UK exposes series of Russian cyber attacks against Olympic and Paralympic Games

Russia's military intelligence service, the GRU, conducted cyber reconnaissance against officials and organisations at the 2020 Olympic and Paralympic Games due to take place in Tokyo this summer before they were postponed, the UK has revealed today.

The targets included the Games' organisers, logistics services and sponsors.

The attacks on the 2020 Summer Games are the latest in a campaign of Russian malicious cyber activity against the Olympic and Paralympic Games.

The UK is confirming for the first time today the extent of GRU targeting of the 2018 Winter Olympic and Paralympic Games in Pyeongchang, Republic of Korea.

The GRU's cyber unit attempted to disguise itself as North Korean and Chinese hackers when it targeted the opening ceremony of the 2018 Winter Games.

It went on to target broadcasters, a ski resort, Olympic officials and sponsors of the games in 2018.

The GRU deployed data-deletion malware against the Winter Games IT systems and targeted devices across the Republic of Korea using VPNFilter.

The National Cyber Security Centre (NCSC) assesses that the incident was intended to sabotage the running of the Winter Olympic and Paralympic Games, as the malware was designed to wipe data from and disable computers and networks.

Administrators worked to isolate the malware and replace the affected computers, preventing potential disruption.

Foreign Secretary Dominic Raab said:

> The GRU's actions against the Olympic and Paralympic Games are cynical and reckless. We condemn them in the strongest possible terms.
>
> The UK will continue to work with our allies to call out and counter future malicious cyber attacks.

The UK has already acted against the GRU's destructive cyber unit by working with international partners to impose asset freezes and travel bans against its members through the EU cyber sanctions regime.

Today (Monday 19 October), the US Department of Justice has announced criminal charges against Russian military intelligence officers working for the GRU's destructive cyber unit – also known by the codenames Sandworm and VoodooBear – for conducting cyber attacks against the 2018 Winter Games and other cyber attacks, including the 2018 spear phishing attacks against the UK's Defence Science and Technology Laboratory (DSTL).

The UK attributed the attacks against DSTL, which followed the Salisbury poisonings, to Russia in 2018.

These cyber attacks were committed by the GRU's Main Centre for Special Technologies, GTsST also known by its field post number 74455 and known in open source as:

- Sandworm
- BlackEnergy Group
- Telebots
- VoodooBear
- Iron Viking
- Quedagh
- Electrum
- Industroyer
- G0034

The UK government is today confirming for the first time that the GRU unit known as GTsST or by its field post number 74455 were responsible for:

	GRU action	UK government response
Winter Olympics, February 2018	GTsST actors launched a significant campaign against the Winter Olympic games, which included the use of Olympic Destroyer malware. This malware targeted the Winter Olympic and Paralympic Games. NCSC assess that the intent behind the incident was almost certainly sabotage as the malware was designed to wipe data from and disable computers and networks. Disruption to the Winter Olympics could have been greater if it had not been for administrators who worked to isolate the malware and replace affected computers. More broadly, the GTsST actors targeted multiple entities across South Korea (and the world) which were linked with the Winter Olympics. This activity utilised a range of capabilities known to be used by the GTsST. This includes targeting of: officials, sponsors, a ski resort, official service providers, and broadcasters	The UK government is publicly exposing this attack as the work of the GRU for the first time today

The UK government has previously publicly exposed that this unit of the GRU was responsible for:

	GRU action	UK government response
BlackEnergy, December 2015	Shut off part of Ukraine's electricity grid, with 230,000 people losing power for between 1 – 6 hours	UK government publicly exposed this attack as the work of the GRU in February 2020
Industroyer, December 2016	Shut off part of Ukraine's electricity grid, also known as CrashOverride. It resulted in a fifth of Kyiv losing power for an hour. It is the first known malware designed specifically to disrupt electricity grids	UK government publicly exposed this attack as the work of the GRU in February 2020
NotPetya, June 2017	Destructive cyber attack targeting the Ukrainian financial, energy and government sectors and affecting other European and Russian businesses	UK government publicly exposed this attack as the work of the GRU in February 2018. EU sanctioned the GRU unit for this attack in July 2020
BadRabbit, October 2017	Ransomware encrypted hard drives and rendered IT inoperable. This caused disruption including to the Kyiv metro, Odessa airport, Russia's central bank and two Russian media outlets	UK government publicly exposed this attack as the work of the GRU in October 2018
VPNfilter, October 2017	VPNFILTER malware infected thousands of home and small business routers and network devices worldwide. The infection potentially allowed attackers to control infected devices, render them inoperable and intercept or block network traffic	In April 2018, the NCSC, FBI and Department for Homeland Security issued a joint Technical Alert exposing that the GRU was responsible
DSTL, April 2018	The GRU attempted to use its cyber capabilities to gain access to the UK's Defence and Science Technology Laboratory (DSTL) computer systems	UK government publicly exposed this attack as the work of the GRU in October 2018
FCO, March 2018	The GRU attempted to compromise the UK Foreign and Commonwealth Office (FCO) computer systems via a spearphishing attack	UK government publicly exposed this attack as the work of the GRU in October 2018
Georgia, 28 October 2019	The GRU carried out large scale disruptive cyber-attacks against Georgian web hosting providers that resulted in widespread defacement of websites, including sites belonging to the Georgian Government, courts, NGOs, media and businesses, and also interrupted the service of several national broadcasters	UK government publicly exposed this attack as the work of the GRU in February 2020

The National Cyber Security Centre has assessed with high confidence that all of these attacks were almost certainly (95%+) carried out by the unit known as the Main Centre for Special Technologies (GTsST) also known as Unit 74455

of the GRU.

See further details on the framework used by the UK government for all source intelligence assessments, including the probability yardstick.