

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:43:22 UTC

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

Tool: HDoor

Names	HDoor Custom HDoor
Category	Malware
Type	Reconnaissance , Backdoor , Info stealer , Wiper , Tunneling
Description	<p>(Kaspersky) The Naikon APT frequently used a custom backdoor that appears to be an HDoor variant, based on old “Honker Union” code like “hscan v120”. For example, once on a victim network, one of the first steps is to run the hdoor -hbs scan to identify target local network hosts.</p> <p>The Naikon APT’s custom-built HDoor tool is a robust reconnaissance tool for lateral movement, supporting the identification of, interfacing with and attacking of multiple technologies and resources:</p> <ul style="list-style-type: none"> • host, user, group, and related authentication resources and cracking/brute forcing capabilities • network asset scanning and identification, including SQL database, embedded network devices like home or SMB routers, and other common network services • fake service listener to sniff traffic • disk wiping – safe delete with multiple overwrites • process management • local filetime modifier • SQL administration toolset • SOCKS5 proxy service • banner-based scanner • AV killer
Information	<p><https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf></p> <p><https://securelist.com/cycldek-bridging-the-air-gap/97157/></p>
MITRE ATT&CK	< https://attack.mitre.org/software/S0061/ >

Last change to this tool card: 30 December 2022

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

All groups using tool HDoor

Changed	Name	Country	Observed
APT groups			
	Goblin Panda , Cycldek , Conimes		2013-Jun 2020
	Naikon , Lotus Panda		2010-Apr 2022

2 groups listed (2 APT, 0 other, 0 unknown)

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=69ede5dc-4d7a-4ae5-8469-e4d93f62b2a6>