

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:43:19 UTC

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

Tool: SWEETCANDLE

Names	SWEETCANDLE
Category	Malware
Type	Backdoor , Downloader
Description	(FireEye) SWEETCANDLE is a downloader that can download and execute a payload received from the C&C server.
Information	< https://paper.bobylive.com/Security/APT_Report/APT-41.pdf >

Last change to this tool card: 20 April 2020

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

All groups using tool SWEETCANDLE

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=3d94c8e5-0e2f4e1c-b45b-81e26e1b3455>