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