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, CryptoCore, 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.

Tactics & Techniques

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.

Cert-Eu, CERT for the EU Institutions, Bodies and Agencies

https://cert.europa.eu or services@cert.europa.eu

CERT-EU, CERT for the EU Institutions, Bodies and Agencies