Russia: UK exposes Russian involvement in SolarWinds cyber compromise

Press release

The UK government has for the first time today exposed details of the SVR's cyber programme.

The SVR is Russia's civilian foreign intelligence service and is the successor organization to the KGB's First Chief Directorate. It predominantly targets overseas governmental, diplomatic, think-tank, healthcare and energy targets for intelligence purposes. It is technologically advanced, developing capabilities to try to operate undetected against countries in Europe, NATO members and its near neighbours.

A compromise of SolarWinds IT services firm was discovered in December 2020. SolarWinds confirmed 18,000 organisations across the world including US Government departments were affected. The overall impact on the UK of the SVR's exploitation of this software is low. National Cyber Security Centre (NCSC) advice on how to protect against this threat is available

The NCSC has assessed that it is highly likely Russia's Foreign Intelligence Services are responsible for the compromise of SolarWinds software, Orion, and subsequent targeting. Further details on the framework used by the UK Government for all source intelligence assessments, including the probability yardstick, are available from here

SVR cyber actors are known and tracked in open source as: APT29 Cozy Bear The Dukes.

This incident is part of a pattern of behaviour by the SVR, which includes:

Date	Incident	Description

Date	Incident	Description
Ongoing since at least 2011	MFAs and MoD establishments in Europe and NATO member countries	The SVR uses their access to governmental networks across Europe and NATO member countries to collect intelligence information, including that of ongoing geopolitical issues.
Ongoing since at least 2015	Targeting research institutes and think tanks.	The SVR targeted research institutes and think tanks for intelligence collection.
2020	SolarWinds	18,000 organisations across the world including US Government departments' were affected by the SVR compromising Solar Winds Orion software.

The UK government has previously exposed details of other parts of the Russia intelligence service conducting cyber operations.

With the information provided today, the UK government has exposed the following parts of the Russian cyber programme:

Russian Intelligence Services Cyber Structures

Russian Intelligence Services Cyber Structures

JPEG, 76.4KB

This file may not be suitable for users of assistive technology.

Request an accessible format.
If you use assistive technology (such as a screen reader) and need a version of this document in a more accessible format, please email fcdo.correspondence@fcdo.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.

Published 15 April 2021

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

Competition concerns remain about FNZ's purchase of GBST

The Competition and Markets Authority (CMA) reassessed the deal, following its request to the Competition Appeal Tribunal (CAT) for a remittal of its original 'Phase 2' decision to block the merger. This request was made after FNZ's appeal to the CAT.

A group of independent CMA panel members has found in its reassessment that the purchase of retail investment platform solutions provider GBST by rival firm FNZ could substantially reduce competition. The CMA is concerned that this could lead to investment platforms – and therefore UK consumers who rely on these platforms to administer their pensions and other investments – facing higher costs and lower quality services.

Overall, the evidence the CMA considered, which included additional and updated evidence submitted during the remittal, shows that FNZ and GBST are close competitors and few other significant suppliers offer effective and competitive alternatives. The CMA's findings are based on the companies' own tender data and internal documents, as well as information provided by customers, competitors and other stakeholders. The CMA also found that if FNZ purchased GBST, the merged business would be the largest supplier in the market.

The CMA inquiry group carrying out the investigation has therefore provisionally concluded that the deal would substantially lessen competition and has considered different remedy options to address these concerns.

In the CMA's original Phase 2 decision, the group found that FNZ selling the entire GBST business was necessary to address its competition concerns. After considering new representations and evidence during the remittal, the group has provisionally found that its current competition concerns would also be

effectively and proportionately addressed by requiring FNZ to sell GBST, but with a right to subsequently buy back a limited set of assets from GBST relating to its capital markets business. These assets would be restricted to those that do not affect GBST's competitiveness in the supply of retail investment platform solutions.

Martin Coleman, Chair of the CMA inquiry group, said:

> Based on the latest evidence, we have come to the provisional conclusion that a merger of FNZ and GBST would significantly decrease competition in the retail investment platform solutions market.
>
> The reduction of competition in the market could lead to higher prices or poorer service for retail platforms to the ultimate detriment of UK consumers who hold pensions or other investments that are managed by these platforms.

Views are invited on the provisional findings and on the proposed remedy being considered by the CMA by 30 April 2021.

For more information, visit the FNZ/GBST merger inquiry case page.

For media enquiries, contact the CMA press office on 020 3738 6460 or press@cma.gov.uk.

Diversion report published

News story

Carbon monoxide poisoning on board a motor cruiser at Museum Gardens quay, River Ouse, York, with the loss of 2 lives.

Our investigation report into the double fatality due to CO poisoning from

Diversion’s cabin heater on 4 December 2019, is now published.

Statement from the Chief Inspector of Marine Accidents:

> The MAIB investigation into this tragic loss of lives once again highlights the importance of installing carbon monoxide alarms on boats with enclosed accommodation spaces. This is the fifth fatal marine accident investigated since 2014, where a functioning carbon monoxide alarm could have saved lives. Carbon monoxide alarms suitable for the marine environment are readily available, inexpensive and simple to fit, and I urge boat owners to invest in one as soon as possible.
>
> It is commonplace for marine engines, generators, cookers and heaters to produce carbon monoxide during normal operation; amateur installation and un-serviced appliances can introduce the risk of boat users inhaling lethal levels of this toxic gas. The importance of checking the installation and routine servicing of all such devices by a professional cannot be overstated.

The report contains details of what happened and the subsequent actions taken: read more.

A safety bulletin highlighting the importance of installing carbon monoxide (CO) alarms on boats with enclosed accommodation spaces was also published last year.

Published 15 April 2021

Defence Secretary statement on UK forces in Afghanistan

Government response

Defence Secretary Ben Wallace has made a statement on UK forces in Afghanistan.

Defence Secretary Ben Wallace said:

> The people of Afghanistan deserve a peaceful and stable future.
>
> As we drawdown, the security of our people currently serving in Afghanistan remains our priority and we have been clear that attacks on Allied troops will be met with a forceful response.
>
> The British public and our Armed Forces community, both serving and veterans, will have lasting memories of our time in Afghanistan. Most importantly we must remember those who paid the ultimate sacrifice, who will never be forgotten.

Published 14 April 2021