North Korean Kimsuky hackers exposed in alleged data breach

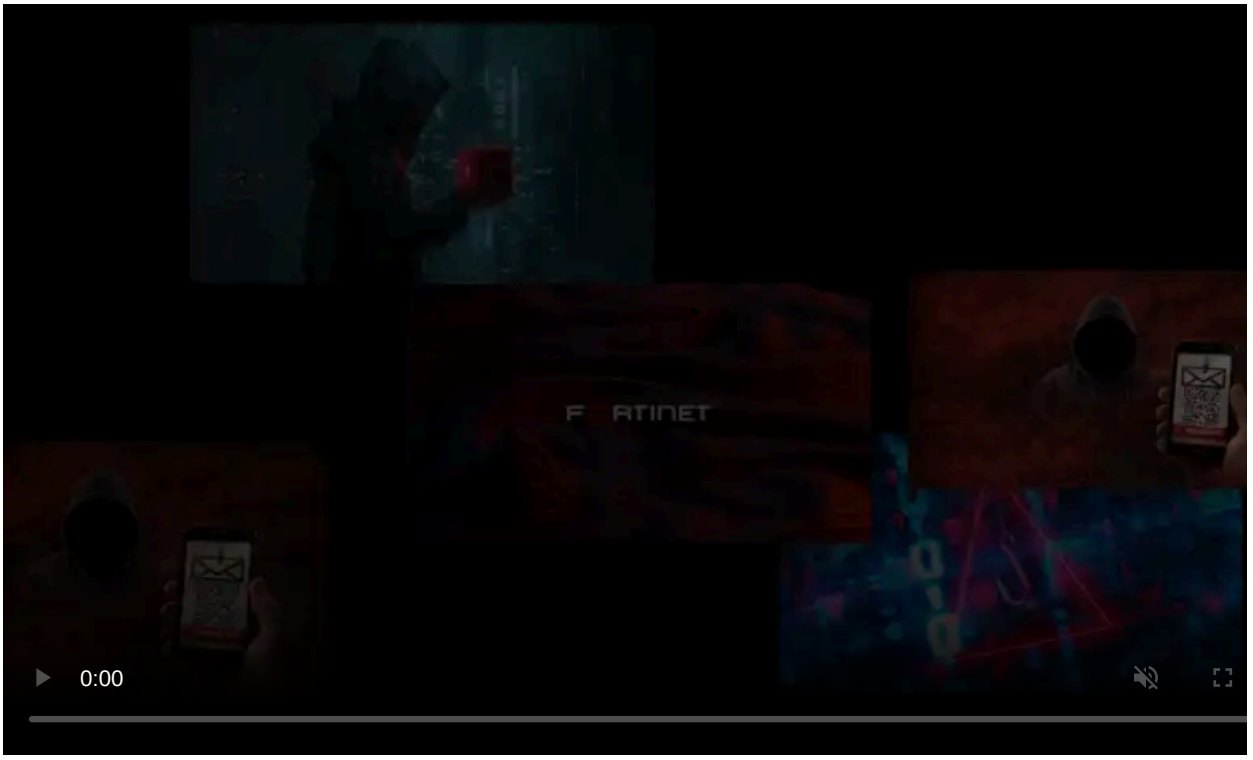
By Bill Toulas

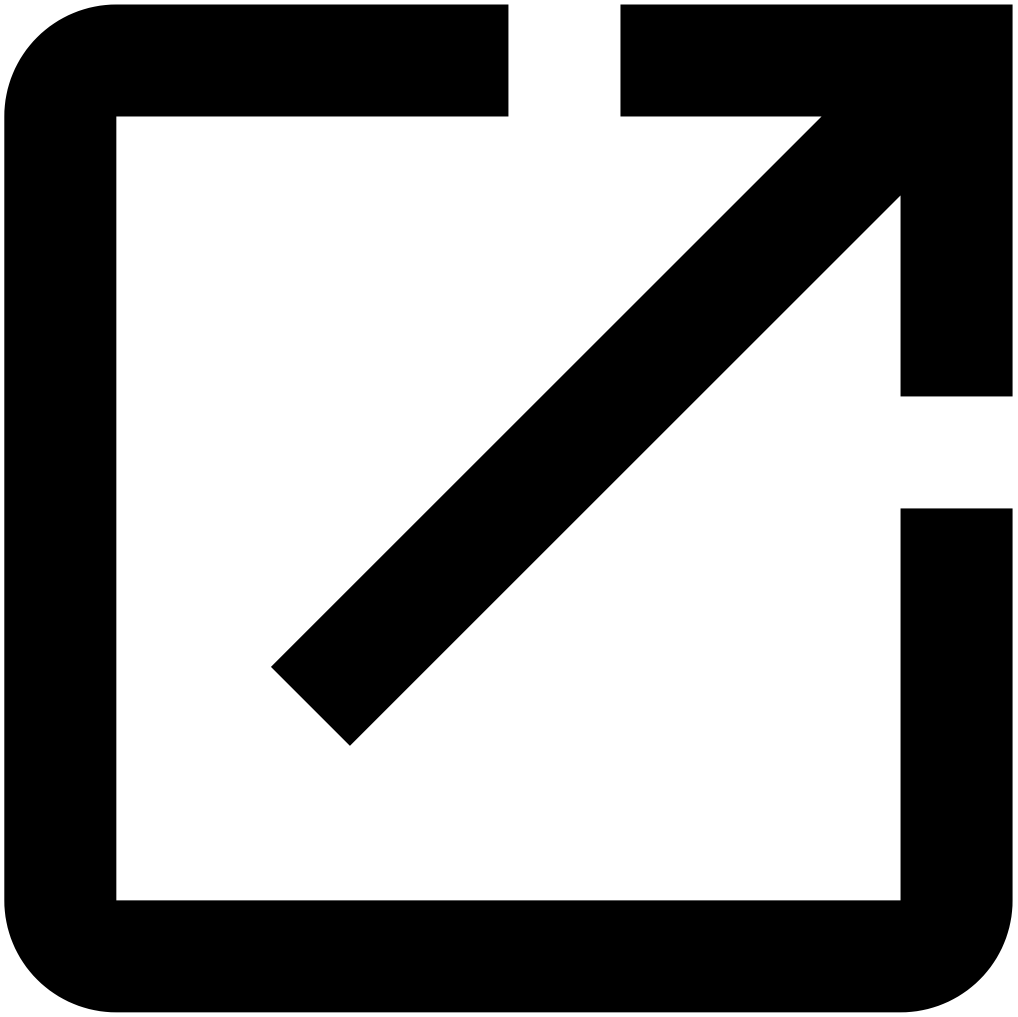
Published: 2025-08-11 · Archived: 2026-04-06 00:23:52 UTC

The North Korean state-sponsored hacking group known as Kimsuky has reportedly suffered a data breach after two hackers, who describe themselves as the opposite of Kimsuky's values, stole the group's data and leaked it publicly online.

The two hackers, named 'Saber' and 'cyb0rg,' cited ethical reasons for their actions, saying Kimsuky is "hacking for all the wrong reasons," claiming they're driven by political agendas and follow regime orders instead of practicing the art of hacking independently.

"Kimsuky, you are not a hacker. You are driven by financial greed, to enrich your leaders, and to fulfill their political agenda," reads the hackers' address to Kimsuky published in the latest issue of Phrack, which was distributed at the DEF CON 33 conference.


F RTINET
0:00



"You steal from others and favour your own. You value yourself above the others: You are morally perverted."

The hackers dumped a portion of Kimsuky's backend, exposing both their tooling and some of their stolen data that could provide insight into unknown campaigns and undocumented compromises.

The 8.9GB dump currently hosted on the 'Distributed Denial of Secrets" website contains, among others:

- Phishing logs with multiple dcc.mil.kr (Defense Counterintelligence Command) email accounts.
- Other targeted domains: spo.go.kr, korea.kr, daum.net, kakao.com, naver.com.
- .7z archive containing the complete source code of South Korea's Ministry of Foreign Affairs email platform ("Kebi"), including webmail, admin, and archive modules.
- References to South Korean citizen certificates and curated lists of university professors.
- PHP "Generator" toolkit for building phishing sites with detection evasion and redirection tricks.
- Live phishing kits.
- Unknown binary archives (voS9AyMZ.tar.gz, Black.x64.tar.gz) and executables (payload.bin, payload_test.bin, s.x64.bin) not flagged in VirusTotal.
- Cobalt Strike loaders, reverse shells, and Onnara proxy modules found in VMware drag-and-drop cache.
- Chrome history and configs linking to suspicious GitHub accounts (wwh1004.github.io, etc.), VPN purchases (PureVPN, ZoogVPN) via Google Pay, and frequent use of hacking forums (freebuf.com, xaker.ru).
- Google Translate use for Chinese error messages and visits to Taiwan government and military sites.
- Bash history with SSH connections to internal systems.

The hackers note that some of the above are already known or previously documented, at least partially.

However, the dump gives a new dimension to the data and provides interlinking between Kimsuky's tools and activities, exposing and effectively "burning" the APT's infrastructure and methods.

BleepingComputer has contacted various security researchers to confirm the veracity of the leaked documents and its value and will update the story if we receive a response.

While the breach will likely not have long-term impact on Kimsuky's operations, it could lead to operational difficulties for Kimsuky and disruptions to ongoing campaigns.

The latest issue of Phrack (#72) is currently only available in a limited physical copy, but the online version should be ready for people to read for free in the following days from here.

Source: https://www.bleepingcomputer.com/news/security/north-korean-kimsuky-hackers-exposed-in-alleged-data-breach/