# France accuses Russian military intelligence of major cyber-attacks including on Macron’s 2017 campaign



France has formally accused Russian military intelligence of orchestrating a series of significant cyber-attacks, including an assault on Emmanuel Macron’s first presidential campaign in 2017, as well as attacks on French media and organisations connected to the 2024 Paris Olympics. This disclosure, made by the French foreign ministry on Tuesday, marks the first time the French government has directly attributed these incidents to Russian state actors.

The 2017 cyber-attack against Macron’s presidential campaign involved the theft and dissemination of thousands of internal campaign emails and other documents, some of which were reportedly falsified. The campaign materials were released online shortly after the official midnight deadline for electioneering ahead of the second round of the presidential election. Despite the extensive data leak intended to influence voters, the foreign ministry stated, “Thousands of documents were stolen and disseminated in the hope of manipulating voters, but the manoeuvre failed to have any real impact on the electoral process.” Macron went on to win the election against far-right candidate Marine Le Pen.

In addition to the 2017 cyber-attack, the French foreign ministry has blamed Russian military intelligence, specifically a unit known as APT28 or Fancy Bear, for targeting several other key French entities. These include the 2015 hacking of the French public broadcaster TV5Monde, an attack in which Russian hackers masqueraded as Islamic State militants to sow confusion and panic within France. The ministry further revealed that since 2021, this branch of Russian military cyber operatives has targeted a wide range of French institutions across defence, financial, and economic sectors. Among these targets was a sports organisation involved in the upcoming Olympic and Paralympic Games hosted by Paris in 2024.

APT28 is notorious for its global cyber-espionage activities, having been linked to numerous attacks worldwide, including interference in the 2016 United States presidential election, where it was accused of leaking Democratic Party and Hillary Clinton campaign emails. A report released by the French Cybersecurity agency (ANSSI) elaborated that since 2021, APT28 has been used to extract strategic intelligence from entities across France, Europe, Ukraine, and North America.

French Foreign Minister Jean-Noël Barrot commented on the ongoing cyber threats, stating, “Russia’s military intelligence has been carrying out cyber-attacks against France for several years using a method known as APT28.” Highlighting the persistent nature of these cyber incursions, Barrot emphasised that the French government, in partnership with international allies, is committed to anticipating, deterring, and responding to Russia’s cyber activities appropriately.

This alert follows warnings issued in September 2024 by various international intelligence agencies, including German authorities, cautioning Nato member states about the heightened risk of cyber-attacks by Fancy Bear operations.

In its official statement, the French foreign ministry condemned Russia’s use of APT28, asserting, “France condemns in the strongest terms the use by Russia’s military intelligence service of the APT28 attack group, at the origin of several cyber-attacks on French interests.”

The techniques employed by APT28 typically involve targeting personal email accounts to retrieve sensitive information and gain broader access to systems, facilitating espionage and potential disruption.

The Guardian is reporting on these developments as part of a broader examination of ongoing cyber warfare threats and the geopolitical tensions surrounding state-sponsored hacking activities.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.reuters.com/world/europe/first-france-accuses-russian-intelligence-repeated-cyber-attacks-2025-04-29/> - This article reports on France's formal accusation of Russian military intelligence orchestrating cyber-attacks, including the 2017 assault on Emmanuel Macron's presidential campaign and attacks on French media and organizations connected to the 2024 Paris Olympics.
* <https://www.lemonde.fr/en/france/article/2024/07/24/russian-spy-arrested-in-paris-after-alleged-plan-to-destabilize-olympic-games_6696920_7.html> - This piece details the arrest of a Russian agent in Paris accused of planning actions to destabilize the Paris Olympics, corroborating the claim of Russian interference in the 2024 Games.
* <https://apnews.com/article/a2fef5133e4ea142bfcb4111d987ff50> - This article discusses French cybersecurity teams preparing for potential cyber-attacks during the 2024 Paris Olympics, highlighting the threat of Russian interference.
* <https://www.ft.com/content/6ab6efea-c23e-428e-b4ab-4eb8fc49c6bb> - This report covers Russia's disinformation campaigns and cyber threats targeting the Paris Olympics, supporting the claim of Russian interference in the 2024 Games.
* <https://www.lemonde.fr/en/sports/article/2024/05/07/paris-olympics-are-prime-target-for-cybercriminals_6670644_9.html> - This article highlights the Paris Olympics as a prime target for cybercriminals, with significant threats from state actors and criminal groups, including Russian intelligence operatives.
* <https://www.axios.com/2017/12/15/polls-open-in-paris-1513302109> - This piece reports on the opening of polls in Paris for the French presidential election, mentioning the impact of hacked campaign emails linked to Macron, attributed to the GRU (Russian military intelligence directorate).
* <https://www.theguardian.com/world/2025/apr/29/france-says-russian-hackers-behind-attack-on-macrons-2017-presidential-campaign> - Please view link - unable to able to access data