Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:37:29 UTC

Tool: HKDOOR

Names	HKDOOR
Category	Malware
Type	Reconnaissance, Backdoor, Credential stealer, Info stealer
Description	(Cylance) The RAT comprises a backdoor and rootkit component, and once active allows for a typical set of remote commands, including: • Gathering system information • Grabbing screenshots and files • Downloading additional files • Running other processes and commands • Listing and killing processes • Opening Telnet and RDP servers • Extracting Windows credentials from the current session The sample of “Hacker’s Door” analyzed by Cylance was signed with a stolen certificate, known to be used by the Winnti APT group. Its discovery within an environment is a clear indication of a broader compromise.
Information	<https://threatvector.cylance.com/en_us/home/threat-spotlight-opening-hackers-door.html>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:hkdoor>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool HKDOOR

Changed	Name	Country	Observed

APT groups

	APT 41		2012-Jul 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=19d36994-3bb2-4f63-84db-15b30e3a1f2f