The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

U.K. Accuses Moscow of Cyber Campaign Against Top Politicians

By AFP

December 07, 2023

U.K. Foreign Minister David Cameron. **Simon Walker / No 10 Downing Street**

The British government on Thursday accused Russian security services of engaging in a sustained cyber espionage campaign against top politicians, journalists and NGOs.

Russia has been suspected of meddling in U.K. politics before, including the divisive 2016 Brexit referendum, however, the Conservative Party-led government has been criticized for failing to investigate.

In the latest claims, the British Foreign Ministry said Russia's Federal Security Service (FSB) was behind "unsuccessful attempts to interfere in U.K. political processes" and said it had summoned Russia's ambassador to London about the issue.

"Russia's attempts to interfere in U.K. politics are completely unacceptable and seek to threaten our democratic processes," Foreign Minister David Cameron said in a statement.

"In sanctioning those responsible and summoning the Russian ambassador today, we are exposing their malign attempts at influence and shining a light on yet another example of how Russia chooses to operate on the global stage," he added.

Cameron's office said Center 18, a unit within the FSB, was accountable for "a range of cyber espionage operations" targeting the United Kingdom.

Leaked documents

The British government claimed the FSB targeted parliamentarians from several political parties, with some attacks resulting in documents being leaked in an operation from at least 2015 through to 2023.

The Russian security service also obtained U.K.-U.S. trade documents that were leaked ahead of the U.K. general election in December 2019, it added.

The British Foreign Office said two Russian operatives had been sanctioned for their involvement in the preparation of so-called "spear-phishing" campaigns and "activity intended to undermine the U.K."

Spear-phishing involves an attacker sending malicious links to specific targets "in order to try to induce them to share sensitive information."

The attacker often undertakes "reconnaissance activity around their target" in order to tailor their attacks more effectively, according to the United Kingdom's National Cyber Security Centre (NCSC).

Attackers typically approach targets via email, social media and professional networking platforms, impersonating real-world contacts of their targets, sending false invitations to conferences and events, and sharing malicious links disguised as Zoom meeting URL links.

Targeting officials

In January, U.K. cyber-security chiefs warned that Russia and Iran were increasingly targeting government officials, journalists and NGOs with spear-fishing attacks in order to "compromise sensitive systems."

The NCSC, which part of the U.K.'s signals intelligence agency, urged greater vigilance about techniques and tactics used, as well as mitigation advice.

It said the Russia-based group SEABORGIUM and the Iran-based TA453 had targeted a range of organizations and individuals in the U.K. and abroad throughout 2022.

Last year, a British newspaper reported that suspected Kremlin agents hacked former prime minister Liz Truss's cellphone when she was foreign minister.

The Mail on Sunday reported that they were believed to have gained access to "top-secret exchanges with international partners."

A source told the paper the "compromised" phone has been placed inside a locked safe in a

secure government location after up to a year's messages were hacked, including "highly sensitive discussions" on the war in Ukraine.

The hacking was discovered in the summer of 2022, when Truss was campaigning to become Conservative Party leader to succeed Boris Johnson as prime minister, the paper reported.

Original url:
https://www.themoscowtimes.com/2023/12/07/uk-accuses-moscow-of-cyber-campaign-against-top-politicians-a83353