Russia: UK and US expose global campaign of malign activity by Russian intelligence services

Press release

The UK and US share US concerns about malign activity by Russia and have attributed a cyber attack to the Russian intelligence service.

- UK shares US concerns about a continuing pattern of Russian malign activity
- UK attributes Russia's Foreign Intelligence Service (SVR) was behind SolarWinds compromise

The UK and US are today calling out Russia for carrying out the SolarWinds compromise, part of a wider pattern of activities by the Russian Intelligence Services against the UK and our allies.

Russia's pattern of malign behaviour around the world – whether in cyberspace, in election interference or in the aggressive operations of their intelligence services – demonstrates that Russia remains the most acute threat to the UK's national and collective security.

The UK, alongside its international partners, will continue to defend against Russia's attempts to destabilise our societies.

Foreign Secretary Dominic Raab, said:

> We see what Russia is doing to undermine our democracies. The UK and US are calling out Russia's malicious behaviour, to enable our international partners and businesses at home to better defend and prepare themselves against this kind of action.
>
> The UK will continue to work with allies to call out Russia's malign behaviour where we see it.

The UK can today also reveal for the first time that Russia's Foreign Intelligence Service (SVR) was behind a series of cyber intrusions, including the SolarWinds compromise.

GCHQ's National Cyber Security Centre (NCSC) assess that it is highly likely the SVR was responsible for gaining unauthorised access to SolarWinds "Orion" software and subsequent targeting.

These incidents are part of a wider pattern of cyber intrusions by the SVR who have previously attempted to gain access to governments across Europe and NATO members.

Since the SolarWinds vulnerability was uncovered, NCSC have been conducting extensive activity to understand and mitigate the compromise. While the overall impact on the UK of the SVR's exploitation of this software is low, the NCSC has identified a low single digit number of public sector organisations targeted through the SolarWinds vulnerability. The government, including the NCSC, has been working hard to ensure those affected were rapidly mitigated.

In addition, the UK government is today making available further information about the SVR's cyber programme available here

Published 15 April 2021