NCSC joins partners to issue warning about China state-sponsored cyber activity targeting CNI networks

The advisory provides technical indicators of compromise and examples of techniques deployed by the actor to help network defenders identify malicious activity.

The UK and agencies in the US, Australia, Canada and New Zealand have issued new advice today (Wednesday) to help organisations detect China state-sponsored activity being carried out against critical national infrastructure networks.

In the new joint advisory the National Cyber Security Centre – a part of GCHQ – alongside international partners highlight how recent activity has targeted networks across critical infrastructure sectors in the US and how the same techniques could be applied worldwide.

The actor has been observed taking advantage of built-in network administration tools on targets' systems to evade detection after an initial compromise.

The advisory provides technical indicators of compromise and examples of techniques deployed by the actor to help network defenders identify the malicious activity.

Paul Chichester, NCSC Director of Operations, said:

> "It is vital that operators of critical national infrastructure take action to prevent attackers hiding on their systems, as described in this joint advisory with our international partners.
>
> "We strongly encourage providers of UK essential services to follow our guidance to help detect this malicious activity and prevent persistent compromise."

The advisory has been jointly issued by the NCSC, the US National Security Agency (NSA), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Communications Security Establishment's Canadian Centre for Cyber Security (CCCS), and the New Zealand National Cyber Security Centre (NCSC-NZ).

The advisory can be found on the NSA's website.

The NCSC has published a range of guidance to help critical national infrastructure organisations protect themselves online. This includes the Cyber Assessment Framework (CAF), which is designed to help organisations effectively manage cyber risk.

PUBLISHED

24 May 2023

WRITTEN FOR

Large organisations

Cyber security professionals

Public sector

NEWS TYPE

Alert