Mar 28, 2023 - Technology

Mandiant identifies new North Korea state-backed hacking group

Sam Sabin, author of Axios Codebook

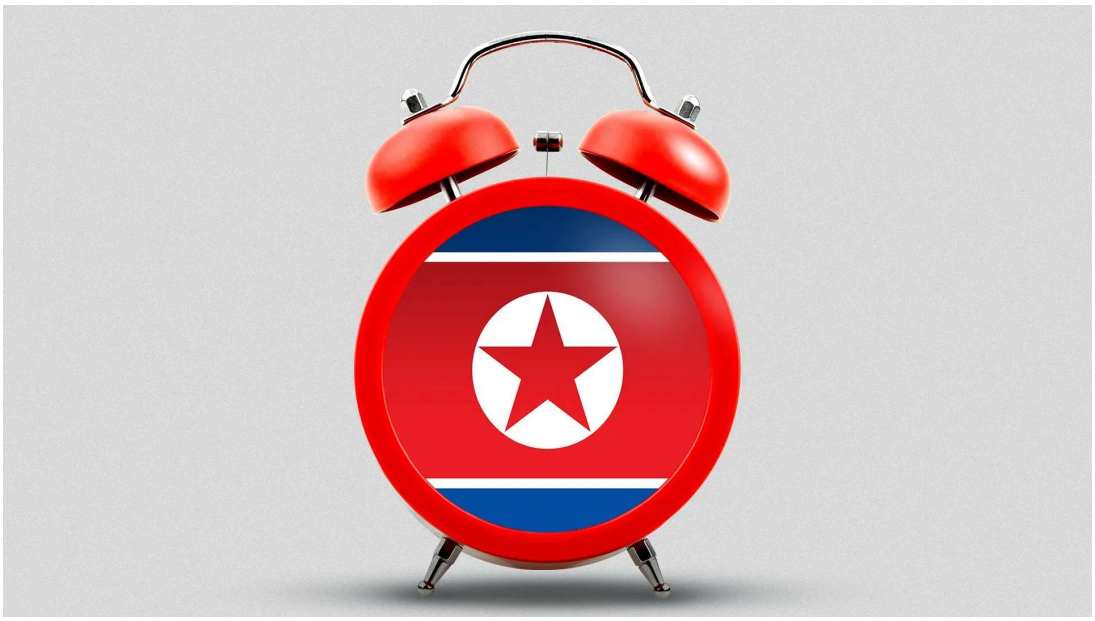

Illustration: Annelise Capossela/Axios

Researchers have identified a new state-backed hacking group in North Korea: APT43.

AXIOS

- APT43 also appears to target cryptocurrency firms and services and uses the profits to fund its espionage operations, the report states.

- The group typically targets organizations in South Korea and the United States, with a special focus on government, business services, manufacturing and education and research groups.

The big picture: Mandiant has "moderate confidence" that APT43 is specifically linked to North Korea's foreign intelligence service.

- Mandiant has been tracking this gang's activities since 2018, and today's report officially elevates the group to an official state-backed hacking group.

Of note: Other companies refer to the group as "Kimsuky" or "Thallium" in their reports. Each cyber research firm uses its own naming conventions for identifying hacking groups.

Details: APT43 engages in two types of cyber activity: Spear-phishing email campaigns to harvest specific targets' credentials and high-value research, and cryptocurrency firm hacks to get funds for its own operations.

- In the spear-phishing attacks, APT43 poses as reporters and researchers to trick employees at U.S. defense and research organizations, as well as South Korea-based think tanks, into clicking on a malicious email link or responding with key intel.

- APT43 has been seen using cryptocurrency services to launder stolen currency, suggesting the group has been involved in the string of recent attacks.

Threat level: Unlike other state-backed hacking groups, APT43 has yet to be seen exploiting critical, unknown vulnerabilities in

AXIOS

activity" and has collaborated with several North Korea state-backed hacking groups.

Sign up for Axios' cybersecurity newsletter Codebook here

Go deeper

Barak Ravid
1 hour ago - Politics & Policy

Jake Sullivan to deliver Davos speech on Gaza, Ukraine and China

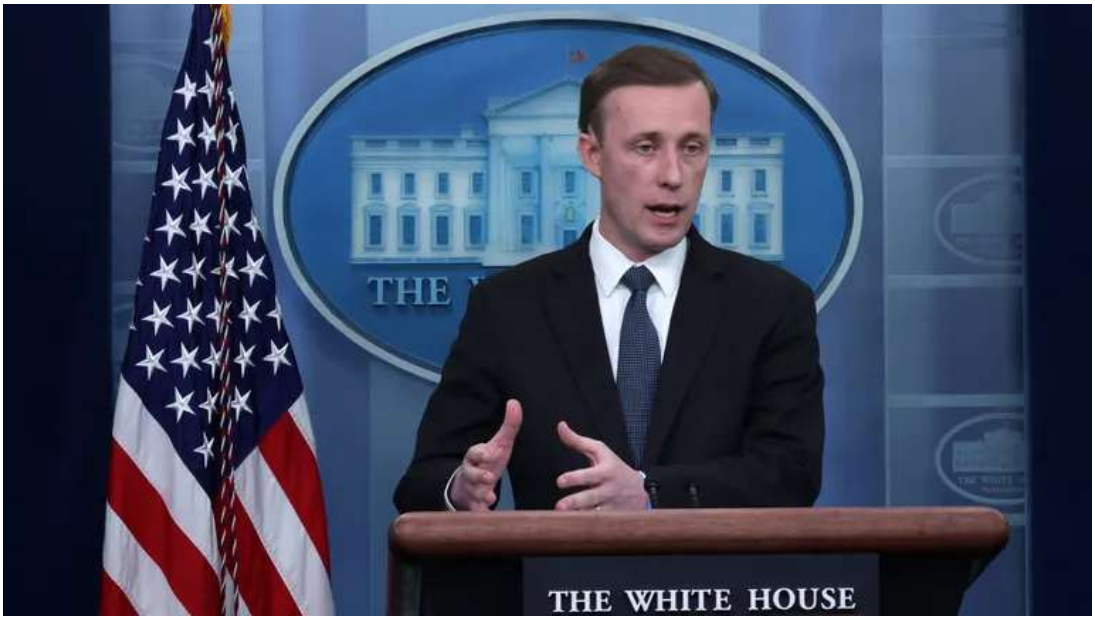

Photo: Alex Wong/Getty Images

White House national security adviser Jake Sullivan will deliver a speech on Tuesday at the World Economic Forum in Davos,

AXIOS

Why it matters: Sullivan's speech comes as the administration seems to be struggling to make progress in two wars in which it's highly invested.

Go deeper (1 min. read) ⟶

Sara Fischer, author of Axios Media Trends
2 hours ago - Business

Baltimore Sun sold to Sinclair chairman David Smith

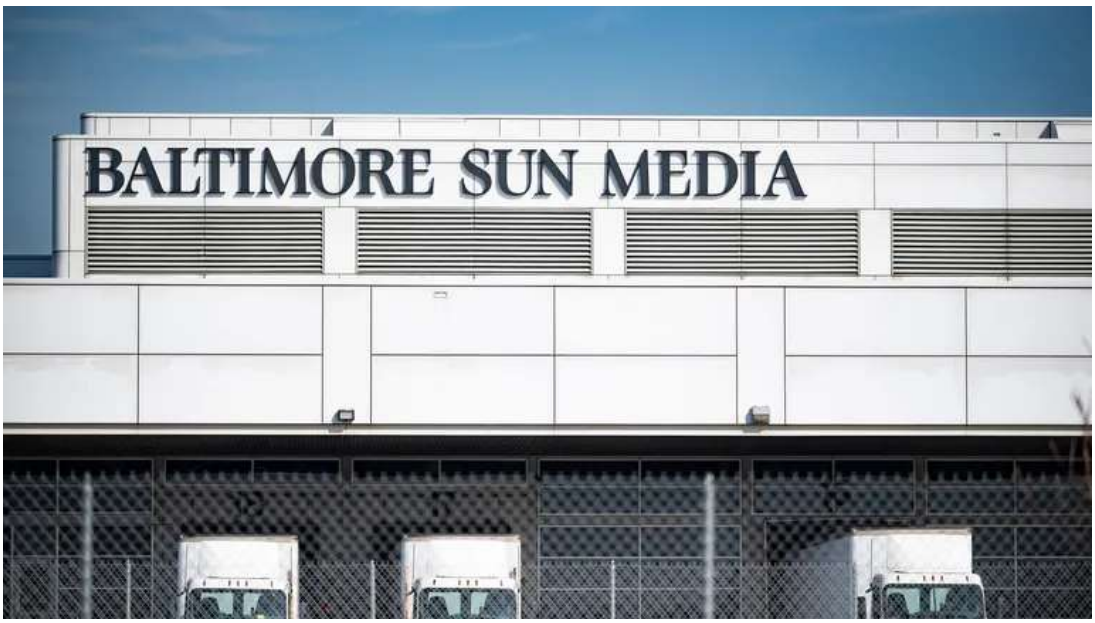

Photo: Jim Watson/AFP via Getty Images

The Baltimore Sun, Maryland's largest newspaper, has been sold by hedge fund Alden Global Capital to David Smith, the executive chairman of the local TV company Sinclair.

AXIOS

Go deeper (1 min. read) ⟶

Emily Peck, author of Axios Markets
2 hours ago - Business

The return-to-office wars are over

Illustration: Annelise Capossela/Axios

Just 6 out of 158 U.S. CEOs said they'll prioritize bringing workers back to the office full-time in 2024, according to a new survey released by the Conference Board.

Why it matters: Executives are increasingly resigned to a world where employees don't come in every day, as hybrid work arrangements — mixing work from home and in-office — become the norm for knowledge workers.

Go deeper (2 min. read) ⟶

AXIOS

News worthy of your time.

Download the app ⟶

About

About Axios

Advertise with us

Careers

Events

Axios on HBO

Axios HQ

Privacy and terms

Accessibility Statement

Online tracking choices

Your Privacy Choices

Contact us

Subscribe

Axios newsletters

Axios Pro

Axios app

Axios podcasts

Courses

Earn Axios rewards

AXIOS