NCSC and international partners shine a light on Lockbit ransomware threat

New advisory recommends mitigations for network defenders to take against the ransomware strain most globally deployed.

THE UK and international partners have warned today (Wednesday) about the enduring threat posed by the Lockbit ransomware operation, which continues to cause disruptive attacks against organisations globally.

In a new joint advisory, it is revealed that Lockbit was the most deployed ransomware variant across the world in 2022, and it continues to be prolific so far in 2023, with activity observed globally as recently as late May.

The National Cyber Security Centre – a part of GCHQ – has issued this advisory alongside agencies from the United States, Australia, Canada, France, Germany and New Zealand, to help organisations take action to reduce the likelihood and impact of future incidents.

Since January 2020, organisations of all sizes across a wide range of critical infrastructure sectors, including financial services, food and agriculture, education and healthcare, have been attacked by Lockbit affiliates using a variety of tactics and techniques.

The NCSC assesses that Lockbit was almost certainly the most deployed ransomware strain in the UK in 2022 and that it continues to present the highest ransomware threat to UK organisations.

The advisory outlines technical details about how Lockbit operates, the common tools and techniques that affiliates use in their attacks, and recommended mitigation advice for network defenders.

Paul Chichester, NCSC Director of Operations, said:

> "Ransomware remains a major threat to businesses worldwide, including in the UK, and the Lockbit operation has been the most active, with widespread consequences.

> "It is essential for organisations to understand the serious consequences that ransomware attacks can have on their operations, finances and reputation.
>
> "This advisory, issued with our international partners, emphasises the importance of network defenders taking the recommended actions to establish effective protections against such attacks."

The advisory describes how the Lockbit operation uses a 'Ransomware-as-a-Service' model where cyber criminals sell access to their ransomware variant to unconnected affiliates and provide them with support in carrying out attacks.

It also highlights the risk of double extortion – a common tactic used by ransomware actors where they encrypt a victim's system and exfiltrate the information, with threats that they will post it online unless a ransom is paid.

The NCSC's ransomware hub shares a range of guidance and advice to help organisations understand, mitigate and respond to ransomware attacks. The NCSC's position, along with law enforcement, is that it does not endorse, promote or encourage the payment of ransoms.

The new advisory has been jointly issued by the NCSC, the United States Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), the US Multi-State Information Sharing and Analysis Center (MS-ISAC), the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the National Cybersecurity Agency of France (ANSSI), Germany's Federal Office for Information Security (BSI), New Zealand's Computer Emergency Response Team (CERT NZ) and the New Zealand National Cyber Security Centre (NCSC-NZ).

Read the advisory on CISA's website

PUBLISHED

14 June 2023

WRITTEN FOR

Cyber security professionals

Large organisations

NEWS TYPE

Alert