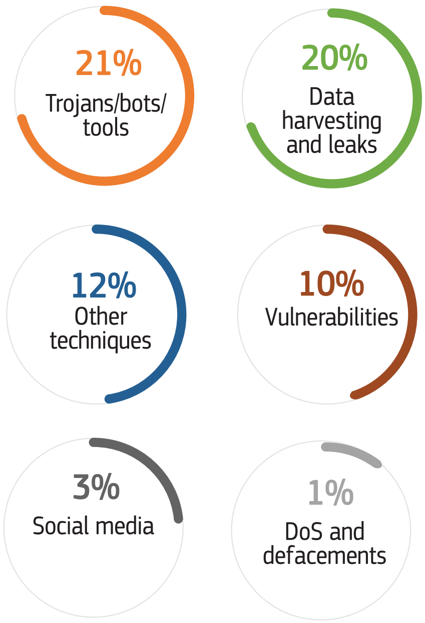
Cyberespionage - Activity from 11 entities has been observed: cyberespionage continues to be a steady occurrence and this has led to 2 serious attacks.

Hacktivist groups - No hacktivist activities against EU-I have been attributed to a specific threat actor.

Attributable activity



Tactics & Techniques



- CERT-EU has responded to 2 significant incidents associated with unidentified APT groups. Additional signs of activity were observed but no incidents have been confirmed.

- A less intense trojan activity has been observed, with at least 15 malware families active in a total of 31 observed cases in the last quarter.

- In 2020 Q2, a slightly higher number of DDoS attacks have been reported to CERT-EU.

- The coronavirus outbreak and cloud-related matters have again been the most observed subjects in generic phishing attacks.

- Targeted phishing and initial access increased within EU-I. A number of EU-I have seen corporate email addresses being spoofed (4 EU-I).

- The discovery – on publicly accessible repositories – of EU-I staff credentials associated with their professional email addresses remains a major issue (28 EU-I).

- A steady number of impersonations of EU official social media accounts have been detected on LinkedIn, Facebook, YouTube, Twitter, and Instagram.

Sectorial Threat Landscape: Government and Administration

Public administrations in several countries have fallen victim to COVID-19 themed advanced business email compromise (BEC) attacks.

A cyberespionage campaign targeted public-private supply chains for the procurement of coronavirus personal protective equipment (PPE) such as face masks and medical gear.

Hacktivist operations have affected websites of public administrations worldwide.

Also, public administrations have been victim of breaches exposing personal data of citizens.

Regional Threat Landscape: Europe

At least 26 organisations in 14 European countries (mostly from the private sector), have been affected by big game hunting (BGH) ransomware attacks involving at least 9 significant ransomware families.

Several cybercrime campaigns have abused beneficiaries of COVID-19 economic aid across Europe.

State-backed disinformation campaigns (originating in CN and RU) aimed at European countries were carried out leveraging social networks.

A significant number of data leaks, involving personal information, have been detected in several countries.