# UK condemns Iran for reckless cyber attack against Albania

Press release

The UK has condemned the Iranian state for a cyber attack against Albania's government that destroyed data and disrupted essential government services.

The UK has today (Wednesday 7 September) condemned the Iranian state for a cyber attack against Albania's government that destroyed data and disrupted essential government services, including paying utilities, booking medical appointments and enrolling schoolchildren.

The National Cyber Security Centre (NCSC) assesses that Iranian state-linked cyber actors are almost certainly responsible for the series of cyber attacks against Albanian government infrastructure from 15 July, which caused significant impact to online public services and other government websites.

The websites of the Albanian Parliament and the Prime Minister's office, as well as 'e-Albania', a portal that Albanians use to access a number of public services, were attacked and subject to a shut down. The attackers also leaked Albanian government data, including details of emails from the Prime Minister and Ministry of Foreign Affairs.

Foreign Secretary James Cleverly said:

> Iran's reckless actions showed a blatant disregard for the Albanian people, severely restricting their ability to access essential public services.
>
> The UK is supporting our valuable partner and NATO ally. We join Albania and other allies in exposing Iran's unacceptable actions.

NCSC assesses that Iran is an aggressive and capable cyber actor. Cyber operations are likely conducted by a complex and fluid network of groups, with differing degrees of association to the Iranian state, the workforces of

which are highly likely a mix of departmental and contractual staff.

These cyber attacks are the latest in an increasingly reckless pattern of behaviour by Iran. Iranian-linked cyber actors have a number of powerful disruptive and destructive tools at their disposal. The UK has previously attributed and advised on a number of cyber incident by Iranian actors:

- 22 March 2018: The UK’s National Cyber Security Centre assessed with high confidence that the MABNA Institute were almost certainly responsible for a multi-year Computer Network Exploitation (CNE) campaign targeting universities in the UK, the US, as well as other Western nations, primarily for the purposes of intellectual property (IP) theft
- 24 February 2022: CISA, FBI, CNMF, NCSC and NSA released a joint Cybersecurity Advisory highlighting a group of Iranian government-sponsored advanced persistent threat (APT) actors, known as MuddyWater, conducting cyber espionage and other malicious cyber operations targeting a range of government and private-sector organisations across sectors in Asia, Africa, Europe, and North America
- 17 November 2021: CISA, FBI, ACSC and NCSC released a joint Cyber Security Advisory on Iranian government-sponsored APT actors exploiting Microsoft Exchange and Fortinet vulnerabilities to gain initial access in advance of follow-on operations. The Iranian government-sponsored APT actors are actively targeting a broad range of multiple US critical infrastructure sectors as well as Australian organisations

Published 7 September 2022