Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:18:51 UTC

Tool: PhpSpy

Names	PhpSpy
Category	Malware
Type	Backdoor
Description	(Symantec) The web shell is a modification of the PhpSpy backdoor and references the author MagicCoder while linking to the (deleted) domain magiccoder.ir. Researching the hacker handle MagicCoder results in references to the Iranian hacking forum Ashiyane as well as defacements by the Iranian hacker group Sun Army.
Information	<https://symantec-blogs.broadcom.com/blogs/threat-intelligence/leafminer-espionage-middle-east>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool PhpSpy

Changed	Name	Country	Observed	
APT groups				
	Leafminer, Raspite		2017	

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