Cybersecurity Insights

Paris 2024 Olympic Games: a breeding ground for cyber threats

PARIS 2024 OLYMPIC GAMES IN NUMBERS

15,3
million visitors expected

An endless pool of potential victims for cybercriminals.

206
nations represented

The Olympic Games are the perfect tribune to any political revendication movement.

2,6
billion of expenses

The risk of cyberattacks increases where financial gain opportunities are exponential

14 850
athletes

As proven in past sporting event, data theft on this specific population can have a geopolitical impact on a country.

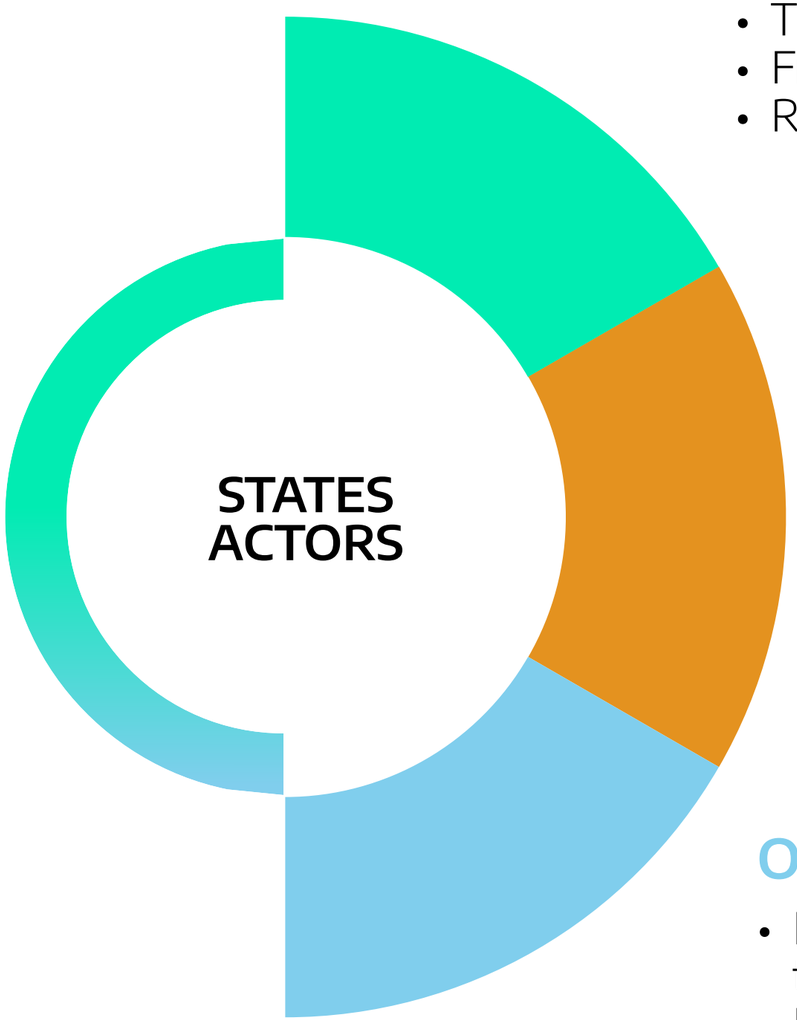
1900
service providers

Companies from diverse sectors like logistics or construction will provide services before and during the Olympics, increasing their exposure to cyberattacks.

34 000
journalists expected

Journalists will be gathered in the same area for short period of time, putting them at a higher risk for both targeted espionage campaigns and opportunistic attacks.

ESPIONAGE CAMPAIGNS



Targeted intelligence operations

- Diplomats and government officials
- High profiles in the business world
- Think tank
- French and foreign authorities
- Reporters

Opportunistic mass spying

- Dissidents, political exiles
- Diasporas from territorial/cultural dispute
- Reporters
- Activists

Opportunistic economic and/or industrial espionage

- High-profile people in the business world and think tanks
- Employees in strategic industries and companies

INFLUENCE OPERATIONS

“France has detected a propaganda network called “Portal Kombat”. In order to mislead European public opinion, particularly in France, this network, made up of so-called digital information portals, spreads pro-Russian content promoting the Russian invasion in Ukraine and denigrating the Ukrainian authorities.”
Stéphane Séjourné, Minister for Europe and Foreign Affairs, February 12th, 2024.

STATE-SPONSORED THREAT ACTORS

GAMES OFFICIALS, ATHLETES, GAMES INFRASTRUCTURES

- Hack-and-leak campaigns
- Sabotage operations (wipers) to avenge French and allies’ position on current conflicts and wars.
- Destabilisation campaigns
- Disruption via DDoS campaigns

HACKTIVISTS

GAMES INFRASTRUCTURES, OFFICIAL MEDIAS, TELECOMMUNICATION ENTITIES

- Low level impact’s disruption via DDoS
- Websites defacement to promote political/ideological revendication
- Hijacked broadcasting to promote political/ideological revendication
- Disinformation campaigns
- Infrastructure sabotage

CYBERCRIME

Government bodies and public services

- Ransomware
- Infostealer campaigns
- Access brokers

Entreprise

- Ransomware
- Spear-phishing campaigns
- CEO fraud

Population

- Phishing and variants
- Tickets scams
- Fraud

1

At least 1 ransomware per 2-3 days in France