Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:47:58 UTC

Tool: BlackMould

Names	BlackMould
Category	Malware
Type	Backdoor
Description	(Microsoft) In addition to standard China Chopper, GALLIUM has been observed using a native web shell for servers running Microsoft IIS that is based on the China Chopper web shell; Microsoft has called this “BlackMould.”
Information	<https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0564/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool BlackMould

Changed	Name	Country	Observed	
APT groups				
	Gallium		2018-Jun 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=edfd17d0-0e3b-416f-b030-f8f62c833336