Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:21:56 UTC

Tool: HALFSHELL

Names	HALFSHELL
Category	Malware
Type	Reconnaissance, Backdoor
Description	(FireEye) The malicious attachment drops the HALFSHELL malware, a .NET backdoor that can enumerate basic system information and retrieve commands to be run by cmd.exe, to the victim machine
Information	<https://content.fireeye.com/web-assets/rpt-unc1151-ghostwriter-update>

Last change to this tool card: 15 May 2021

Download this tool card in JSON format

All groups using tool HALFSHELL

Changed	Name	Country	Observed	
APT groups				
	Operation Ghostwriter		2017-Jan 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=eaeab922-e49b-4f9d-898a-b643c1c7e411