NCSC and partners issue warning over North Korean state-sponsored cyber campaign to steal military and nuclear secrets

Critical infrastructure organisations are strongly encouraged to stay vigilant to DPRK-sponsored cyber operations.

THE UK and international allies have exposed a global cyber espionage campaign carried out by attackers sponsored by the Democratic People's Republic of Korea (DPRK) to further the regime's military and nuclear ambitions.

The National Cyber Security Centre – a part of GCHQ – has issued a new advisory today (Thursday) alongside partners in the United States and the Republic of Korea which reveals how a cyber threat group known as Andariel has been compromising organisations around the world to steal sensitive and classified technical information and intellectual property data.

The NCSC assesses that Andariel is a part of DPRK's Reconnaissance General Bureau (RGB) 3rd Bureau and that the group's malicious cyber activities pose an ongoing threat to critical infrastructure organisations globally.

The cyber actors have primarily targeted defence, aerospace, nuclear and engineering entities, and organisations in the medical and energy sectors to a lesser extent, in order to obtain information such as contract specification, design drawings and project details.

As part of its operations, Andariel has also launched ransomware attacks against US healthcare organisations in order to extort payments and fund further espionage activity.

This advisory shares technical details and mitigation advice to help defend against the actors who have been seen exploiting known vulnerabilities to access victims' systems before deploying malware and other tools to maintain persistence, evade detection and exfiltrate data.

Paul Chichester, NCSC Director of Operations, said:

> “The global cyber espionage operation that we have exposed today shows the lengths that DPRK state-sponsored actors are willing to go to pursue their military and nuclear programmes.
>
> “It should remind critical infrastructure operators of the importance of protecting the sensitive information and intellectual property they hold on their systems to prevent theft and misuse.
>
> “The NCSC, alongside our US and Korean partners, strongly encourage network defenders to follow the guidance set out in this advisory to ensure they have strong protections in place to prevent this malicious activity.”

The advisory outlines how Andariel has evolved its operations from conducting destructive attacks targeting US and South Korea organisations to conducting specialised cyber espionage and ransomware attacks.

It warns that in some cases the actors have even been observed launching ransomware attacks and espionage operations on the same day and leveraging both activities against the same victim.

The advisory has been co-sealed by the NCSC, the US Federal Bureau of Investigation (FBI), the US Cyber National Mission Force (CNMF), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Department of Defense Cyber Crime Center (DC3), the US National Security Agency (NSA), the Republic of Korea’s National Intelligence Service (NIS), and the Republic of Korea’s National Police Agency (NPA).

It can be read on the FBI website:
https://www.ic3.gov/Media/News/2024/240725.pdf

PUBLISHED

25 July 2024

WRITTEN FOR

Public sector

Cyber security professionals

Large organisations

/

NEWS TYPE

General news