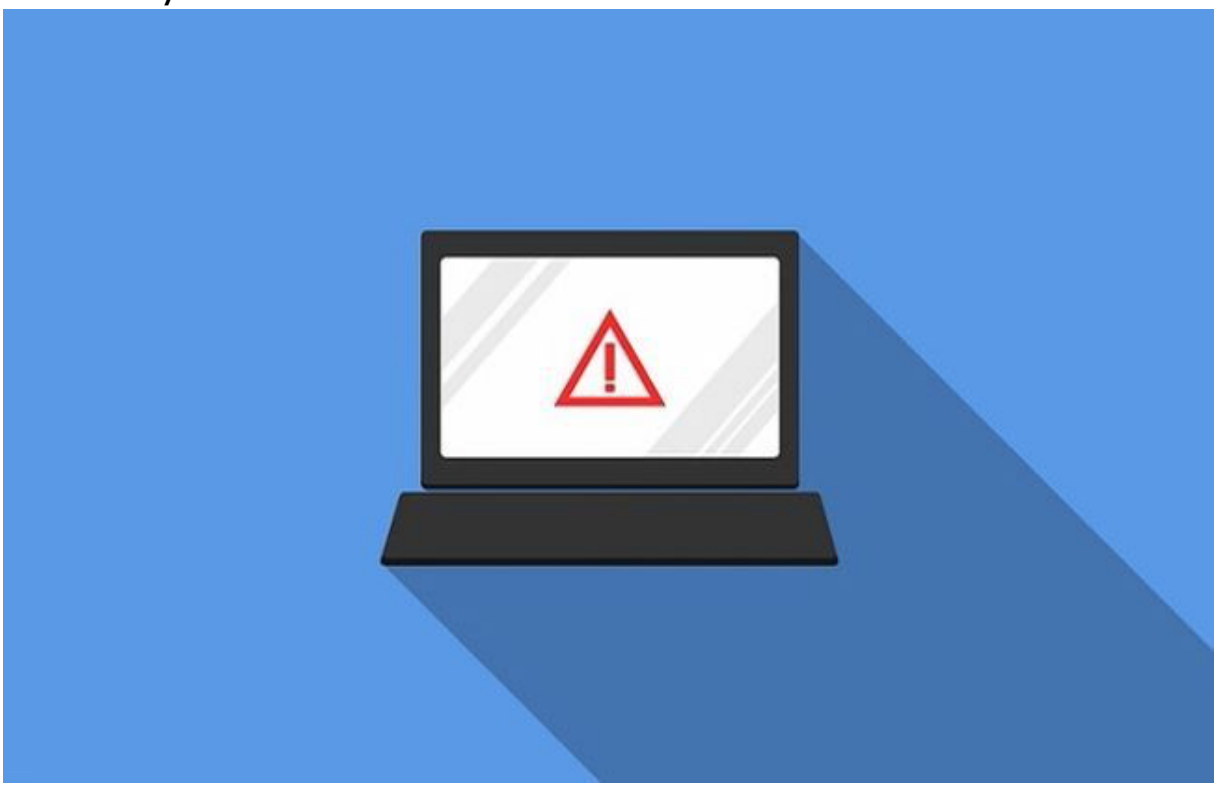
National Cyber Security Centre

New Sandworm malware Cyclops Blink replaces VPNFilter

Joint advisory published by the UK and US identifies a new malware known as Cyclops Blink that could be used to remotely access networks.



The UK and US have today published a joint advisory that identifies a new malware used by the actor Sandworm. Sandworm, also

known as Voodoo Bear, has previously been attributed to Russia's GRU.

The malware dubbed Cyclops Blink appears to be a replacement for the VPNFilter malware exposed in 2018, and its deployment could allow Sandworm to remotely access networks.

The advisory, published by the NCSC (UK) and CISA, FBI and NSA (USA), includes steps outlining how to identify a Cyclops Blink infection and points to mitigation advice to help organisations remove it.

The advisory also includes information on the associated tactics, techniques and procedures (TTPs) used by Sandworm.

The NCSC has also published a malware analysis report on Cyclops Blink which provides a more detailed view of the malware.

N.B This is a routine advisory and not directly linked to the situation in Ukraine.