UK exposes Russian spy agency behind cyber incidents

- KGB's successor agency, the Federal Security Service (FSB) is behind a historic global campaign targeting critical national infrastructure.

- Long list of cyber operations includes UK energy sector, US aviation and a Russian dissident in the UK targeted using sophisticated hacking and spear-phishing.

- Foreign Secretary Liz Truss sanctions a Russian MOD subsidiary for carrying out malicious cyber activity on a Saudi petro-chemical plant.

The UK, together with the US and other allies, has today (Thursday 24 March) exposed historic malign cyber activity of Russia's Federal Security Service (FSB) – the successor agency to the KGB.

One month on since Putin's unprovoked and illegal war in Ukraine started, the global scope of the FSB's Centre 16 cyber campaign has been revealed.

The National Cyber security Centre (NCSC) assess it is almost certain that the FSB's Centre 16 are also known by their hacker group pseudonyms of 'Energetic Bear', 'Berserk Bear' and 'Crouching Yeti', and conducted a malign programme of cyber activity, targeting critical IT systems and national infrastructure in Europe, the Americas and Asia. They have today been indicted by the FBI for targeting the systems controlling the Wolf Creek nuclear power plant in Kansas, US in 2017 but failed to have any negative impact.

Separately, Foreign Secretary Liz Truss has used the UK's cyber sanctions regime to designate a Russian defence ministry subsidiary, the Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), for an incident involving safety override controls in a Saudi petro-chemicals plant in 2017.

Foreign Secretary Liz Truss said:

> Russia's targeting of critical national infrastructure is calculated and dangerous. It shows Putin is prepared to risk lives to sow division and confusion among allies.
>
> We are sending a clear message to the Kremlin by sanctioning those who target people, businesses and infrastructure. We will not tolerate it.

> We will continue to work together with our allies to turn the ratchet and starve Putin’s war machine of its funding and resources.

The malware used against the petro-chemical plant was designed specifically to target the plant’s safety override for the Industrial Control System and resulted in two emergency shutdowns of the plant.

The malware was designed to give the actors complete control of infected systems and had the capability to cause significant impact, possibly including the release of toxic gas or an explosion – either of which could have resulted in loss of life and physical damage to the facility.

The FSB’s long raft of malign cyber activity includes:

- Targeting UK energy companies
- Sustained and substantial scanning and probing of networks in the American aviation sector, and exfiltration of data in aviation and other key US targets
- Posing as the Russian Federal Tax Service to conduct spear-phishing attacks against Russian nationals
- Attempting to spear-phish the press secretary of Mikhail Khodorkovskiy, a UK-based longstanding critic of the Kremlin, and monitoring a website he set up to expose corruption in the Russian government

These sanctions follow a further 65 oligarchs and banks targeted earlier today by the Foreign Secretary, bringing the UK’s sanctions on those who enable Putin’s war to more than £500 billion worth of bank assets and £150 billion in personal net worth.

ENDS

Notes to editors:

- Spear-phishing is the practice of sending targeted electronic communication, such as emails and SMS messages, to specific individuals, groups or organisations for malicious purposes, including data theft, espionage and fraud.