

NCSC joins US partners to promote understanding and mitigation of Russian state-sponsored cyber threats

The NCSC supports CISA, FBI, and NSA advice in understanding and countering Russian cyber threats.

The National Cyber Security Centre – a part of GCHQ – has added its support to new advice from international partners on countering Russian state-sponsored cyber threats targeting critical infrastructure.

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) have [published a joint advisory](#) encouraging network defenders of critical infrastructure to remain vigilant against Russian-backed hacking groups.

The advisory provides an overview of Russian state-sponsored cyber operations, including commonly observed tactics, techniques, and procedures (TTPs), detection actions, incident response guidance, and mitigations.

Critical infrastructure organisations are advised to take immediate actions to strengthen their cyber security posture:

- [Patch all systems](#) and prioritise patching [known exploited vulnerabilities](#)
- [Implement multi-factor authentication](#)
- [Use antivirus software](#)

The NCSC recommends that organisations follow the advice set out within the advisory, which also lists 13 vulnerabilities known to have been exploited by Russian-backed actors in order to gain access to networks, and warns that actors have also used [spear phishing](#) and [brute force](#) techniques successfully.

PUBLISHED

12 January 2022

WRITTEN FOR

[Small & medium sized organisations](#)

[Large organisations](#)

[Public sector](#)

[Cyber security professionals](#)

NEWS TYPE

[Alert](#)