Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:25:46 UTC

Tool: POTROAST

Names	POTROAST
Category	Malware
Type	Backdoor, Exfiltration
Description	(FireEye) POTROAST is a backdoor that connects to a hard-coded C&C server. Its capabilities include downloading, uploading, and executing files and creating a reverse shell.
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 POTROAST

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=30c0b822-228c-462b-bbf0-85a0d61080d4