National Cyber Security Centre
a part of GCHQ

News (/)

Reckless campaign of cyber attacks by Russian military intelligence service exposed

Created: 04 Oct 2018
Updated: 04 Oct 2018

Today, the UK and its allies can expose a campaign by the GRU, the Russian military intelligence service, of indiscriminate and reckless cyber attacks targeting political institutions, businesses, media and sport.

The National Cyber Security Centre (NCSC) has identified that a number of cyber actors widely known to have been conducting cyber attacks around the world are, in fact, the GRU. These attacks have been conducted in flagrant violation of international law, have affected citizens in a large number of countries, including Russia, and have cost national economies millions of pounds.

Cyber attacks orchestrated by the GRU have attempted to undermine international sporting institution WADA, disrupt transport systems in Ukraine, destabilise democracies and target businesses.

This campaign by the GRU shows that it is working in secret to undermine international law and international institutions.

The Foreign Secretary, Jeremy Hunt said:

> *"These cyber attacks serve no legitimate national security interest, instead impacting the ability of people around the world to go about their daily lives free from interference, and even their ability to enjoy sport.*
>
> *"The GRU's actions are reckless and indiscriminate: they try to undermine and interfere in elections in other countries; they are even prepared to damage Russian companies and Russian citizens. This pattern of behaviour demonstrates their desire to operate without regard to international law or established norms and to do so with a feeling of impunity and without consequences.*
>
> *"Our message is clear: together with our allies, we will expose and respond to the GRU's attempts to undermine international stability."*

Today, the UK and its allies are once again united in demonstrating that the international community will stand up against irresponsible cyber attacks by other Governments and that we will work together to respond to them. The British Government will continue to do whatever is necessary to keep our people safe.

As the Prime Minister said in Parliament on 5 September 2018, the UK will work with our allies to shine a light on the activities of the GRU and expose their methods.

The UK's National Cyber Security Centre assess that the GRU is almost certainly the cyber actors listed below. Given the high confidence assessment and the broader context, the UK government has made the judgement that the Russian Government – the Kremlin – was responsible.

The GRU are associated with the names:

- APT 28
- Fancy Bear
- Sofacy
- Pawnstorm
- Sednit
- CyberCaliphate
- Cyber Berkut
- Voodoo Bear
- BlackEnergy Actors
- STRONTIUM
- Tsar Team
- Sandworm

New attributions

Attack	NCSC Assessment
In October 2017, BadRabbit 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.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
In August 2016, confidential medical files relating to a number of international athletes were released. WADA stated publicly that this data came from a hack of its Anti-Doping Administration and Management system.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
In 2016, the Democratic National Committee (DNC) was hacked and documents were subsequently published online.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
Between July and August 2015 multiple email accounts belonging to a small UK-based TV station were accessed and content stolen.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.

Previously attributed

Attack	NCSC Assessment
In June 2017 a destructive cyber attack targeted the Ukrainian financial, energy and government sectors but spread further affecting other European and Russian businesses.	The UK Government attributed this attack to the GRU in February 2018. NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
In 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(/file/3138/download?token=bRXnaQHx) about this activity by Russian state-sponsored actors.

The NCSC has issued a technical advisory: Indicators of Compromise for Malware used by APT28(/alerts/indicators-compromise-malware-used-apt28).

Update at 1pm

This update follows the joint statement from Prime Minister May and Prime Minister Rutte (https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte) and the statement in The Netherlands (https://www.gov.uk/government/speeches/minister-for-europe-statement-attempted-hacking-of-the-opcw-by-russian-military-intelligence) on the attempted hacking of the OPCW by Russian military intelligence.

Attack	NCSC Assessment
In May 2018 GRU hackers sent spearphishing emails which impersonated Swiss federal authorities to directly target OPCW employees, and thus OPCW computer systems. These employees were likely attending a forthcoming conference in Spiez.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
In April 2018 the GRU attempted to use its cyber capabilities to gain access to official OPCW computer networks.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
In April 2018 the GRU attempted to use its cyber capabilities to gain access to the UK Defence and Science Technology Laboratory (DSTL) computer systems.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.
In March 2018 the GRU attempted to compromise the UK Foreign and Commonwealth Office (FCO) computer systems via a spearphishing attack.	NCSC assess with ***high confidence*** that the GRU was ***almost certainly*** responsible.

Topics

Cyber threats(/topics/cyber-threats)
The NCSC(/topics/ncsc)

Was this news helpful?

We need your feedback to improve this content.

Yes No