Pro-Russia hacktivist activity continues to target UK organisations

The NCSC encourages local government and critical infrastructure operators to harden their 'denial of service' (DoS) defences

Russian-aligned hacktivist groups continue to target the UK and global organisations by attempting to disrupt operations, take websites offline and disable services.

In December 2025, the NCSC co-sealed an advisory highlighting that pro-Russian hacktivists groups have been conducting worldwide cyber operations against numerous organisations and critical infrastructure sectors.

In particular, the group **NoName057(16)** has been active since March 2022, and have been conducting attacks against government and private sector entities in NATO member states and other European countries that are perceived as hostile to Russian geopolitical interests. These attacks have included frequent DDoS attempts against UK local government.

The group operates primarily through Telegram channels and used GitHub (and other websites and repositories) to host the proprietary tool DDoSia, and to share tactics, techniques, and procedures (TTPs) with their followers.

This is not the first time that the NCSC has called out activity from Russian-aligned groups targeting UK organisations. In 2023, the NCSC published an alert on the risk posed by state-aligned adversaries following the Russian invasion of Ukraine. These attacks are ideologically (rather than financially) motivated, and reflect an evolution in the threat which now target UK operational technologies. As a result, the NCSC encourages all OT owners to follow recommended mitigation advice to harden their cyber defences.

Understand and mitigate denial of service (DoS) attacks

The NCSC is advising all organisations review their defences, and to improve resilience against attacks from Russian-aligned groups. In particular, we're encouraging all organisations review their DoS protections, which includes:

Understanding your service

There are probably many points in your service where an attacker can attempt to overload or exhaust available resources, thereby preventing you from serving legitimate users. You should understand where these points are, and in each case, determine whether you, or a supplier, are responsible.

Upstream defences

Ensure your service providers are ready to deal with resource exhaustion in places where they are uniquely placed to help. We recommend you:

- understand the denial of service mitigations that your ISP has in place on your account
- look into third-party DDoS mitigation services that can be used to protect against network traffic based attacks
- consider deploying a content delivery network, for web-based services
- understand when and how your service provider might limit your network access in order to protect their other customers
- consider using multiple service providers for some functionality

Building to allow scaling

To deal with attacks which can't be handled upstream (or only once detected and blocked), make sure your service can rapidly scale. Ideally, you should be able to scale all aspects of your application and infrastructure. Cloud-native applications can be automatically scaled using the cloud providers' APIs. In private data centres, automated scaling is possible using modern virtualisation, but this will require spare hardware capacity to deal with the additional load.

Defining your response plan

Design your service and plan your response to an attack so that it can continue to operate (albeit in a degraded fashion). We recommend your plan includes:

- graceful degradation
- dealing with changing tactics

- retaining administrative access during an attack
- having a scalable fall-back plan for essential services

Testing and monitoring your service

Gain confidence in your defences by testing them, and ensure you can spot when attacks start by having the right tools in place. Test your defences so you know the types (and volume) of attacks you are able to defend. System monitoring will help you spot attacks when they begin, and analyse your response while it's underway.
For more information, please refer to the NCSC's core Denial of Service (DoS) guidance. In addition, the NCSC encourage all organisations to review our heightened cyber threat guidance collection, in particular the guidance on actions to take when the cyber threat is heightened.

PUBLISHED

19 January 2026

WRITTEN FOR

Large organisations

Public sector

Cyber security professionals

NEWS TYPE

Alert