

UK Warns of Russian Hackers Targeting Critical Infrastructure

The UK government's intelligence and security arm this week issued an alert on Russian state-aligned threat actors aiming to conduct disruptive and destructive attacks against critical infrastructure in Western countries.

To date, says the National Cyber Security Centre (NCSC), the information security arm of the UK's Government Communications Headquarters (GCHQ), these threat groups have focused on distributed denial-of-service (DDoS) attacks, defacements, and misinformation attacks.

"Some have stated a desire to achieve a more disruptive and destructive impact against western critical national infrastructure (CNI), including in the UK," the NCSC warns.

The agency believes that these groups will focus on identifying poorly protected critical infrastructure systems, to cause disruptions.

Threat actors that pose a threat include not only groups that are actually sponsored by the Russian government, but also hacktivists that are sympathetic to Russia.

Aligned with Moscow's interests, these threat actors support Russia's invasion of Ukraine, are ideologically motivated, and may not be subject to formal state control, which makes them less predictable, as their targeting is broader compared to that of cybercriminal groups, the NCSC says.

The agency believes that these groups are not sophisticated

enough and that they lack the resources to launch destructive attacks on their own.

“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,” the agency says.

Nonetheless, the NCSC notes that these groups may become more effective over time and recommends that organizations take the necessary precautions to prepare themselves for potential attacks.

Related: Microsoft: Iranian Hackers Moved From Recon to Targeting US Critical Infrastructure

Related: CISA Program Warns Critical Infrastructure Organizations Vulnerable to Ransomware Attacks

Related: Pro-Russian Group DDoS-ing Governments, Critical Infrastructure in Ukraine, NATO Countries

<https://www.securityweek.com/uk-warns-of-russian-hackers-targeting-critical-infrastructure/>