Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:11:54 UTC

Tool: KGH_SPY

Names	KGH_SPY KGH Spyware Suite
Category	Malware
Type	Backdoor, Info stealer, Keylogger
Description	(Cybereason) During our analysis, Cybereason Nocturnus discovered a new malware suite dubbed “KGH” which contains several modules used as spyware. The name “KGH” is derived from the PDB path and internal names found in the malware samples. A possible link to North Korean attacks referencing the name “KGH” was mentioned in 2017 in a research by Ahnlab, however it is unclear whether it is related to the same malware authors.
Information	<https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite>
MITRE ATT&CK	<https://attack.mitre.org/software/S0526/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.kgh_spy>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool KGH_SPY

Changed	Name	Country	Observed	
APT groups				
	Kimsuky, Velvet Chollima		2012-Aug 2025	

1 group listed (1 APT, 0 other, 0 unknown)