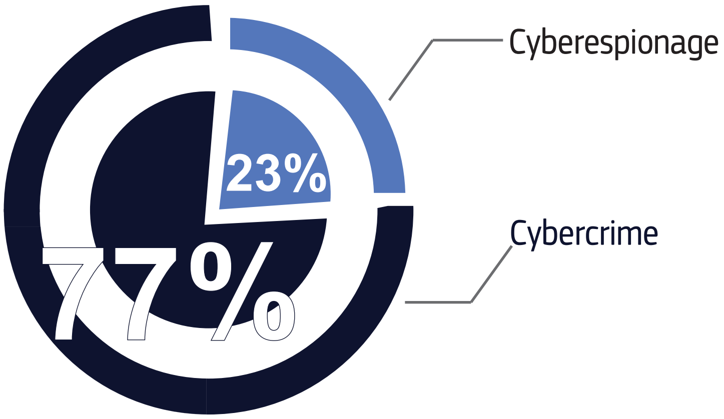
CERT-EU

TLP:WHITE

Direct Threats to EU Institutions, Bodies and Agencies

2020 Q1 : EU-I | Threat Actors



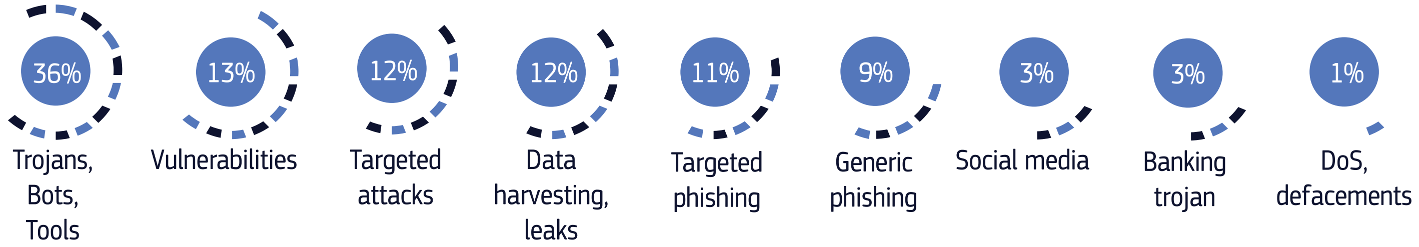
EU institutions, bodies and agencies (EU-I) usually face threats from 3 categories :

Cybercriminals - 3 main eCrime groups have been identified: Magecart groups (deploying credic card data skimmer on ecommerce websites), TA505 (operating several crimeware including Dridex), Mummy Spider (operator of the Emotet malware).

Cyber espionage - Within EU-I, 5 main espionage highly likely state-sponsored threat actors have been observed.

Hacktivist groups - Denial of services (DoS) attacks have been observed but could not be attributed to a specific threat actor.

Techniques & Tactics



- ○ Targeted attacks have been a steady trend throughout 2020 Q1 EU-I.
- ○ At least 15 new malware families for a total of 31 were observed in this first quarter.
- ○ EU-I staff are continuously exposed to credit card data web-skimming activities.
- ○ A reduced number of DDoS attacks have been reported to CERT-EU, compared to 2019 Q4.
- ○ The corona virus outbreak and cloud related matters have been the most observed subject in generic phishing attacks.
- ○ The impersonation of a contractor/service provider, several cases of typosquatting EU-I domain names, and cases of impersonation of EU-I Cabinet member or director have been the most significant forms of tailored attacks.
- ○ The discovery – on publicly accessible repositories – of EU-I staff credentials associated to their professional email addresses remains a major issue.
- ○ 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

Public administrations are victims of sophisticated cybercrime attacks including advanced business email compromise and ransomware big game hunting.

State-sponsored attacks target administrations all around the world.

Public administrations in several countries inadvertently exposed personal data of millions of citizens on misconfigured, publicly accessible IT resources.

Geographical Threat Landscape: Europe

Ransomware remains the most substantial cyber-crime threat in Europe, with at least 10 countries reporting major breaches in several sectors.

Diverse hacktivist campaigns (defacement, denial of service) are carried out by nationalist or ideological groups.

Many European countries have reported cyber-criminal abuse of the COVID-19 crisis: COVID-19 themed phishing or spam, malware distribution, malicious Apps, DDoS attacks against healthcare organisations, COVID-19 themed fraudulent or fake websites, and state-sponsored influence campaigns.