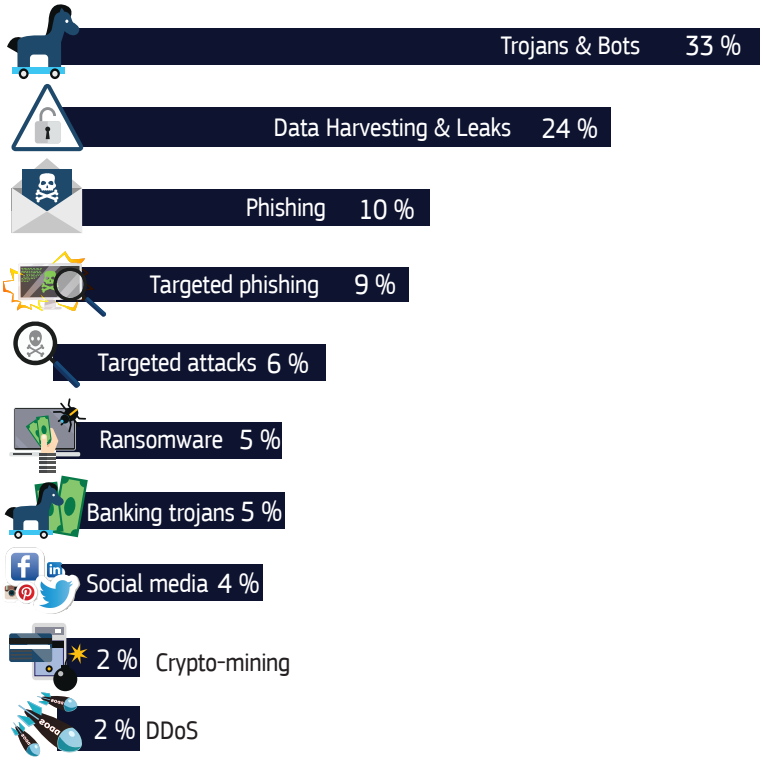
Direct Threats to EU institutions/bodies/agencies

2019 : EU-I | Techniques,Tactics, Procedures



Targeted attacks have been a steady trend throughout 2019 within EU institutions, bodies and agencies.

Trojan and Bots: an intense activity has been observed within EU-I.

Data Harvesting & Leaks: active attempts to harvest cloud service credentials have been observed. The use of EU-I staff professional email addresses for private web accounts expose them to leakage.

Phishing: this technique has remained an ongoing threat that includes phone scams, invoices, purchases, payments, etc...

Targeted Phishing: a rise in phishing messages has been observed in 2019; impersonation of EU-I employee or training provider, EU member state's administration.

Ransomware: several ransomware families have been observed, but no successful infection has been reported. Criminal crypto-mining remains an active threat, although the number of observed attempts has declined compared to previous quarters.

DDoS - Distributed Denial of Service: several cases have been reported to CERT-EU, yet they did not cause any significant impact.

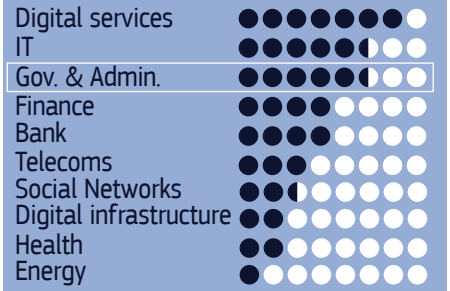
Ransomware: several ransomware families have been observed, but no successful infection has been reported.

Social media: a number of fake accounts impersonating EU-I members have been detected (Facebook, Twitter, Instagram).

Sectoral threats

TOP 10 TARGETED SECTORS

2019



FOCUS ON: *Government and Administration*

Public administrations in several countries have once again fallen victim to ransomware attacks.

Cybercriminals have spoofed public administrations to lure victims during malware distribution campaigns. The procurement services of administrations are attractive targets for business email compromise frauds or credential harvesting campaigns.

Hacktivist activities (denial of service attacks, web defacements, and intrusions) against governmental entities sometimes coincide with increased social unrest in the country.

Geographical threats

FOCUS ON: *EUROPE*

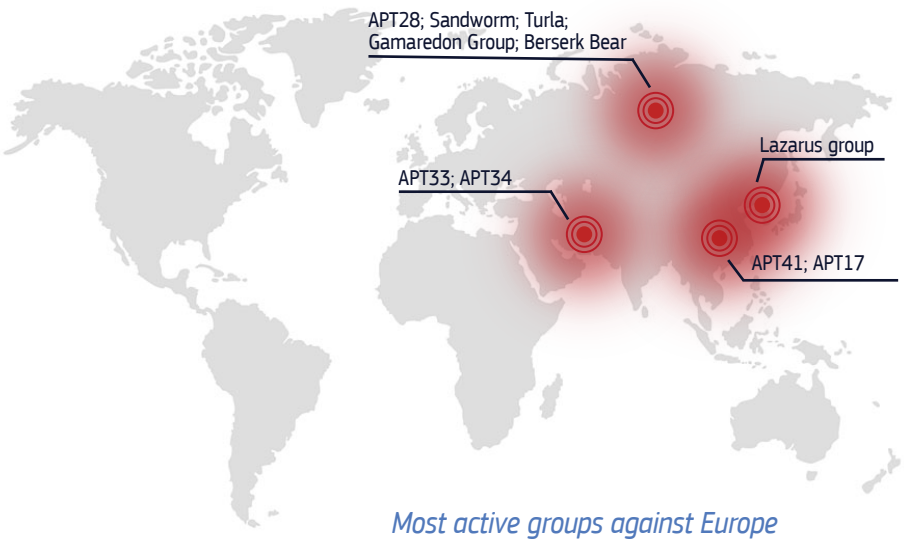
Ransomware attacks represent a major threat for all sectors (administrations, universities, digital services, hospitals, etc.).

The Cobalt cybercriminal group has been the most active against European financial institutions.

Cyberespionage operations have affected important sectors (industry, foreign affairs, government).

Disinformation campaigns are frequently observed as part of hybrid operations.

Politically motivated hacktivists have carried out campaigns (DDoS, intrusions, disruptions) in some countries. Large European companies (e.g. hotels, telecom operators) have been compromised resulting in large personal data leaks.



Most active groups against Europe