Heightened threat of state-aligned groups against western critical national infrastructure

This alert highlights the emerging risk posed by state-aligned adversaries following the Russian invasion of Ukraine.

Update: 01/05/2024

The NCSC and international partners have issued a warning today about the evolving threat from Russia state-aligned actors targeting critical infrastructure.

As of early 2024, pro-Russia hacktivists have been observed targeting vulnerable, small-scale industrial control systems in North America and Europe.

Whilst most of the activity remains technically unsophisticated, this targeting has resulted in US agencies responding to incidents where victims have seen some limited physical disruption to operations.

There continues to be a heightened threat from state-aligned actors to operational technology (OT) operators. The NCSC urges all OT owners and operators, including UK essential service providers, to follow the recommended mitigation advice now to harden their defences.

Read the factsheet, including mitigation advice, on CISA's website.

Over the past 18 months, a new class of Russian cyber adversary has emerged. These state-aligned groups are often sympathetic to Russia's invasion and are ideologically, rather than financially, motivated.

Although these groups can align to Russia's perceived interests, they are often not subject to formal state control, and so their actions are less constrained and their targeting broader than traditional cyber crime actors. This makes them less predictable.

While the cyber activity of these groups often focuses on DDoS attacks, website defacements and/or the spread of misinformation, some have stated a desire to

achieve a more disruptive and destructive impact against western critical national infrastructure (CNI), including in the UK. We expect these groups to look for opportunities to create such an impact, particularly if systems are poorly protected.

Without external assistance, we consider it unlikely that these groups have the capability to deliberately cause a destructive, rather than disruptive, impact in the short term. But they may become more effective over time, and so the NCSC is recommending that organisations act now to manage the risk against successful future attacks.

Recommendation

The NCSC recommends that organisations implement the measures described in actions to take when the cyber threat is heightened, particularly the NCSC advice on secure system administration.

As noted in the guidance, larger organisations could benefit from using the Cyber Assessment Framework (CAF) to help them identify areas for improvement. The CAF 'indicators of good practice' may be helpful here.

PUBLISHED

19 April 2023

WRITTEN FOR

Public sector

Large organisations

Cyber security professionals

NEWS TYPE

Alert