

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:45:39 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool HOOKSHOT

Tool: HOOKSHOT

Names	HOOKSHOT
Category	Malware
Type	Tunneling
Description	(Mandiant) HOOKSHOT is a tunneler that leverages a statically linked implementation of OpenSSL to communicate back to its C2. While it connects over TCP, it does not make use of a client certificate for encryption.
Information	< https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970 >

Last change to this tool card: 25 April 2023

Download this tool card in [JSON](#) format

All groups using tool HOOKSHOT

Changed	Name	Country	Observed
APT groups			
	Lazarus Group , Hidden Cobra , Labyrinth Chollima		2007-May 2025 

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=76d5c402-eb81-4a1f-be61-6b9a3d5357b4>